



Actuando como la voz de la industria de la **seguridad**

Confederation of European Security Services



## Carta de **COESS** sobre el uso ético y responsable de la **Inteligencia Artificial** en los servicios de seguridad privada en Europa



#### Derechos de Autor:

A menos que se indique lo contrario, todo el material e información está sujeto a derechos de autor de CoESS (Confederación Europea de Servicios de Seguridad). Todos los derechos están reservados. No se permite la duplicación o venta de ninguna parte de este documento. Se debe obtener permiso de CoESS para cualquier otro uso. Cualquier uso no autorizado del material puede infringir las leyes de derechos de autor, marcas registradas, privacidad y publicidad, así como la normativa aplicable. En la máxima medida permitida por la ley, los autores (y todas sus empresas y organizaciones afiliadas) declinan cualquier responsabilidad por pérdidas o daños (incluyendo pérdidas o daños directos, indirectos, económicos o consecuentes) sufridos como resultado del uso de los contenidos de este manual.

#### Advertencia:

Esta Carta ha sido desarrollada por un Grupo de Expertos de CoESS para el sector de la seguridad privada europea y se centra exclusivamente en ofrecer orientación para quienes implementan sistemas de IA.

Este documento proporciona a las empresas de seguridad un conocimiento inicial de la Ley de Inteligencia Artificial de la UE y de los códigos de conducta importantes antes y durante el uso de un sistema de IA. La información contenida en esta Carta no sustituye a las evaluaciones de riesgos específicas del sistema y de los casos de uso que deben ser realizadas por el responsable del despliegue para garantizar el cumplimiento del Reglamento de IA de la UE.

#### Diseño y gráficos:

<https://blog.acapella.be/>

#### Créditos fotográficos:

© AdobeStock: 713733409: Milan, 913052673\*: suratin, 874669432\*: Andres Mejia, 588772865: NicoElNino, 846542130\*: ImageFlow, 802446835\*: ERiK, 728100169\*: Miumzlik, 355680792 and 516647240: .shock, 794014906\*: Natanong, 720464800\*: inthasone, 725689364\*: sandsun, 777449543\*: Bartek, 185898613: Kadmy, 732479109\*: ALL YOU NEED studio, 861484312\*: ALEXSTUDIO, 824935213: pressmaster, 326350464: PX Media

\* Generadas con IA

© iStock: 2130201321: Suriya Phosri, 1472578503: Pakpoom Makpan, 1428421517: Galeanu Mihai, 1168365129: metamorworks

#### Un reconocimiento especial a los colaboradores activos que han contribuido a esta Carta:

Carolina Garcia Cortés. Gerente de Innovación, Prosegur  
Cornelius Toussaint. Director General (CEO), Condor Group  
Daniel Sandberg. Director de Inteligencia Artificial, Grupo Securitas  
Graham Evans. Oficial Técnico, BSIA  
Helena Eriksvik. Directora Global de Datos Legales y Privacidad, Grupo Securitas  
Pauline Norstrom. Directora General (CEO) Anekanta®AI y representante de BSIA  
Victoria Ferrera López. Gerente Senior de Asuntos Regulatorios de Verisure  
Wim Bartsoen. Director de Seguridad Digital, Grupo Securitas

#### Acerca de CoESS:

La Confederación Europea de Servicios de Seguridad (CoESS) actúa como la voz de la industria de seguridad privada, cubriendo 22 países en Europa y representando a 45,000 empresas con 2 millones de profesionales de seguridad. Los servicios de seguridad privada brindan una amplia gama de servicios, tanto para clientes privados como públicos, que abarcan desde Infraestructuras Críticas hasta espacios públicos, cadenas de suministro y dependencias gubernamentales.

CoESS es reconocida por la Comisión Europea como la organización representante de los empleadores europeos en el sector. Estamos involucrados activamente en el Diálogo Social Sectorial Europeo y en múltiples grupos de expertos de la UE, incluyendo SAGAS, SAGMAS, LANDSEC, el Foro de Operadores para la Protección de Espacios Públicos de la UE y la Alianza de Puertos de la UE.

#### Registro de Transparencia de la UE:

**Número 61991787780-18**

## Resumen Ejecutivo

Esta Carta, desarrollada en consonancia con la Ley de Inteligencia Artificial de la UE y los valores fundamentales de CoESS, establece un marco de **10 requisitos esenciales** para la **implementación ética y responsable de la Inteligencia Artificial (IA)** por parte de las empresas de seguridad privada europeas:



**GESTIÓN DE RIESGOS:** adoptar medidas de gestión de riesgos adecuadas y específicas.



**GOBERNANZA DE DATOS:** asegurar un riguroso tratamiento de datos, garantizando la utilización de datos confiables y el estricto cumplimiento del RGPD.



**SUPERVISIÓN HUMANA:** dotar al personal de la formación y políticas necesarias para cumplir con los requisitos de supervisión humana, de acuerdo con el caso de uso específico de la IA.



**MEDIDAS DE RESILIENCIA:** conseguir una protección física y cibernética robusta para los activos de la empresa, los sistemas de IA y la infraestructura asociada.



**MANTENIMIENTO DE REGISTROS:** documentar el rendimiento operativo de los sistemas de IA.



**TRANSPARENCIA Y EXPLICABILIDAD:** implementar medidas de transparencia que garanticen el cumplimiento del RGPD y el Reglamento de IA de la UE, y aspirar a niveles adecuados de explicabilidad.



**EVALUACIÓN DEL IMPACTO EN LOS DERECHOS FUNDAMENTALES:** realizar evaluaciones del impacto potencial en los derechos fundamentales, incluso si no constituye una obligación legal, en el supuesto que haya preocupaciones plausibles sobre impactos poco probables, pero posibles.



**DILIGENCIA DEBIDA:** seguir políticas de diligencia debida al adquirir sistemas de IA.



**PARTICIPACIÓN DE LOS TRABAJADORES:** fomentar la concienciación entre los trabajadores sobre el uso de la IA en la empresa y establecer mecanismos para abordar preocupaciones, especialmente si se utilizan sistemas de IA de alto riesgo.



**INTERACCIÓN CON LAS ADMINISTRACIONES PÚBLICAS:** trabajar activamente con las autoridades competentes para obtener orientación adicional y aclarar las incertidumbres legales y los requisitos de cumplimiento.

# ÍNDICE

<b>Resumen Ejecutivo</b>	<b>3</b>
<b>Introducción</b>	<b>6</b>
<b>Capítulo I: Definición de IA y casos de uso en los servicios de seguridad privada europeos</b>	<b>8</b>
I. ¿Qué es la IA? En busca de una definición	8
II. El uso de criterios transversales para diferenciar entre IA de bajo riesgo y de alto riesgo	10
III. El Reglamento de IA de la UE y el cumplimiento normativo: IA de bajo riesgo frente a IA de alto riesgo	11
IV. Ejemplos de posibles casos de uso de IA de bajo y alto riesgo	14
<b>Capítulo II: Oportunidades y riesgos del uso de IA en los servicios de seguridad</b>	<b>18</b>
I. Oportunidades	18
II. Riesgos	20





<b>Capítulo III: Valores y Requisitos</b>	<b>25</b>
I. Los valores transversales de CoESS para el uso ético y responsable de la IA	25
II. Principales pasos para asegurar un uso ético y responsable de la IA	26
III. Requisitos para el uso ético y responsable de la IA	27
<b>Capítulo IV: Lista de comprobación</b>	<b>33</b>
<b>Anexo: Repositorio de directrices y normas útiles</b>	<b>34</b>

# Introducción

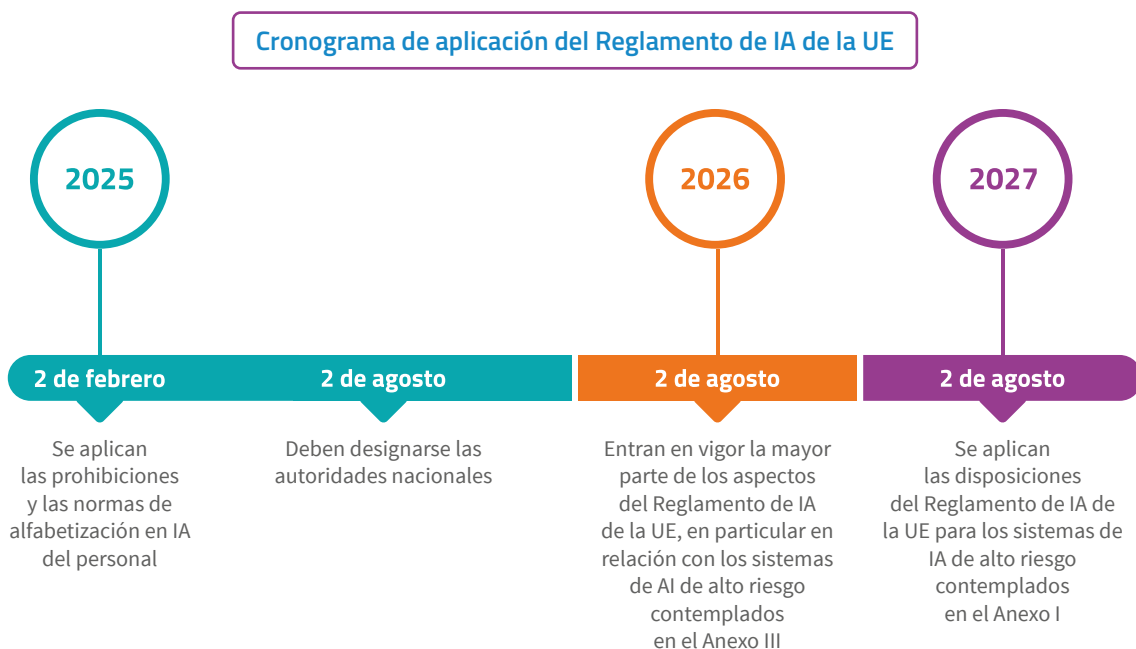
Se espera que la integración de la Inteligencia Artificial (IA) en los servicios de seguridad desempeñe un papel importante en la continua transformación de la industria de la seguridad.

Desde el análisis de riesgos habilitado por datos hasta la videovigilancia integrada, los sistemas de IA pueden implementarse en numerosos casos de uso en los servicios de seguridad, aportando beneficios para los trabajadores, clientes, empresas y la seguridad pública. Sin embargo, algunos casos de uso conllevan riesgos.

La Unión Europea (UE) ha regulado el desarrollo e implementación de la denominada IA de “alto riesgo” en el Reglamento de IA de la UE. Las empresas de seguridad que operen en la UE e integren sistemas de IA en sus servicios deberán cumplir con la mayoría de los aspectos del Reglamento a partir del 2 de agosto de 2026, si bien algunas disposiciones serán aplicables a partir del 2 de febrero de 2025 (ver gráfico cronológico).

Es importante ayudar a las empresas a comprender el impacto del Reglamento de IA de la UE en sus operaciones comerciales. Es posible que muchas empresas ni siquiera sean conscientes de si utilizan actualmente la IA en sus servicios. Sin embargo, a partir de ahora, toda empresa de seguridad, sea grande o pequeña, deberá saber si emplea un sistema de IA y qué hacer al respecto. Pero eso no es todo.

La Confederación Europea de Servicios de Seguridad (CoESS) y sus miembros defienden la innovación centrada en el ser humano para el bien público y un firme compromiso con la ética, la responsabilidad y el cumplimiento normativo.





Por lo tanto, esta Carta no solo ayudará a las empresas a cumplir con el Reglamento de IA de la UE, sino también a integrar los sistemas de IA de manera responsable y ética, yendo más allá del mero cumplimiento normativo. Para este fin, esta Carta está estructurada en cuatro capítulos:

- **EL CAPÍTULO I** ofrece orientación para ayudar a las empresas a identificar los sistemas de IA y los casos de uso de “alto riesgo” en los servicios de seguridad, basándose en criterios legales y otros criterios transversales.
- **EL CAPÍTULO II** presenta una visión general de las oportunidades y riesgos asociados con el uso de la IA en los servicios de seguridad.
- **EL CAPÍTULO III** establece requisitos para los responsables del despliegue de IA en la industria de la seguridad que abordan los riesgos pertinentes, tanto de acuerdo con las obligaciones legales del Reglamento de IA de la UE como con los valores de CoESS.
- **EL CAPÍTULO IV** proporciona una lista de comprobación fácil de entender para las empresas, detallando los pasos a seguir al planificar el uso de un sistema de IA en la actualidad.

#### ADVERTENCIA

Esta Carta ha sido desarrollada por un Grupo de Expertos de CoESS para el sector de la seguridad privada europea y se centra exclusivamente en ofrecer orientación para quienes implementan sistemas de IA.

Este documento proporcionará a las empresas de seguridad un primer conocimiento de la Ley de IA de la UE y de los códigos de conducta importantes antes y durante el uso de un sistema de IA. La información contenida en esta Carta no sustituye a las evaluaciones de riesgos y normativas específicas del sistema y de los casos de uso, que deben ser realizadas por el responsable del despliegue para garantizar el cumplimiento del Reglamento de IA de la UE.

# Capítulo I: Definición de IA y casos de uso en los servicios de seguridad privada europeos

## I. ¿Qué es la IA? En busca de una definición

La primera pregunta que cada responsable del despliegue deberá responder es: ¿Estoy utilizando IA? La definición legal de IA es, sin embargo, un ejercicio complejo con diferentes enfoques en todo el mundo. Esta Carta promueve el cumplimiento normativo, en particular, del Reglamento de IA de la UE, por lo que en este documento nos referiremos a la definición de IA establecida en la legislación de la UE.

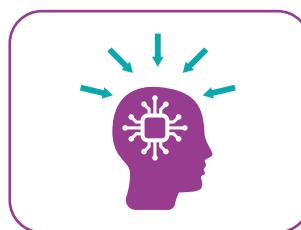
En el Reglamento de IA de la UE, la definición legal de IA se alinea estrechamente con la de la Organización para la Cooperación y el Desarrollo Económicos (OCDE). Según el Artículo 3.1 del Reglamento de IA de la UE, un sistema de IA se define como:

*“un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.”*

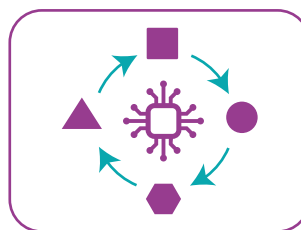
Esta definición legal es bastante compleja. Por ello, es útil revisar los Principios de IA de la OCDE<sup>1</sup>, un estándar

intergubernamental sobre IA, y analizar sus diferentes aspectos:

**AUTONOMÍA<sup>2</sup>:** Un sistema de IA puede realizar una tarea con un rango variable de implicación humana, desde una autonomía parcial hasta una autonomía total. Esto representa tanto una ventaja como un riesgo asociado con el uso de IA. Dependiendo del resultado de la tarea y del nivel de supervisión humana, incluso sistemas simples y totalmente autónomos pueden representar un riesgo sustancial para los derechos fundamentales.



**ADAPTABILIDAD:** Otro aspecto clave, aunque también un riesgo, de muchos sistemas de IA es su capacidad de autoaprendizaje, adaptación o evolución. Estos sistemas pueden evolucionar a partir de la información recibida de los usuarios, es decir, después de su diseño y uso. Esto introduce el riesgo inherente de que el sistema procese datos de una manera que a menudo se describe como una “caja negra”, reduciendo la capacidad de explicar los resultados que produce el sistema de IA.



<sup>1</sup> R. Stuart, K. Perset, M. Grobelnik (2023): Actualizaciones a la definición de un sistema de IA de la OCDE explicadas. Disponible aquí: <https://oecd.ai/en/work/ai-system-definition-update>

<sup>2</sup> Definición de autonomía en sistemas de IA: EN ISO/IEC 22989 y Considerando 12 del Reglamento de IA de la UE. Reglamento de IA, 2024/1689 <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32024R1689>



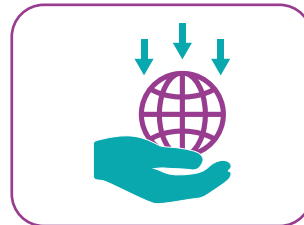
**OBJETIVOS EXPLÍCITOS E IMPLÍCITOS:** Un sistema de IA puede tener diferentes objetivos. Los objetivos explícitos son generalmente el resultado de las reglas establecidas por el desarrollador (y posiblemente también por el responsable del despliegue); por ejemplo, un dron que transporta un objeto de A a B de manera autónoma. Sin embargo, también existen sistemas de IA con objetivos implícitos, como los modelos de lenguaje a gran escala utilizados en IA de propósito general.



**INFORMACIÓN DE ENTRADA:** Los sistemas de IA se basan en la entrada de datos, que es necesaria para generar un resultado de salida. La información de entrada puede incluir conjuntos de reglas y algoritmos definidos por el desarrollador, datos de entrenamiento usados por el desarrollador para hacer evolucionar el sistema de IA, instrucciones adicionales del responsable del despliegue y datos recibidos del entorno, que pueden contribuir aún más al autoaprendizaje del sistema.



**RESULTADO DE SALIDA:** El desarrollador (y potencialmente aquellos que usan el sistema) determina las funcionalidades previstas del sistema de IA y los tipos de resultados que generará, tales como predicciones, contenido, recomendaciones o decisiones. Para producir un resultado, un sistema de IA procesa su información de entrada en base a reglas, instrucciones y algoritmos creados por sus desarrolladores y posiblemente perfeccionados por quienes lo despliegan. Las aplicaciones de alto riesgo suelen implicar resultados con impactos significativos en el mundo real y operan con un alto nivel de automatización, con escasa supervisión humana.



**ENTORNOS:** Los entornos que proporcionan datos de entrada a los sistemas de IA y que se ven afectados por sus resultados pueden ser tanto físicos (por ejemplo, la detección y verificación de objetos y personas físicas) como virtuales (por ejemplo, en el análisis de operaciones comerciales).



## II. El uso de criterios transversales para diferenciar entre IA de bajo riesgo y de alto riesgo

Los diferentes aspectos que explican el funcionamiento de los sistemas de IA también pueden utilizarse como criterios transversales interdependientes, que pueden proporcionar una primera orientación para los responsables del despliegue sobre:

- Cómo saber si un sistema es en sí mismo un producto de IA o un componente de seguridad de un producto.
- Cómo distinguir entre sistemas y casos de uso de IA de bajo riesgo y de alto riesgo.

Sin embargo, cada evaluación de un sistema y de un caso de uso de IA es única y, dentro de la UE, está sujeta a la definición de IA de bajo riesgo y de alto riesgo en el Reglamento de IA de la UE.

Otro enfoque más extenso para definir diferentes criterios y características de la IA se puede encontrar en la norma EN ISO/IEC 23053:2022 (Marco para sistemas de inteligencia artificial mediante el uso de aprendizaje automático).

### “Cada evaluación de un sistema de IA y su caso de uso es único”

<b>AUTONOMÍA</b>		Si el sistema de IA genera resultados de salida autónomos en un entorno físico, es probable que se clasifique como de alto riesgo. Por esta razón, el Reglamento de IA de la UE establece que la supervisión humana sea obligatoria para los sistemas y casos de uso de IA de alto riesgo.
<b>ADAPTABILIDAD</b>		Si el proceso de toma de decisiones del sistema de IA se basa en un autoaprendizaje lógico en una “caja negra” y evoluciona con el tiempo, esto puede conducir a una mayor falta de explicabilidad y es más probable que se categorice como de alto riesgo.
<b>OBJETIVOS</b>		Si los objetivos del sistema de IA tienen un impacto en personas físicas o son implícitos, es más probable que el sistema y el caso de uso de IA se clasifiquen como de alto riesgo.
<b>INFORMACIÓN DE ENTRADA</b>		Si la información de entrada se basa en datos personales de personas físicas, en ese supuesto el cumplimiento del RGPD es clave, y el riesgo de que se clasifique como de alto riesgo aumenta.
<b>RESULTADOS DE SALIDA</b>		Si los resultados de salida del sistema de IA representan un riesgo de daño para la salud, la seguridad o los derechos fundamentales de las personas físicas, incluido el hecho de influir materialmente en el resultado de un proceso de toma de decisiones, es probable que se clasifique como de alto riesgo.
<b>ENTORNO</b>		Si los resultados de salida afectan a un entorno en el que están presentes personas físicas, la probabilidad de que el sistema de IA y el caso de uso se clasifiquen como de alto riesgo es mayor.

### III. El Reglamento de IA de la UE y el cumplimiento normativo: IA de bajo riesgo frente a IA de alto riesgo

Los diferentes sistemas y casos de uso de IA implican diferentes niveles de riesgo. El Reglamento de IA de la UE sigue un planteamiento basado en el riesgo y regula principalmente los sistemas y casos de uso de IA de alto riesgo. Con este capítulo, buscamos proporcionar a los responsables del despliegue de sistemas de IA en los servicios de seguridad privada en Europa un conocimiento inicial del enfoque adoptado por el Reglamento de IA de la UE. Es importante recordar que se espera que la Oficina Europea de IA, dependiente de la Comisión Europea, desarrolle directrices para la definición de sistemas de IA, prohibiciones y clasificaciones de alto riesgo.

Para empezar: todo responsable del despliegue de sistemas de IA en la UE tiene que cumplir con el Reglamento de IA de la UE.

Sin embargo, esa es la única parte sencilla. Las obligaciones legales para los responsables del despliegue de sistemas de IA (véase a partir de la página 27) varían según el riesgo asociado al sistema y al caso de uso en cuestión. El Reglamento de IA de la UE distingue entre las siguientes categorías de sistemas y casos de uso de IA:

1. SISTEMAS Y CASOS DE USO DE IA DE BAJO RIESGO
2. PRÁCTICAS DE IA PROHIBIDAS
3. SISTEMAS Y CASOS DE USO DE IA DE ALTO RIESGO

#### 1. IA de bajo riesgo



La IA de bajo riesgo incluye generalmente aquellos sistemas y casos de uso de IA que no se incluyen en las categorías de “prohibidos” y de “alto riesgo”. El Reglamento (UE) 2024/1689 aclara además en su Artículo 6.3 que un sistema de IA se clasifica generalmente como de bajo riesgo si está destinado a:

- Realizar una tarea procedimental limitada o una tarea meramente preparatoria en casos de uso de IA de alto riesgo.
- Mejorar el resultado de una actividad humana previamente realizada.
- No reemplazar ni influir en la evaluación humana previamente realizada, sin una revisión humana adecuada.

Dentro de la categoría de bajo riesgo, el Reglamento distingue además entre sistemas con riesgo mínimo, sin obligaciones legales, y ciertos sistemas de IA con riesgo de transparencia, que deben cumplir con determinadas obligaciones de transparencia<sup>3</sup>.

**“Todo responsable del despliegue de sistemas de IA en la UE tiene que cumplir con el Reglamento de IA de la UE”**



<sup>3</sup> Los sistemas de IA que interactúan con personas físicas, pero que se consideran de bajo riesgo (como los modelos de lenguaje de gran tamaño (LLM) y los asistentes virtuales), deben cumplir con ciertas obligaciones de transparencia establecidas en el Artículo 50 de la Ley de IA de la UE. Por ejemplo, se debe informar a la persona en cuestión que está interactuando con un sistema de IA. Todos los sistemas de IA que no están prohibidos ni se califican como “de alto riesgo” (véase la página 13), o sistemas con un riesgo de transparencia, se consideran de riesgo mínimo. Los responsables de su despliegue no están obligados a cumplir con extensas obligaciones legales según la Ley de IA de la UE, pero se les anima a aplicar códigos de conducta voluntarios, que serán desarrollados por los organismos de la UE, los Estados miembros o entidades representativas.

## 2. Prácticas de IA prohibidas



El Artículo 5 del Reglamento (UE) 2024/1689 define aquellos sistemas y casos de uso de IA que presentan un riesgo inaceptable para los derechos fundamentales de los ciudadanos europeos. Por lo tanto, están prohibidos y no pueden comercializarse ni utilizarse en la UE a partir del 2 de febrero de 2025. Entre estos se cuentan:

- *La elaboración de perfiles para evaluar o predecir el riesgo de que una persona cometa un delito.*
- *La creación de bases de datos de reconocimiento facial mediante búsquedas automáticas de imágenes en CCTV o en Internet.*
- *La clasificación social que dé lugar a un trato desfavorable de las personas físicas.*
- *La categorización biométrica de conjuntos de datos obtenidos de manera ilícita.*
- *La identificación biométrica remota en tiempo real en espacios públicos, como el uso de tecnología de reconocimiento facial (FRT), con importantes excepciones en el ámbito de la aplicación de la ley<sup>4</sup>.*
- *El reconocimiento de emociones en el lugar de trabajo o en instituciones educativas (excepto cuando se utilice por razones médicas o de seguridad).*

La Oficina Europea de IA publicará más directrices sobre la definición de sistemas de IA así como sobre las prohibiciones.



<sup>4</sup>Existen excepciones para el uso de sistemas de identificación biométrica remota en tiempo real en espacios accesibles al público por parte de las autoridades policiales o en su nombre. Estos sistemas identifican automáticamente a una persona física sin su consentimiento. Los Estados miembros pueden permitir total o parcialmente el uso de estas tecnologías en espacios públicos, dentro de los límites establecidos en el Reglamento de IA de la UE (como autorizaciones judiciales), si se utilizan para la búsqueda específica de una víctima de secuestro o de una persona sospechosa de haber cometido un delito (según lo definido en el Anexo II del Reglamento de IA de la UE), así como para la prevención de una amenaza específica, sustancial e inminente para la vida o la seguridad física de los ciudadanos, como un ataque terrorista. Sin embargo, los Estados miembros también pueden establecer normas más restrictivas. Por lo tanto, la regulación puede variar de un Estado miembro de la UE a otro.

### 3. IA de alto riesgo



Esta es la categoría más importante, ya que el Reglamento (UE) 2024/1689 establece normas para el uso de sistemas de IA de alto riesgo.

## “El Reglamento Europeo de IA establece normas para el uso de los sistemas de IA de Alto Riesgo”

Una vez que el responsable del despliegue ha determinado si se está utilizando un sistema de IA, es importante evaluar si este se clasifica como de alto riesgo según la definición del Reglamento en su Artículo 6:

1. El sistema de IA es un producto en sí mismo o un componente de seguridad de un producto que está (1) amparado por la legislación preexistente enumerada en el Anexo I del Reglamento y (2) requiere pasar por una evaluación de terceros.

*Ejemplos: Según el Anexo I, esto concierne a drones con IA incluidos en el ámbito de aplicación del Reglamento 2018/1139, sistemas de IA utilizados en equipos de seguridad de aviación cubiertos por el Reglamento 300/2008, así como dispositivos inalámbricos habilitados por IA sujetos a la Directiva 2014/53<sup>5</sup>.*

2. Y/o se implementa en sectores de alto riesgo definidos en el Anexo III del Reglamento.

*Entre los ejemplos se encuentran los sistemas de IA destinados a ser usados:*

- ♦ *Para la identificación biométrica y el reconocimiento de emociones y que no están en el ámbito de las prácticas prohibidas. Esto incluye sistemas de identificación biométrica, que identifican a una persona física con un retraso de tiempo (no en tiempo real) y sin su intervención activa mediante la comparación de sus datos biométricos con los datos biométricos contenidos en una base de datos de referencia (véase la página 16)<sup>6</sup>. Los sistemas de verificación y autenticación biométrica (por ejemplo, como parte del control de acceso o*

*para desbloquear un dispositivo móvil, tal como se describen a partir de la página 15) no se consideran IA de alto riesgo.*

- ♦ *Como componentes de seguridad en la gestión y operación de infraestructuras críticas.*
- ♦ *Para evaluar el acceso de una persona a la educación y formación profesional.*
- ♦ *En la gestión de empleo y trabajadores, como en la selección de personal o en decisiones relacionadas con las condiciones de trabajo, la asignación de tareas, la evaluación de rendimiento y las relaciones contractuales.*
- ♦ *Para evaluar y clasificar llamadas de emergencia.*
- ♦ *Para evaluaciones de riesgo, como aquellas realizadas por autoridades de seguridad pública o en su nombre para evaluar el riesgo de que una persona física se convierta en víctima de un delito.*

## “Los responsables del despliegue, así como los desarrolladores y distribuidores de sistemas de IA de alto riesgo, deberán cumplir con las diferentes disposiciones del Reglamento (UE) 2024/1689 a partir del 2 de agosto de 2026”

Estas disposiciones se describen más detalladamente en el Capítulo III de esta Carta (véase la página 27).

Pero, ¿cómo saber con certeza si un sistema de IA es de alto riesgo o entra en un caso de uso regulado?

Es responsabilidad del proveedor de un sistema de IA documentar la evaluación para determinar si un sistema de IA es de alto riesgo o no antes de que el sistema se comercialice o entre en servicio.

Sin embargo, también depende del caso de uso. Los productos y casos de uso de alto riesgo están definidos para los responsables del despliegue en el Reglamento (UE) 2024/1689 en el Artículo 6 y en los Anexos I y III, aunque el Reglamento es complejo.

La Comisión Europea desarrollará directrices sobre la implementación de la clasificación de alto riesgo. Mientras tanto, los criterios transversales a los que hemos hecho referencia pueden proporcionar a los responsables del despliegue una primera orientación.

<sup>5</sup> Se esperan más directrices de la Oficina Europea de IA sobre la definición de sistemas de alto riesgo y la existente legislación sobre productos.

<sup>6</sup> Se espera que la Oficina Europea de Inteligencia Artificial publique próximamente directrices adicionales sobre la definición de sistemas de IA, prohibiciones y clasificación de alto riesgo.

## IV. Ejemplos de posibles casos de uso de IA de bajo y alto riesgo en los servicios de seguridad europeos

### ADVERTENCIA

Este documento proporciona a las empresas de seguridad un conocimiento inicial de posibles sistemas y casos de uso de IA de bajo riesgo y alto riesgo. La información contenida en esta Carta no sustituye a las evaluaciones de riesgos y normativas específicas del sistema y de los casos de uso, que deben ser realizadas por el responsable del despliegue para garantizar el cumplimiento del Reglamento de IA de la UE.

### Casos de uso de IA de bajo riesgo



Cabe suponer que muchos casos de uso de IA en los servicios de seguridad no se califican como de alto riesgo. Teniendo en cuenta el Reglamento de IA de la UE y nuestros criterios transversales, se espera que los siguientes casos de uso en los servicios de seguridad pertenezcan a la categoría de bajo riesgo:

#### 1. Análisis de riesgos



Mediante la recopilación de grandes volúmenes de datos no personales de infraestructuras de seguridad existentes, como cámaras de video, los sistemas de IA pueden proporcionar a los

clientes información específica sobre sus medidas de seguridad y recomendaciones de mejora. Cuando se usan aplicaciones de IA de este tipo, las empresas de seguridad pueden ofrecer de forma rápida información concreta basada en datos y análisis predictivo sobre tendencias y patrones como:

- Patrones históricos de flujo y movimiento de visitantes.
- Horarios, días o meses de mayor afluencia de visitantes y de delitos en una instalación o vecindario.

- Evaluaciones de vulnerabilidad de una instalación, basadas en los planes de seguridad existentes.

Este tipo de análisis de riesgos puede mejorar la toma de decisiones y hacer que los servicios de seguridad sean más efectivos. Las empresas de seguridad pueden ofrecer recomendaciones para proporcionar un conjunto de soluciones específicas, como personal adicional o tecnologías específicas.

#### 2. Análisis de operaciones comerciales



Las aplicaciones de IA también pueden analizar la eficiencia de las operaciones comerciales internas, en base a datos como:

- Períodos de mayor uso de ciertos servicios comerciales.
- Gestión de instalaciones, como por ejemplo los niveles de eficiencia energética de los edificios, productos y flotas de vehículos.
- Seguimiento de visitantes.
- Datos sobre incidentes de salud y seguridad en el trabajo.
- Impacto de los servicios proporcionados con fines de marketing.

Las operaciones comerciales internas, y por lo tanto los servicios ofrecidos a los clientes, pueden adaptarse para ser más rentables, ecológicos y seguros. Las evaluaciones del impacto de los servicios pueden utilizarse con fines de marketing.

#### 3. Gestión de multitudes



La videovigilancia habilitada con IA puede usarse para controlar el número de personas presentes en un evento, identificar automáticamente ubicaciones con alta densidad de visitantes, analizar los patrones de movimiento de la multitud, así como identificar cuellos de botella que pueden generar riesgos para la seguridad de los visitantes. El personal en el lugar puede tomar las medidas correspondientes, por ejemplo, en el control de acceso o dirigiendo el flujo de personas.



Estos sistemas son especialmente útiles en eventos multitudinarios, como partidos de fútbol o festivales, y resultan valiosos para guiar a los primeros intervinientes y ayuda de emergencia durante un incidente. Sin embargo, el uso de tales sistemas probablemente se clasifique como de alto riesgo si comienza a incluir datos personales en su análisis y resultados (por ejemplo, si el sistema comienza a recopilar datos biométricos y los combina con datos no personales para producir ciertos resultados, como la identificación biométrica o la categorización).

#### 4. Verificación biométrica



Los sistemas de verificación biométrica son muy distintos de los sistemas de identificación biométrica:

- Los sistemas de verificación confirman que una persona es quien dice ser al comparar sus datos biométricos con los proporcionados previamente (Pregunta: ¿Eres tú?).
- Los sistemas de identificación identifican a una persona desconocida sin su consentimiento (Pregunta: ¿Quién es? Véase la página 16).

Por lo tanto, el Anexo III del Reglamento de IA de la UE clasifica como de “alto riesgo” los sistemas de identificación biométrica, pero no los sistemas de verificación. La verificación biométrica puede mejorar significativamente la efectividad y eficiencia del control de acceso, especialmente en instalaciones sensibles como infraestructuras críticas.

#### 5. Otros casos de uso de análisis de datos no personales habilitados por IA



La lista de posibles casos de uso de análisis de datos habilitados por IA podría extenderse indefinidamente. Especialmente como parte de los servicios de videovigilancia, el potencial para ofrecer servicios más efectivos, precisos y rápidos es inmenso:

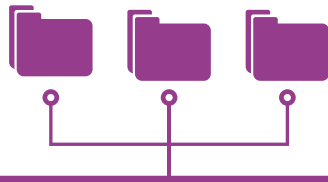
- **Verificación de alarmas:** Las cámaras habilitadas con IA pueden utilizarse para ayudar a diferenciar entre alarmas reales y falsas en centrales receptoras de alarmas (CRA). Por ejemplo, una cámara puede distinguir, basándose en la forma y patrones de movimiento, si quien acaba de entrar en el perímetro de una instalación vigilada es un perro o una persona. El sistema puede así verificar la alarma, determinar

si probablemente sea falsa, y proporcionar una recomendación al operador de la CRA. Esto puede reducir el tiempo de respuesta a incidentes reales y mejorar tanto la eficiencia operativa como el nivel de protección proporcionado a un cliente.

- **Análisis de objetos:** Similar a la verificación de alarmas, los sistemas de IA pueden analizar y clasificar rápidamente ciertos objetos detectados. Por ejemplo, pueden analizar si determinado vehículo está autorizado a estar en una zona restringida (por ejemplo, basándose en una base de datos o lista blanca de matrículas “autorizadas”). En un caso más crítico, un sistema de detección de drones habilitado con IA podría analizar rápidamente si un dron lleva una carga potencialmente peligrosa y evaluar su velocidad y el tiempo probable de impacto. Esta información puede mejorar enormemente el tiempo de respuesta y la toma de decisiones en las medidas contra drones.
- **Detección de comportamientos:** Las cámaras de CCTV pueden verse potenciadas por aplicaciones de IA para identificar comportamientos sospechosos asociados a delitos, como patrones de movimiento y otras actividades. Los sistemas de IA pueden entonces emitir una alerta, que será evaluada por el personal de seguridad en el terreno o en una CRA antes de tomar medidas preventivas. Este tipo de casos de uso mejoran las medidas de seguridad y permiten respuestas rápidas en situaciones críticas.

Sin embargo, el uso de IA en sistemas de videovigilancia puede caer rápidamente en la categoría de alto riesgo, dependiendo de los datos que se utilicen, el nivel de supervisión humana/autonomía, y los resultados que proporcione el sistema.





## Casos de uso de IA de alto riesgo

Los casos de uso de IA de alto riesgo pueden proporcionar un valor sustancial en los servicios de seguridad, pero deben garantizar el cumplimiento del Reglamento de IA de la UE y de esta Carta.

El Reglamento (UE) 2024/1689 establece muchas categorías de productos y casos de uso que se clasifican automáticamente como de alto riesgo. Basándose en esta definición legal (véase la página 13) que también puede contrastarse con nuestros criterios transversales, cabe esperar que los siguientes casos de uso en los servicios de seguridad entren en la categoría de alto riesgo:

### 1. Identificación biométrica



El Reglamento de IA de la UE identifica claramente las tecnologías de identificación biométrica como prohibidas en gran medida (identificación en tiempo real en espacios públicos) o como sistemas de

IA de alto riesgo (identificación remota posterior al evento). Los sistemas de reconocimiento facial (FRT) son un ejemplo típico de tecnología de identificación biométrica. Para fines de identificación, los sistemas de FRT comparan el mapa facial de una persona con una base de datos de datos biométricos a la que la persona podría no haber dado su consentimiento (en contraste con los sistemas de verificación o autenticación biométrica, que se basan en el consentimiento del titular de los datos y se utilizan para el control de acceso o desbloquear un dispositivo móvil).

El uso de sistemas de identificación biométrica en espacios públicos puede ser muy valioso en la búsqueda de terroristas y otras personas de interés, y por lo tanto es de gran beneficio para las autoridades de seguridad pública. Sin embargo, también puede presentar riesgos sustanciales para los derechos fundamentales de los ciudadanos de la UE, particularmente porque pueden usarse sin el consentimiento explícito del titular de los datos.

Según nuestros criterios transversales, los sistemas de FRT proporcionan recomendaciones autónomas desarrolladas en una “caja negra” basándose en la comparación de datos biométricos. La información de entrada se basa en

datos personales, posiblemente sin el consentimiento del interesado. Sus objetivos son explícitos, pero sus resultados pueden tener consecuencias legales para las personas físicas. Esto hace que la supervisión humana de esta tecnología, que aborde todos estos riesgos, sea especialmente importante.

Por lo tanto, el Reglamento de IA de la UE prohíbe en gran medida el uso de identificaciones biométricas en tiempo real y establece salvaguardas adicionales para el uso de identificaciones posteriores al evento en comparación con otra IA de alto riesgo<sup>7</sup>. Para una orientación adicional, la Asociación de la Industria de Seguridad Británica (BSIA) ha publicado una guía sobre el uso ético y legal del reconocimiento facial, disponible en <https://www.bsia.co.uk/>, que es muy útil para las empresas de seguridad que desean no solo cumplir con la ley, sino también adherirse a importantes valores éticos<sup>8</sup>.

### 2. Reconocimiento de emociones



Los sistemas de reconocimiento de emociones identifican las emociones o intenciones de las personas basándose en sus datos biométricos. Estas tecnologías funcionan de manera similar a otros sistemas

de detección de comportamientos, pero su uso se basa en la evaluación de los datos biométricos de una persona, quien podría no haber dado su consentimiento para su uso. Su implementación puede ser más eficiente que los sistemas de detección de comportamientos habilitados por IA de bajo riesgo. Sin embargo, al igual que los sistemas de identificación biométrica, cumplen con todos los criterios transversales para ser considerados de alto riesgo, y están claramente identificados en el Reglamento de IA de la UE como sistemas de IA prohibidos (por ejemplo, en el lugar de trabajo y en instituciones educativas) o como sistemas de IA de alto riesgo con obligaciones adicionales de transparencia.

### 3. Detección de objetos prohibidos en seguridad aeroportuaria



Un ejemplo típico de sistemas habilitados por IA en la seguridad aeroportuaria son los “Sistemas Automáticos de Detección de Objetos Prohibidos” (APIDS, por sus siglas en inglés). Estos sistemas

identifican automáticamente objetos prohibidos en la seguridad aeroportuaria en función de las imágenes y datos que les han sido proporcionados por los desarrolladores. El uso de equipos de seguridad aeroportuaria habilitados

<sup>7</sup> Por ejemplo, no se deberá tomar ninguna decisión basada únicamente en los resultados de estos sistemas, y dichos resultados siempre deberán ser revisados por al menos dos personas físicas debidamente cualificadas y autorizadas, excepto si los Estados miembros consideran que este requisito es desproporcionado en casos de uso relacionados con la aplicación de la ley.

<sup>8</sup> Además de la Guía de la BSIA, próximamente se publicará un nuevo estándar británico (BS 9347) que orientará a los usuarios de la industria de la seguridad hacia políticas seguras y confiables para la verificación e identificación a lo largo de la cadena de suministro de la tecnología de reconocimiento facial.

## “Los casos de uso de IA de alto riesgo pueden proporcionar un valor sustancial en los servicios de seguridad, pero deben garantizar el cumplimiento del Reglamento de IA de la UE y de esta Carta”

con IA puede mejorar significativamente las medidas de seguridad y la eficacia operativa en los aeropuertos, siempre que se acompañe de una supervisión humana adecuada. Sin embargo, los sistemas de detección habilitados por IA como APIDS también pueden presentar riesgos sustanciales, particularmente debido al entorno en el que funcionan: no detectar un objeto prohibido en el entorno de seguridad aeroportuaria puede tener consecuencias significativas para la seguridad pública. Por ello, el Reglamento de IA de la UE los clasifica automáticamente como de alto riesgo<sup>9</sup>, lo cual resulta lógico si aplicamos nuestros criterios transversales.

### 4. Drones habilitados por IA



Hoy en día, la IA es un componente esencial de seguridad en vehículos no tripulados, especialmente en el caso de drones autónomos. Los algoritmos de IA permiten que los drones operen de forma autónoma, reduciendo la necesidad de intervención humana. Los drones pueden incluir sensores habilitados por IA y sistemas de detección que proporcionan información en tiempo real a un profesional de seguridad o al propio dron autónomo. Los drones habilitados con IA pueden ayudar a los profesionales de seguridad a tomar decisiones informadas en tiempo real. Los profesionales de seguridad pueden monitorizar grandes áreas con varios drones a la vez, sin tener que pilotarlos todos, lo que hace que las tareas de vigilancia sean mucho más eficientes. Además, la integración de sistemas de IA puede hacer que las operaciones con drones sean más seguras, ya que pueden ayudar al dron a adaptarse a las condiciones de vuelo cambiantes, como la entrada en zonas de exclusión aérea y condiciones meteorológicas adversas.

Sin embargo, el nivel avanzado de autonomía y los riesgos para el entorno físico hacen que sea necesario someter el uso de drones habilitados con IA a reglas específicas. Por ejemplo, un dron autónomo que funcione incorrectamente representa un riesgo tanto para las personas en tierra como para los vehículos aéreos. El Reglamento de IA de la UE, por lo tanto, clasifica todos los sistemas de IA como de “alto riesgo” tanto si son un componente de seguridad de un producto como si ellos mismos son un producto sujeto al Reglamento de Drones de la UE, y deben superar una evaluación de terceros<sup>10</sup>.

### 5. Gestión de recursos humanos



El uso de la denominada “gestión algorítmica” en el lugar de trabajo puede apoyar sustancialmente la asignación de tareas y la selección de personal, especialmente en empresas con un alto número de empleados.

- **Asignación de tareas:** El análisis de operaciones comerciales con IA puede proporcionar recomendaciones a la gerencia sobre la asignación de trabajadores en diferentes servicios y turnos. Existe por tanto un gran potencial para optimizar la organización del trabajo, lo que puede contribuir a ganancias de productividad que beneficien a las empresas y a los trabajadores. Al mismo tiempo, los sistemas de IA no pueden considerar el trabajo realizado por los trabajadores desde una perspectiva humana, como lo haría un gestor humano, teniendo en cuenta las habilidades sociales y las relaciones interpersonales. Por tanto, la supervisión humana es clave.
- **Selección de personal:** Si se basan en datos confiables, los análisis con IA pueden ayudar a emparejar mejor los perfiles laborales con los candidatos potenciales, en beneficio de las empresas, de los solicitantes de empleo y de los lugares de trabajo inclusivos.

Estos casos de uso y las oportunidades asociadas también conllevan riesgos y tienen un posible impacto en el trabajador, tanto en la asignación de tareas como en sus oportunidades en el mercado laboral. En particular en la selección de personal, dependiendo de la programación del sistema, la IA también puede llevar a una discriminación sistémica de ciertos grupos de trabajadores. Los resultados del sistema de IA pueden afectar las perspectivas de carrera profesional futuras, los medios de vida de estas personas y los derechos de los trabajadores. Por lo tanto, el uso de IA para la gestión de recursos humanos se clasifica automáticamente como de alto riesgo en el Reglamento de IA de la UE cuando estos sistemas están destinados a ser utilizados para la contratación o selección de personas físicas, o para decisiones de gestión que afecten a la relación contractual del trabajador y a la asignación de tareas. Es importante destacar que los responsables del despliegue de estos sistemas de IA deben garantizar, según el Reglamento de IA de la UE, la información a los trabajadores afectados y a sus representantes antes de su uso.

<sup>9</sup> Como todos los sistemas de IA que forman parte de productos regulados por el Reglamento N.º 300/2008 sobre normas comunes en el ámbito de la seguridad de la aviación civil, y que deben pasar por una evaluación de terceros. Se espera que la Oficina Europea de IA publique próximamente directrices adicionales sobre la interacción entre la definición de alto riesgo de la Ley de IA de la UE y la existente legislación sobre productos.

<sup>10</sup> Se espera que la Oficina Europea de IA publique próximamente directrices adicionales sobre la interacción entre la definición de alto riesgo de la Ley de IA de la UE y la existente legislación sobre productos.

# Capítulo II: Oportunidades y riesgos del uso de IA en los servicios de seguridad

Los ejemplos de casos de uso demuestran que el uso de IA puede aportar numerosos beneficios a la seguridad pública y a los ciudadanos europeos. **La integración de la IA en los servicios de seguridad transforma los conceptos de seguridad, mejora la resiliencia operativa de las empresas, hace que las misiones de los trabajadores de seguridad sean más seguras y conduce a servicios de seguridad más efectivos.** Sin embargo, aunque la tecnología de IA encierra un gran potencial para ayudar a los profesionales de la seguridad a identificar y combatir mejor las actividades delictivas, su uso también requiere evaluaciones de riesgo rigurosas. Este capítulo analiza las oportunidades más importantes que los servicios basados en IA pueden aportar a los ciudadanos, empresas y trabajadores europeos, pero también los principales factores de riesgo y los resultados no deseados.

**“Al integrar la IA en los servicios, esta deberá aportar valor añadido garantizando la complementariedad y la sinergia entre las personas y las tecnologías”**

## I. Oportunidades

### 1. Mayor rendimiento en seguridad por medio de sinergias con servicios centrados en las personas

**La integración de la IA en soluciones de seguridad no es un fin en sí mismo. Al integrar la IA en los servicios, esta debe aportar valor añadido asegurando la complementariedad y sinergia entre personas y tecnologías,** proporcionando a los trabajadores de seguridad un “sexto sentido” que se traduce en un nivel de seguridad sin precedentes.

#### 1.1. Identificación, clasificación y mitigación de riesgos de seguridad basados en datos en tiempo real

**Las nuevas capacidades para detectar, clasificar y responder rápidamente a movimientos sospechosos, intrusiones o anomalías se destacan como una ventaja fundamental de la integración de la IA en los servicios de seguridad:**

- ♦ Los sistemas de análisis de objetos y detección de elementos prohibidos basados en IA pueden analizar y clasificar rápidamente los objetos o peligros detectados.
- ♦ Los sistemas (ópticos, acústicos) de detección de comportamiento y reconocimiento de emociones pueden ayudar a identificar comportamientos inusuales y acelerar la intervención para una mejor protección de los espacios públicos e Infraestructuras Críticas.
- ♦ Los drones dotados de IA y la tecnología C-UAS (tecnología anti-drones) ofrecen una herramienta adicional de gran valor en la vigilancia y supervisión remota de Infraestructuras Críticas y espacios públicos, especialmente en grandes perímetros (por ejemplo, vías de tren, tuberías, infraestructuras energéticas en el mar, etc.).
- ♦ Los sistemas de identificación biométrica remota pueden aportar un valor considerable en la búsqueda



dirigida de terroristas, otras personas específicas de interés y personas vulnerables.

- ♦ La IA puede ayudar a distinguir entre alarmas reales y falsas en las Centrales Receptoras de Alarmas (CRA) y mantener niveles constantes de calidad en el servicio.

Todos estos casos de uso ofrecen información útil en tiempo real, que puede proporcionar al personal de seguridad un “sentido” adicional, mejorar las medidas de seguridad mediante una mayor capacidad de decisión y reducir el tiempo de respuesta en caso de incidente. Los servicios de seguridad se vuelven más sofisticados y alcanzan un nuevo nivel de “inteligencia”.

### 1.2. Mayor adaptabilidad de las soluciones de seguridad

**La IA hace que los servicios de seguridad sean más ágiles y permite adaptar los servicios a las necesidades de los clientes en tiempo real.**

El análisis de riesgos utilizando la IA puede guiar la toma de decisiones informada y orientar las soluciones de seguridad a las necesidades específicas de un cliente, fortaleciendo así la resiliencia de la instalación del cliente, previniendo incidentes futuros mediante el análisis predictivo y mejorando la seguridad de los trabajadores y de los agentes de seguridad.

En la gestión de multitudes, la IA puede proporcionar información rápida a los proveedores de servicios de seguridad en entornos difíciles y facilitar la toma de decisiones informadas en tiempo real, lo que hace que la gestión de multitudes sea más efectiva, permite tomar decisiones rápidas y adaptar las medidas de protección y seguridad, y mejora sustancialmente la seguridad en eventos.

### 1.3. Potenciación de los trabajadores a través de la automatización

**La IA aporta a los trabajadores de seguridad nuevos conocimientos e información gracias a la automatización de tareas.**

Los sistemas de verificación biométrica apoyan a los trabajadores en la comprobación de la identidad de personas y el control de acceso, particularmente en instalaciones sensibles como Infraestructuras Críticas.

Los drones automatizados pueden ayudar a los agentes de seguridad remotos a tomar decisiones informadas en tiempo real, permitiendo la vigilancia de áreas amplias o múltiples con enjambres de drones sin tener que pilotarlos todos. La seguridad de las operaciones se sustenta en el análisis mediante IA de parámetros externos, como las condiciones meteorológicas.

La clasificación de alarmas evita que los agentes de seguridad tengan que validar repetidamente falsas alarmas que causan molestias (por ejemplo, en ciertas condiciones meteorológicas como nevadas) y les permite centrarse en sus tareas principales, evitando la sobrecarga de información. Cualquier tipo de análisis de datos y sensores ópticos/acústicos con IA puede reducir la carga de tareas estándar de los trabajadores de seguridad y apoyar la toma de decisiones.

### 1.4. Mejora de la protección de datos y la ciberseguridad

**La IA puede mejorar la protección de datos y la ciberseguridad** al apoyar a los analistas en la detección acelerada de amenazas y anomalías en el acceso a datos, ahorrando un valioso tiempo de respuesta. La IA puede apoyar significativamente las evaluaciones de riesgo cibernético y ayudar a detectar phishing, malware y otras actividades maliciosas.

## 2. Beneficios para empresas y trabajadores

Los beneficios de la IA en los servicios de seguridad no son excluyentes: muchos casos de uso no solo representan una oportunidad para la seguridad pública y la protección de los clientes, sino también para las empresas de seguridad y los trabajadores.



### 2.1. Mayor seguridad y protección de los trabajadores

**Un activo clave del uso de la IA es un mayor nivel de protección de los trabajadores de seguridad.** El análisis de riesgos con IA puede tener en cuenta los riesgos laborales de los trabajadores de seguridad. La IA permite a los trabajadores detectar y validar riesgos de forma remota. Los drones y robots con IA no solo proporcionan a los agentes de seguridad una mejor visión general de los riesgos potenciales, sino que también les evitan adentrarse en entornos peligrosos.

### 2.2. Promoción de lugares de trabajo inclusivos

La OCDE<sup>11</sup> destaca que **el uso de la gestión algorítmica en el lugar de trabajo puede ayudar a aumentar la diversidad, la inclusión, la igualdad y la no discriminación.** Es crucial, por ello, utilizar datos confiables. El uso de IA en el lugar de trabajo debe basarse en datos relevantes y de alta calidad para combatir el sesgo o la discriminación en el trabajo. De esta forma, la gestión algorítmica puede promover evaluaciones más objetivas de solicitudes de empleo y de rendimiento, así como ofrecer mejores oportunidades de reconocimiento y promoción a trabajadores que tradicionalmente han sufrido prejuicios en el mercado laboral.

### 2.3. Nuevas oportunidades laborales

**La mejor capacitación y protección de los trabajadores en los servicios dotados de IA pueden hacer que la profesión de servicios de seguridad sea más atractiva.** En su investigación, la OCDE descubrió que, en sectores como la manufactura o las finanzas, la reducción del tiempo dedicado

por los trabajadores a tareas repetitivas les ofrecía una mayor oportunidad de dedicar tiempo a tareas más estratégicas<sup>12</sup>. Además, las tareas relacionadas con servicios dotados de IA pueden atraer a nuevos grupos de trabajadores, actualmente insuficientemente representados en los servicios de seguridad europeos, como mujeres y jóvenes.

### 2.4. Optimización de las operaciones comerciales y de la competitividad

**La optimización de operaciones comerciales basada en datos puede mejorar la resiliencia operativa, ayudar a mantener la calidad en el servicio y permitir inversiones basadas en información, aumentando la competitividad en la industria.** La IA puede respaldar procesos operativos para que sean más rentables, sostenibles medioambientalmente y seguros, con beneficios para los trabajadores, las empresas de seguridad y los clientes, por ejemplo, mediante una mejor programación de turnos o planificación de rutas de las patrullas.

## II. Riesgos

**Junto a estas oportunidades, es importante reconocer que el uso de la IA puede implicar riesgos.** Lograr un equilibrio entre aprovechar el potencial de la IA y mitigar sus riesgos requiere una cuidadosa consideración de las implicaciones éticas, legales, sociales y de seguridad relacionadas con el uso en cuestión.

Este capítulo ofrece una breve visión general de importantes categorías de riesgos asociados al uso de IA en servicios de seguridad.

<sup>11</sup> OCDE (2023), *Perspectivas del Empleo de la OCDE 2023: Inteligencia Artificial y el Mercado Laboral*, Publicaciones de la OCDE, París, <https://doi.org/10.1787/08785bba-en>.

<sup>12</sup> OCDE (2023), *Perspectivas del Empleo de la OCDE 2023: Inteligencia Artificial y el Mercado Laboral*, Publicaciones de la OCDE, París, <https://doi.org/10.1787/08785bba-en>.



## Factores de riesgo

Cuando hablamos de riesgos relacionados con el uso de la IA, el discurso público a menudo se centra en el posible impacto negativo de su uso. Sin embargo, primero deberíamos centrarnos en los factores de riesgo.

Para quienes implementan estos sistemas, existen cinco factores de riesgo principales, que se refuerzan entre sí y que deben abordarse de forma holística antes y durante el uso de la IA:

### 1. Falta de procesos diligentes de gestión de riesgos

La IA no es una tecnología cualquiera. La ausencia de un proceso de gestión de riesgos específico y diligente para el caso de uso a lo largo del ciclo de vida de un sistema de IA puede dar lugar a incumplimientos de la legislación pertinente (como el Reglamento de IA de la UE o el RGPD) y a riesgos inesperados para la salud, la seguridad o los derechos fundamentales de los ciudadanos y el personal de seguridad.

### 2. Uso de conjuntos de datos no confiables y sesgados

El uso de datos poco confiables en las aplicaciones de IA puede dar lugar a la amplificación de sesgos en las decisiones de IA, producir resultados no fiables y generar riesgos para los derechos fundamentales, lo que socava la explicabilidad y la responsabilidad de los sistemas de IA, así como la confianza en ellos, y puede acarrear importantes riesgos reputacionales para quienes implementan estas tecnologías.

### 3. Falta de supervisión humana

La supervisión humana es fundamental en el uso de IA en servicios de seguridad. Su ausencia puede ser consecuencia de una dotación insuficiente de personal o de que este no esté capacitado o gestionado de manera adecuada para operar eficazmente el sistema en el caso de uso específico. La falta de supervisión humana puede conllevar una pérdida de explicabilidad del funcionamiento y de los resultados del sistema de IA. El personal puede confiar excesivamente en los resultados del sistema, como falsos positivos o negativos. La falta de supervisión humana no solo limita, desvía y/o socava la autonomía humana, sino que es un factor de riesgo significativo para la salud, la seguridad y los derechos fundamentales de los ciudadanos.

### 4. Falta de resiliencia

Los sistemas de IA y sus algoritmos deben ser resilientes frente a manipulaciones físicas y ciberataques. De lo contrario, su funcionamiento y sus resultados pueden ser influenciados o desactivados, lo que genera riesgos sustanciales, especialmente en los casos de uso en servicios de seguridad.

### 5. Falta de gobernanza de la IA

Una política específica de gobernanza de la IA debe asignar a un responsable y establecer una cadena clara de procesos y responsabilidades, de manera que la responsabilidad última y la obligación de rendir cuentas sobre el buen uso o mal uso de la IA recaiga en la Junta Directiva o el órgano de gobierno de quien implemente la tecnología. Sin dicha política, existe el riesgo de que aquellos responsables legales puedan negar tener conocimiento o responsabilidad (“negación plausible”), y que los niveles de gestión en la empresa hayan adoptado medidas sin la participación de dicho órgano.

## Categorías de riesgo

Estos factores de riesgo pueden traducirse en una variedad de riesgos materiales e inmateriales específicos de cada caso de uso, que se resumen a continuación en diferentes categorías:

### 1. Riesgos para los derechos fundamentales de los ciudadanos

**En el debate público, el uso general de la IA genera temores de que los derechos fundamentales puedan ser vulnerados** debido a:

- ♦ una pérdida de autonomía humana y de la explicabilidad de los sistemas de IA;

- ♦ desconfianza hacia diferentes casos de uso y sus objetivos/fines;
- ♦ preocupaciones sobre la privacidad de los datos y los conjuntos de datos utilizados como información de entrada para el sistema de IA;
- ♦ la vulneración de derechos fundamentales importantes debido a los resultados de salida del sistema.

Las violaciones de los derechos fundamentales pueden ser materiales o inmateriales, e incluir daños físicos, psicológicos, sociales o económicos. Los riesgos asociados al uso de la IA para fines de seguridad, especialmente para la aplicación de la ley, incluyen temores de una vigilancia masiva e intrusiva, violaciones de la privacidad de datos, prácticas de seguridad discriminatorias y falta de rendición de cuentas en caso de mal funcionamiento del sistema y

sus consecuencias<sup>13</sup>. Las salvaguardas contra estos riesgos están contempladas en el Reglamento de IA de la UE y son cruciales para el uso ético y legal de la IA en los servicios de seguridad (véase el Capítulo III).

## 2. Riesgos para los derechos de los trabajadores y la salud y seguridad en el trabajo

**El uso de la IA también puede implicar riesgos para los trabajadores**, especialmente los asociados a herramientas de gestión algorítmica de trabajadores<sup>14 15</sup>, entre los que se cuentan:

- ◆ Discriminación de trabajadores debido al uso de conjuntos de datos sesgados en el uso de sistemas de gestión algorítmica durante procesos de contratación, renovación de contratos, asignación de tareas y acceso a la formación.
- ◆ Percepción de un entorno laboral de alto estrés debido a un ritmo de trabajo más intenso, a una mayor complejidad en las tareas y los flujos de información y a la percepción de una vigilancia y evaluación constante.
- ◆ Reducción de la interacción humana con compañeros y supervisores si se pide a los trabajadores que trabajen cada vez más de manera aislada.

El Reglamento de IA de la UE y otras normativas europeas establecen salvaguardas contra estos riesgos.

## 3. Riesgos reputacionales para las empresas

**La confianza es fundamental para el desempeño de los servicios de seguridad y para el uso de la IA.** La UE publicó en 2019 las Directrices Éticas para el uso fiable de la IA, destacando que cada implementación debe ser jurídicamente sólida, ética y robusta para generar confianza<sup>16</sup>. Sin embargo, los datos de 2023 confirman que la confianza pública en la tecnología sigue siendo baja<sup>17</sup>.

En Europa, el interés público y mediático en la IA ha sido elevado en los últimos años debido también a varios incidentes (véase la página 23). A menudo, el foco recae sobre organizaciones que cometen errores. Si una empresa carece de transparencia sobre su uso de la IA, emplea personal sin formación adecuada para supervisarla y gestiona mal los riesgos, lo que lleva a incidentes, puede ser rápidamente señalada como poco ética e insensible con respecto a los trabajadores, clientes y ciudadanos. Como

ocurre con cualquier tecnología nueva, un solo incidente puede usarse para generalizar el riesgo potencial y poner en peligro o ralentizar su desarrollo posterior.

## 4. Riesgos de seguridad

**El uso de la IA en los servicios de seguridad conlleva riesgos, especialmente si los factores de riesgo no se abordan adecuadamente.** La ausencia de supervisión humana y la falta de resiliencia física y cibernética del sistema pueden dar lugar a un mal funcionamiento importante del sistema con repercusiones en la seguridad pública:

- ◆ El personal no adecuadamente cualificado podría no ser consciente de falsos negativos con importantes consecuencias, por ejemplo, en la seguridad aeroportuaria.
- ◆ Los actores malintencionados pueden manipular un sistema de IA físicamente o mediante ciberataques para provocar su mal funcionamiento y preparar una acción delictiva<sup>18</sup>.
- ◆ La inexactitud y el sesgo de los modelos de entrenamiento, así como la complejidad de los sistemas pueden dar lugar a afirmaciones incorrectas y resultados de la IA no deseados (fallos de interpretación<sup>19</sup>), conduciendo a consecuencias indeseables y socavando la confianza en el sistema<sup>20</sup>.
- ◆ La IA proporciona nuevas herramientas a actores malintencionados y puede ser utilizada para crear falsificaciones digitales<sup>21</sup> y ciberataques<sup>22</sup>. También podrían piratear los datos del sistema de IA, como datos biométricos, para llevar a cabo ciberataques de ingeniería social y eludir protocolos de seguridad.

## 5. Efectos secundarios

**El uso de sistemas de IA puede tener efectos secundarios, que pueden fácilmente pasarse por alto sin procedimientos de gestión de riesgos adecuados antes de su implementación.** Por ejemplo, el uso de sistemas de GPS inteligentes puede mejorar significativamente el flujo de tráfico en una ciudad, pero también puede llevar a un aumento indeseado de uso de carreteras secundarias en zonas residenciales. De manera similar, el análisis de riesgos de seguridad basado en datos puede mejorar significativamente la protección y seguridad de una instalación específica, pero también puede tener repercusiones en los precios de los alquileres y las primas de seguros en ciertos vecindarios.

<sup>13</sup> [https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_EN.html)

<sup>14</sup> Baiocco, S., et al. (2022), *La gestión algorítmica del trabajo y sus implicaciones en diversos contextos*, Comisión Europea, JRC129749.

<sup>15</sup> OCDE (2023), *Perspectivas del Empleo de la OCDE 2023: Inteligencia Artificial y el Mercado Laboral*, Publicaciones de la OCDE, París, <https://doi.org/10.1787/08785bba-en>.

<sup>16</sup> <https://digital-strategy.ec.europa.eu/es/library/ethics-guidelines-trustworthy-ai>

<sup>17</sup> [https://kpmg.com/xx/en/home/insights/2023/09/trust-in-artificial-intelligence.html#:~:text=AI%20trust%20and%20acceptance,depend%20on%20the%20AI%20application.&text=Three%20in%20five%20\(61%20percent,wary%20about%20trusting%20AI%20systems.&text=67%20percent%20report%20low%20to%20moderate%20acceptance%20of%20AI](https://kpmg.com/xx/en/home/insights/2023/09/trust-in-artificial-intelligence.html#:~:text=AI%20trust%20and%20acceptance,depend%20on%20the%20AI%20application.&text=Three%20in%20five%20(61%20percent,wary%20about%20trusting%20AI%20systems.&text=67%20percent%20report%20low%20to%20moderate%20acceptance%20of%20AI)

<sup>18</sup> <https://csrc.nist.gov/pubs/ai/100/2/e2023/final>

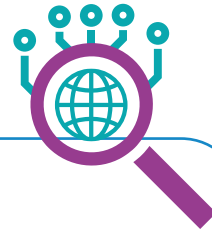
<sup>19</sup> Definición de “fallos de interpretación” en IA: Los fallos de interpretación de IA definen una situación en la que un sistema de IA genera resultados sin sentido, extraños e inexactos debido a modelado imperfecto del sistema o complejas interacciones en sistemas de aprendizaje profundo.

<sup>20</sup> <https://www.economist.com/science-and-technology/2024/02/28/ai-models-make-stuff-up-how-can-hallucinations-be-controlled>

<sup>21</sup> [https://www.dhs.gov/sites/default/files/publications/increasing\\_threats\\_of\\_deepfake\\_identities\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf)

<sup>22</sup> <https://www.wired.com/story/here-come-the-ai-worms/>

## CÓMO PODEMOS APRENDER DE INCIDENTES PASADOS Y RIESGOS EXISTENTES



### Clearview AI

En 2020, el *New York Times*<sup>23</sup> reveló que Clearview AI, una empresa estadounidense de software de reconocimiento facial, había recopilado más de 3 mil millones de imágenes faciales de redes sociales, incluidos datos adicionales como nombres de personas, y las almacenaba en una base de datos. El acceso a esta base de datos se vendió a fuerzas y cuerpos de seguridad, lo que les permitía identificar instantáneamente a una persona mediante una foto. Las Agencias de Protección de Datos (APD) expresaron importantes preocupaciones éticas y relacionadas con el RGPD sobre este modelo de negocio, y las APD en Francia y Alemania ordenaron a la empresa que cesara sus actividades y eliminara todos los datos personales<sup>24</sup>.

### El escándalo de las prestaciones por cuidado infantil en los Países Bajos

De 2013 a 2019, las autoridades fiscales neerlandesas utilizaron un algoritmo de autoaprendizaje para desarrollar perfiles de riesgo destinados a detectar fraudes en las prestaciones por cuidado infantil. Actuando según las recomendaciones del sistema, las autoridades penalizaron a familias incluso por mera sospecha de fraude. Como resultado, decenas de miles de familias, a menudo de bajos ingresos o pertenecientes a minorías étnicas, se vieron sumidas en la pobreza debido a deudas considerables con la autoridad fiscal. La APD de los Países Bajos señaló varias infracciones de las regulaciones de protección de datos de la UE e impuso una multa de 3,7 millones de euros a la autoridad fiscal<sup>25</sup>.

### Intervención física o ciberataques que manipulan el comportamiento de los sistemas de IA

Científicos informáticos del Instituto Nacional de Estándares y Tecnología de EE. UU. advierten que los sistemas de IA pueden fallar si un adversario encuentra una forma física o cibernética de manipular su toma de decisiones<sup>26</sup>. Los vehículos autónomos aprenden de capturas de calles dónde y cómo conducir, mientras que los asistentes virtuales analizan registros de conversaciones para predecir respuestas. Sin embargo, los datos de entrenamiento pueden ser alterados con datos corruptos. Actores malintencionados pueden llevar a cabo un ciberataque sobre sistemas de IA para acceder a información sensible con el fin de utilizarla de forma indebida. La información de entrada al sistema puede ser alterada físicamente para confundir o manipular el sistema.

### El escándalo de la Oficina de Correos del Reino Unido

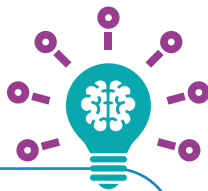
El sistema informático de la Oficina de Correos del Reino Unido, Horizon, acusó erróneamente a cientos de operadores de oficinas de correos de discrepancias financieras entre 2000 y 2014, que no fueron causadas por negligencia humana sino por fallos en el software informático. Más de 900 empleados fueron condenados por robo, fraude y contabilidad falsa, lo que llevó a personas inocentes a enfrentarse a acusaciones falsas y procesamientos. Numerosos empleados habían informado de la existencia de problemas con el software a la gerencia, e incluso el proveedor de software era consciente de los errores. No obstante, estas quejas no fueron atendidas por la Oficina de Correos del Reino Unido. Aunque Horizon no era un sistema de IA, este incidente ilustra la importancia de la supervisión humana, los datos cualitativos, los algoritmos de los sistemas, las políticas de gobernanza de la IA y los procesos de gestión de riesgos.

<sup>23</sup> <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>

<sup>24</sup> <https://www.law.kuleuven.be/citip/blog/clearview-ai-illegally-collecting-and-selling-our-faces-in-total-impunity-part-ii/>

<sup>25</sup> <https://www.politico.eu/article/dutch-scandal-erves-as-a-warning-for-europe-over-risks-of-using-algorithms/#:~:text=In%202019%20it%20was%20revealed,on%20the%20system's%20risk%20indicators.>

<sup>26</sup> <https://csrc.nist.gov/pubs/ai/100/2/e2023/final>



### LECCIONES QUE SE PUEDEN APRENDER

Los siguientes ejemplos muestran lo rápido que el uso de IA puede desviarse y convertirse en riesgos concretos. Por lo tanto, es importante abordar los factores de riesgo de forma holística desde el principio:

1. Los procesos de gestión de riesgos a lo largo del ciclo de vida de uso de un sistema de IA son clave para identificar y abordar riesgos específicos del caso de uso y garantizar el cumplimiento. Para el uso de la tecnología de Reconocimiento Facial Automatizado (FRT), la Asociación Británica de la Industria de Seguridad (BSIA) publicó una útil “Guía para el uso ético y legal del Reconocimiento Facial Automatizado”<sup>27</sup>.
2. El uso de sistemas de IA que se basan en datos y algoritmos fiables es fundamental para obtener resultados fiables y evitar violaciones de derechos fundamentales.
3. La supervisión humana cualitativa con personal adecuadamente capacitado es fundamental para asegurar que una persona siempre pueda evaluar la recomendación del sistema de IA y adoptar una decisión final e independiente.
4. Unos altos niveles de protección física y resiliencia cibernética a lo largo del ciclo de vida del sistema de IA son cruciales para proteger a los ciudadanos, usuarios y clientes del mal funcionamiento del sistema de IA.
5. La existencia de líneas jerárquicas, procesos y responsabilidades claros en el marco de una política de gobernanza de la IA es esencial para que los responsables de su implantación tomen medidas en caso de mal funcionamiento o uso indebido de un sistema de IA.

“La confianza es fundamental para el desempeño de los servicios de seguridad y el uso de la IA”



<sup>27</sup>[https://www.bsia.co.uk/zappfiles/bsia-front/public-guides/form\\_347\\_automated\\_facial%20recognition\\_a\\_guide\\_to\\_ethical\\_and\\_legal\\_use-compressed.pdf](https://www.bsia.co.uk/zappfiles/bsia-front/public-guides/form_347_automated_facial%20recognition_a_guide_to_ethical_and_legal_use-compressed.pdf)



# Capítulo III: Valores y Requisitos

## MISIÓN DE CoESS

Nuestra misión es apoyar el crecimiento de la industria de los servicios de seguridad mediante la promoción de soluciones de alta calidad y profesionalismo, basadas en la selección y desarrollo de personal capacitado y en la tecnología. Este objetivo se logra mediante la promoción de la capacitación cualitativa y las condiciones laborales de los trabajadores, el cumplimiento de las normativas y estándares de la industria, los más altos niveles de seguridad para trabajadores, clientes y ciudadanos, así como la confianza de los ciudadanos y las autoridades en la industria.

CoESS promueve la integración de sistemas de IA en los servicios de seguridad como parte de su misión. La integración de la IA no consiste solo en añadir tecnología a los conceptos de seguridad, sino en garantizar la complementariedad y optimización de las personas y la tecnología para alcanzar nuevos niveles de calidad y eficiencia en los servicios de seguridad.

El uso de soluciones de IA debe atenerse al principio de neutralidad tecnológica, buscando el mejor y más fiable rendimiento en materia de seguridad, ya sea mediante humanos o mediante una combinación de estos con IA.

**El uso de IA debe seguir un código de conducta basado en valores.** Este capítulo define dichos valores y ofrece una visión general de los principales requisitos para ayudar a los responsables del despliegue de la IA en los servicios de seguridad a cumplirlos, basándose en el Reglamento de IA de la UE, los Principios de IA de la OCDE<sup>28</sup> y las Directrices Éticas para una IA Fiable de la UE<sup>29</sup>.

## I. Los valores transversales de CoESS para el uso ético y responsable de la IA

CoESS define los siguientes ocho valores transversales e interdependientes para el uso ético y responsable de la IA en los servicios de seguridad:

### 1. Respeto de los Derechos Fundamentales:

La industria de los servicios de seguridad en Europa debe ser líder en el uso ético y responsable de la IA. Los responsables del despliegue de IA deben asegurar en todo momento el pleno respeto a la Carta de Derechos Fundamentales de la UE<sup>30</sup>.

### 2. Promoción de la Diversidad, la Igualdad, la Inclusión y la No Discriminación:

El uso de la IA por parte de los proveedores de servicios de seguridad debe fomentar la diversidad, la igualdad, la inclusión y la no discriminación<sup>31</sup>.

### 3. IA centrada en el ser humano:

El uso de sistemas de IA debe estar siempre supervisado por personal adecuadamente capacitado, proporcional al caso de uso. El uso de sistemas de IA en los servicios de seguridad debe fortalecer a los trabajadores, permitiéndoles tomar decisiones informadas basadas en nuevos

<sup>28</sup> <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

<sup>29</sup> <https://digital-strategy.ec.europa.eu/es/library/ethics-guidelines-trustworthy-ai>

<sup>30</sup> La Carta de los Derechos Fundamentales de la Unión Europea establece los derechos fundamentales protegidos en el ámbito de la UE. Abarca derechos civiles, políticos, económicos y sociales, incluyendo el derecho a la integridad de la persona, el derecho a la libertad y seguridad, la protección de los datos personales, el respeto de la vida privada y la libertad de movimiento, expresión e información. La Carta prohíbe la discriminación por motivos como raza, género, religión y orientación sexual. Garantiza derechos como condiciones laborales justas, el derecho de los trabajadores a la información, el derecho de negociación y acción colectiva, el derecho a una buena administración y a altos niveles de protección del consumidor. La Carta está disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12012P/TXT>

<sup>31</sup> De conformidad con la Carta de los Derechos Fundamentales de la UE y la Declaración Conjunta de los Socios Sociales Sectoriales de la UE sobre Diversidad, Igualdad, Inclusión y No Discriminación en los Servicios de Seguridad Privada, CoESS y UNI Europa (2024), disponible en: <https://coess.org/download.php?down=Li9kb2N1bWVudHMvdW5pLWV1cm9wYS1jb2Vzcy1qb2ludC1zdGF0ZW1bnQtZGl2ZXJzaXR5LWVxdWFsaXR5LWJ1e2x1c2lvbi1maW5hbC5wZGY>

conocimientos e información. La IA centrada en el ser humano también implica una mejor protección de las personas, promoviendo sus derechos fundamentales y principios relacionados con la no discriminación, la transparencia y la privacidad. Para CoESS, el uso de la IA centrada en el ser humano también significa que la IA debe convertirse en un bien público y servir a los ciudadanos europeos en todas las dimensiones.

**4. Transparencia y explicabilidad:** El uso de IA debe ser transparente para los interesados, según corresponda al caso de uso. La explicabilidad del funcionamiento y los resultados de los sistemas de IA es crucial, no solo para el uso ético y responsable de la IA, sino también para la comprensión y la confianza públicas.

**5. Privacidad de los datos:** La gobernanza de datos a lo largo de la cadena de valor del uso debe garantizar la protección de los derechos de privacidad de datos de los ciudadanos europeos, consagrados en la Carta de Derechos Fundamentales de la UE y el RGPD.

**6. Resiliencia física y cibernética y seguridad:** Los sistemas de IA y su uso en los servicios de seguridad deben ser seguros, resilientes y fiables para prevenir, soportar y superar incidentes. Los sistemas deben funcionar de manera repetible y predecible, y debe garantizarse un nivel constante de servicios de calidad durante todo el uso de los sistemas de IA. El daño material e inmaterial no intencionado a los trabajadores y partes interesadas afectadas debe minimizarse y prevenirse.

**7. Responsabilidad:** Toda la cadena de valor en el desarrollo y uso de sistemas de IA debe rendir cuentas del correcto funcionamiento de los sistemas de IA de acuerdo con sus roles y requisitos legales.

**8. Sostenibilidad:** El uso de la IA debe contribuir de manera holística a los Objetivos de Desarrollo Sostenible de las Naciones Unidas, promoviendo el crecimiento inclusivo, el desarrollo (medioambientalmente) sostenible y el bienestar. Debe garantizarse que las soluciones de IA sean sostenibles y respetuosas con el medio ambiente, considerando debidamente el impacto de las operaciones en el entorno.

## “El desarrollo de la IA debería regirse por un código de conducta basado en valores”

## II. Primeros pasos para asegurar un uso ético y responsable de la IA

El objetivo fundamental de esta Carta es proporcionar a los responsables del despliegue de sistemas de IA en los servicios de seguridad orientación sobre los requisitos legales y voluntarios para el uso ético y responsable de la IA, abordando los riesgos identificados en el Capítulo II y basándose en el conjunto de valores transversales de CoESS. Antes de decidir implantar un sistema de IA y de establecer las medidas adecuadas para garantizar su uso ético y responsable, el implantador debe seguir los siguientes tres pasos preparatorios con un planteamiento multilateral<sup>32</sup>:

### Paso 1: Identificar el sistema de IA

Como primer paso, el responsable del despliegue debe establecer si realmente está planeando utilizar un sistema de IA antes de adquirirlo. Aunque los sistemas de IA deberían estar etiquetados como tales por el proveedor, esto puede no ser siempre el caso, especialmente para los sistemas que se hayan comercializado antes de la aplicación del Reglamento de IA de la UE. Por lo tanto, el responsable del despliegue debe considerar examinar, con el proveedor, de forma interna y/o externa, la tecnología subyacente que se aplica en un determinado caso de uso. Basándose en la “Definición de IA” del Reglamento de IA de la UE (véase la página 8), es probable que el sistema esté clasificado como un sistema de IA si incorpora algoritmos de aprendizaje automático o modelos de aprendizaje profundo para generar resultados tales como predicciones, contenido, recomendaciones y decisiones basadas en la entrada de datos. Una revisión de nuestros criterios transversales (véase la página 10) puede ser útil.

### Paso 2: Evaluar los requisitos legales aplicables y determinar si el sistema de IA y el caso de uso son de bajo o alto riesgo según el Reglamento de IA de la UE

Antes de cada uso, el responsable del despliegue debe definir el propósito y el resultado esperado del uso del sistema de IA y llevar a cabo una evaluación para comprender si el sistema de IA y el caso de uso se califican como de bajo o alto riesgo. Esta evaluación es crucial para cumplir con el Reglamento de IA de la UE y utilizar la IA de manera responsable y ética. Debe comenzar con las siguientes preguntas:

<sup>32</sup> CoESS recomienda evaluar e implantar estos requisitos mediante un planteamiento multilateral, que incluya (entre otros) a los responsables de proyectos, gestores de asuntos regulatorios y expertos en cumplimiento, técnicos expertos en IA, responsables de protección de datos, personal de recursos humanos y expertos en seguridad tanto física como cibernética, así como gestores de unidades de negocio del segmento de servicios correspondiente. Estos equipos deben ser diversos, también para detectar posibles sesgos a lo largo de las operaciones de un sistema de IA. Las políticas y los códigos de conducta relacionados con la IA deben ser una prioridad para el consejo de administración de la empresa.



### 1. ¿Está prohibido el sistema de IA o el caso de uso según el Reglamento de IA de la UE (véase la página 12)?

### 2. ¿Se considera a mi empresa solo responsable del despliegue o también proveedora del sistema de IA?

Si el responsable del despliegue añade su nombre al sistema de IA o realiza modificaciones en el sistema o en su uso previsto, entonces se le consideraría un proveedor de sistemas de IA<sup>33</sup> según el Reglamento de IA de la UE, lo que le sometería a obligaciones legales adicionales en el caso de sistemas de IA de alto riesgo.

### 3. ¿Se considera el sistema de IA o el caso de uso como de alto riesgo? Nuestros criterios transversales pueden ayudar a realizar una primera evaluación. Para tener certeza legal, el responsable del despliegue debe verificar:

a. Si el sistema de IA en cuestión tiene el marcado CE y está registrado en una base de datos oficial y públicamente disponible de la UE (disponible a partir del 2 de agosto de 2026).

b. Si el caso de uso se encuentra dentro de alguna de las categorías de alto riesgo definidas en el Anexo III del Reglamento de IA de la UE (véase la página 13).

### 4. ¿Se combinan diferentes sistemas de IA en un solo caso de uso (por ejemplo, la instalación de sistemas de gestión de multitudes en un dron dotado de IA) y, en caso afirmativo, cuál es el impacto en la categorización de bajo o alto riesgo del caso de uso?

### 5. Si el sistema de IA o el caso de uso no consideran de alto riesgo, ¿interactúa el sistema en el caso de uso con personas físicas y por lo tanto conlleva riesgos de transparencia (véase la página 11)?

### Paso 3: Evaluar el valor añadido del uso del sistema de IA

Antes de utilizar el sistema de IA, el responsable del despliegue debe evaluar si la integración de la IA en el caso de uso específico aporta algún valor añadido, y establecer su propósito específico y los resultados que se pretenden. A continuación, el responsable del despliegue debe evaluar las posibles ventajas, desventajas y resultados no deseados de la integración de la IA en el servicio en cuestión, valorándolos en función del objetivo general de mejorar su calidad y efectividad. Esta evaluación debe considerar factores como la efectividad en el campo, el impacto en las condiciones laborales y la toma de decisiones, la cualificación de los trabajadores y la necesidad de mejorar sus habilidades, así como la rentabilidad.

### III. Requisitos para el uso ético y responsable de la IA

#### ADVERTENCIA

Este documento proporcionará a las empresas de seguridad un conocimiento inicial de la Ley de Inteligencia Artificial de la UE y de los códigos de conducta importantes antes y durante el uso de un sistema de IA. La información contenida en esta Carta no sustituye a las evaluaciones de riesgos y normativas específicas del sistema y de los casos de uso, que deben ser realizadas por el responsable del despliegue para garantizar el cumplimiento del Reglamento de IA de la UE.

Los actores de IA son responsables del funcionamiento adecuado de los sistemas de IA, en función de sus roles, el contexto y en coherencia con el estado de la técnica. Para asegurar el cumplimiento de nuestro conjunto de valores, de la UE y otras normativas pertinentes, esta Carta recomienda que los responsables del despliegue establezcan una política de gobernanza de la IA que asigne la responsabilidad legal y la obligación de rendir cuentas por el buen o mal uso de la IA a la Junta Directiva o al órgano de gobierno del responsable del despliegue. Además, el responsable del despliegue debe formular, en el marco de un planteamiento multilateral<sup>34</sup>, un código de conducta interno que establezca las siguientes medidas:

<sup>33</sup> Si el responsable del despliegue añade su nombre o marca comercial a un sistema de IA, realiza una modificación sustancial en él o cambia el propósito previsto del sistema de IA (en comparación con las instrucciones de uso del proveedor), podría considerarse que es además proveedor de un sistema de IA de alto riesgo según el Artículo 25 del Reglamento de IA de la UE y, por lo tanto, estaría obligado a cumplir con un rango mucho más amplio de obligaciones legales que las descritas en esta Carta.

<sup>34</sup> CoESS recomienda evaluar e implantar estos requisitos mediante un planteamiento multilateral, que incluya (entre otros) a los responsables de proyectos, gestores de asuntos regulatorios y expertos en cumplimiento, técnicos expertos en IA, responsables de protección de datos, personal de recursos humanos y expertos en seguridad tanto física como cibernética, así como gestores de unidades de negocio del segmento de servicios correspondiente. Estos equipos deben ser diversos, también para detectar posibles sesgos a lo largo de las operaciones de un sistema de IA. Las políticas y los códigos de conducta relacionados con la IA deben ser una prioridad para el consejo de administración de la empresa.



## GESTIÓN DE RIESGOS

Los sistemas de gestión de riesgos son una obligación legal para la IA de alto riesgo según el Artículo 9 del Reglamento de IA de la UE

**Los riesgos asociados al uso de un sistema de IA deben gestionarse adecuadamente durante todo su ciclo de vida y de acuerdo con su finalidad prevista y contexto de uso.** Para ello, el responsable del despliegue debe establecer un sistema de gestión de riesgos para:

- asegurar el cumplimiento de la normativa vigente, incluyendo el RGPD y el Reglamento de IA de la UE.
- identificar y analizar los riesgos conocidos, los razonablemente previsibles y otros posibles riesgos que el sistema de IA pueda plantear para la salud, la seguridad o los derechos fundamentales de los ciudadanos de la UE y los trabajadores, así como para la seguridad de los clientes cuando se utilice de acuerdo con su finalidad prevista, pero también bajo condiciones de uso indebido razonablemente previsibles;
- adoptar medidas de gestión de riesgos apropiadas y específicas, técnica y físicamente viables, diseñadas para minimizar los riesgos identificados a un nivel razonablemente aceptable;
- establecer procedimientos de contingencia y otras medidas adecuadas de mitigación y control para abordar riesgos que no se puedan eliminar.

Estas medidas deben considerar todos los requisitos enumerados en esta Carta y abordar adecuadamente los factores y categorías de riesgo establecidos en el Capítulo II. Existen muchas Normas<sup>35</sup> y Directrices<sup>36</sup> internacionales que pueden ayudar a los operadores a llevar a cabo procesos de gestión de riesgos.



## GOBERNANZA DE DATOS

La gobernanza de datos es una obligación legal para la IA de alto riesgo según los Artículos 10 y 26 del Reglamento de IA de la UE

**Los responsables del despliegue deben implantar prácticas diligentes de tratamiento de datos:**

- La gobernanza de datos debe garantizar el pleno cumplimiento del RGPD.

- Debe asegurarse la adecuada seguridad cibernética y física de los conjuntos de datos, incluidos los datos personales y sensibles, así como de los centros de datos pertinentes.

- El uso de IA en los servicios de seguridad debe basarse en datos fiables, sólidos y de calidad. Con este fin, las políticas y procedimientos de diligencia debida en la selección de sistemas de IA deben garantizar que los proveedores hayan entrenado, validado y probado el sistema de IA con datos de entrada que cumplan ciertos criterios de calidad y excluyan posibles sesgos, conforme al Reglamento de IA de la UE. En la medida en que el responsable del despliegue ejerza control sobre los datos de entrada, deberá asegurarse de que sean relevantes en función de la finalidad prevista del sistema de IA de alto riesgo.

La gobernanza de datos también debe garantizar la trazabilidad del procesamiento de datos, la explicabilidad del resultado del sistema de IA, la auditabilidad y la rendición de cuentas.



## SUPERVISIÓN HUMANA

Muchas medidas relacionadas con la supervisión humana constituyen una obligación legal para los responsables del despliegue de sistemas de IA de alto riesgo según los Artículos 4, 14 y 26 del Reglamento de IA de la UE

**La supervisión humana adecuada de cualquier sistema de IA es esencial para el cumplimiento de los valores establecidos en esta Carta.** El Reglamento de IA de la UE también prevé en su Artículo 4 que, a partir del 2 de febrero de 2025, los responsables del despliegue de sistemas de IA deberán tomar medidas para garantizar, en la medida de lo posible, un nivel adecuado de alfabetización en IA de su personal. Para los servicios de seguridad europeos, CoESS subraya que el personal responsable debe estar capacitado para cumplir con los requisitos establecidos



<sup>35</sup> Como la ISO/IEC 23894 "Inteligencia Artificial: Directrices para la Gestión de Riesgos" y la ISO/IEC 42001 "Sistema de Gestión de la Inteligencia Artificial".

<sup>36</sup> Estos recursos incluyen la Lista de Autoevaluación de la UE para una IA fiable disponible en <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-ai-self-assessment>, el Portafolio del Reino Unido de técnicas de seguridad de IA, que incluye el sistema de inteligencia de riesgos Anekanta AI para IA biométrica y de alto riesgo, disponible en <https://www.gov.uk/ai-assurance-techniques>; y el Marco de Gestión de Riesgos de IA del Instituto Nacional de Estándares y Tecnología de los EE. UU., disponible en <https://www.nist.gov/itl/ai-risk-management-framework>.



en esta Carta, **de manera adecuada y proporcional al caso de uso específico.**

El responsable del despliegue deberá tomar medidas técnicas y organizativas adecuadas para asegurarse de que utiliza los sistemas de IA conforme a las instrucciones de uso que acompañan a estos. Además, el responsable del despliegue deberá garantizar que el personal encargado de la supervisión de los sistemas de IA esté capacitado mediante una formación adecuada, medidas técnicas y operativas, y delegación de autoridad, para:

- comprender las instrucciones de uso, la finalidad prevista y el caso de uso de un sistema de IA, y las conclusiones extraídas de la gestión de riesgos;
- conocer las capacidades y limitaciones relevantes del sistema de IA;
- estar al tanto del nivel de precisión, solidez y ciberseguridad del sistema de IA, incluyendo cualquier circunstancia conocida y previsible que pueda afectar a su precisión, solidez y ciberseguridad;
- conocer las condiciones de uso indebido previsible, que pueden dar lugar a riesgos para la salud y la seguridad o para los derechos fundamentales de las personas afectadas debido a los resultados del sistema;
- ser capaz de explicar a las personas afectadas la finalidad prevista de la recopilación de datos y proporcionar información sobre cómo se ha alcanzado el resultado de la IA;
- conocer los cambios en el sistema de IA que puedan influir en su funcionamiento<sup>37</sup>;
- ser capaz de monitorizar debidamente el funcionamiento del sistema de IA, incluyendo la detección y gestión de anomalías, disfunciones y resultados inesperados;
- ser consciente de la posible tendencia a depender o confiar automáticamente en los resultados generados por un sistema de IA;

- interpretar correctamente los resultados de un sistema de IA de alto riesgo y tomar decisiones de manera autónoma;
- decidir, en cualquier situación particular, no utilizar el sistema de IA o, en otro caso, desestimar, anular o revertir su resultado;
- intervenir en la operación del sistema de IA y establecer procedimientos de emergencia pertinentes, así como otras medidas adecuadas de mitigación y control en caso de un incidente;
- informar al proveedor y a las autoridades pertinentes en caso de un incidente.

En el caso de usos de IA de alto riesgo, el Artículo 14 del Reglamento de IA de la UE exige que los responsables del despliegue establezcan políticas, procesos y procedimientos diligentes para garantizar el cumplimiento de la ley. Existen disposiciones especiales de supervisión humana para los casos de uso de identificación biométrica<sup>38</sup>.

Los responsables del despliegue deben tener en cuenta la posible necesidad de mejorar las competencias del personal antes del uso de la IA. La industria de la seguridad debe trabajar en estrecha colaboración con las autoridades para prepararse para la integración de los sistemas de IA en los servicios y, si es necesario, adaptar marcos de formación que reflejen los requisitos de alfabetización en IA, habilidades y cualificación, así como los requisitos de autorización administrativa. El Diálogo Social puede desempeñar un papel importante para liderar este proceso y garantizar el uso responsable de la IA en el lugar de trabajo, en beneficio de la salud y seguridad laboral y la calidad del empleo.

**“El Diálogo Social puede desempeñar un papel importante para garantizar el uso responsable de la IA en los puestos de trabajo”**

<sup>37</sup> Las personas capacitadas en supervisión humana también pueden reducir el riesgo de decisiones sesgadas que surjan de sistemas de IA previamente no sesgados, pero que hayan desarrollado sesgos durante su uso. Según sea apropiado para el caso de uso, los trabajadores deben recibir formación para que el despliegue de la IA se ajuste a los valores centrados en las personas durante toda su operación.

<sup>38</sup> En el caso de usos relacionados con la identificación biométrica, el Artículo 14.5 del Reglamento de IA de la UE establece que el responsable del despliegue no debe actuar ni tomar ninguna decisión basándose en el resultado del sistema, a menos que este haya sido verificado y confirmado por separado por al menos dos personas físicas con la competencia, formación y autoridad necesarias. Existen excepciones a esta disposición para casos de uso que cumplan fines de aplicación de la ley.



## RESILIENCIA

Las medidas relacionadas con la precisión, solidez y ciberseguridad de los sistemas de IA constituyen una obligación legal de los responsables del despliegue de IA de alto riesgo, conforme al Artículo 15 del Reglamento de IA de la UE

**En línea con el Reglamento de IA de la UE y otras normas pertinentes, como el Reglamento de Resiliencia Cibernética de la UE, el proveedor del sistema de IA tiene la responsabilidad de diseñar y desarrollar sus productos de manera que garantice adecuadamente su precisión, resiliencia y ciberseguridad.**

No obstante, los responsables del despliegue también deberán adoptar las medidas técnicas, operativas y organizativas necesarias para responder a los riesgos físicos y de ciberseguridad pertinentes, de acuerdo con una evaluación de riesgos previa, la finalidad prevista y el entorno del caso de uso. Los sistemas de IA deben ser sólidos, seguros y fiables a lo largo de todo su ciclo de vida, de modo que, en condiciones de uso normal, uso previsible o uso indebido, u otras condiciones adversas, funcionen de manera adecuada, repetible y predecible, sin plantear riesgos de seguridad excesivos. Por lo tanto, es importante que los riesgos físicos y cibernéticos se aborden de manera holística<sup>39</sup>.

- La manipulación física de los sistemas de IA puede dar lugar a resultados erróneos y, en consecuencia, a riesgos significativos para la seguridad y protección. Las medidas de protección física pueden incluir el control y monitoreo de acceso al hardware físico de IA, a la infraestructura y al almacenamiento de datos; el mantenimiento de condiciones ambientales óptimas para el funcionamiento de los sistemas de IA; y la implantación de procedimientos seguros para la eliminación de sistemas de IA. El personal debe estar adecuadamente capacitado para la puesta en práctica de estas medidas. Además, se debe prestar especial atención a la seguridad y resiliencia de los centros de datos.

- Los ciberataques al sistema de IA durante su operación pueden “envenenar” el conjunto de datos de entrenamiento o los modelos, o presentar importantes riesgos de privacidad y protección de datos. Existen normas<sup>40</sup> y directrices<sup>41</sup> en el ámbito de la resiliencia cibernética que pueden ser útiles para los responsables del despliegue de sistemas de IA.

Especialmente en el sector de los servicios de seguridad, **la resiliencia física y cibernética ejemplar de los sistemas de IA es crucial para evitar incidentes y proteger la reputación del responsable del despliegue.** Para superar incidentes y garantizar la continuidad del negocio, los responsables del despliegue deberán establecer procedimientos de emergencia y planes de contingencia. Los profesionales de seguridad pueden necesitar sustituir la operación del sistema de IA en el caso de uso respectivo. Los datos pueden almacenarse en ubicaciones geográficamente dispersas para minimizar el impacto de las perturbaciones físicas localizadas y los ciberataques.



## REGISTRO DE ACTIVIDADES

El registro de actividades es una obligación legal para la IA de alto riesgo según los Artículos 12 y 26 del Reglamento de IA de la UE

**El registro automático de actividades es, conforme a el Reglamento de IA de la UE, una característica técnica obligatoria de los sistemas de IA de alto riesgo y de los responsables de su despliegue, en la medida en que esté bajo el control de estos últimos.** Es importante que los responsables del despliegue garanticen el respeto de los valores relacionados con la trazabilidad, explicabilidad y rendición de cuentas. En proporción a la finalidad prevista del sistema, la documentación del rendimiento operativo de los sistemas de IA garantiza que el responsable del despliegue pueda rastrear, explicar y justificar cómo se toman las decisiones. La obligación de rendir cuentas exige registros claros para establecer quién es responsable de las operaciones de IA (y de sus posibles modificaciones), garantizando la transparencia y el cumplimiento (voluntario) de los requisitos normativos.

<sup>39</sup> Para obtener más información, consulte el Libro Blanco de CoESS y la International Security Ligue titulado “Seguridad ciber-física e Infraestructuras Críticas”, disponible en <https://www.coess.eu/>.

<sup>40</sup> La norma ISO/IEC CD 27090, titulada “Ciberseguridad – Inteligencia Artificial – Directrices para abordar las amenazas de seguridad a los sistemas de inteligencia artificial”, aborda los riesgos de ciberseguridad asociados a los sistemas de IA.

<sup>41</sup> El Centro Común de Investigación de la Unión Europea ha publicado los “Principios rectores para abordar los requisitos de ciberseguridad en sistemas de IA de alto riesgo”, disponibles en español en <https://op.europa.eu/es/publication-detail/-/publication/7d0a4007-51dd-11ee-9220-01aa75ed71a1/language-es>.

Además, CoESS y Euralarm han elaborado las “Directrices de ciberseguridad para la industria de la seguridad”, que ofrecen orientaciones más generales y están disponibles en <https://www.coess.eu/>.



El Reglamento de IA de la UE prevé un período de conservación de los registros de al menos seis meses cuando se usan sistemas de IA de alto riesgo y establece obligaciones adicionales cuando se usen sistemas de identificación biométrica remota.



#### TRANSPARENCIA Y EXPLICABILIDAD

Existen diversas medidas de transparencia que constituyen una obligación legal para la IA de alto riesgo y de riesgo limitado según los Artículos 13, 26, 49, 50 y 71 del Reglamento de IA de la UE

**El cumplimiento del RGPD es un aspecto clave del uso ético y responsable de la IA.** Pero hay más: los responsables del despliegue de IA deberán comprometerse a la transparencia, la explicabilidad y la divulgación responsable en lo que respecta a los sistemas de IA.

- **Transparencia hacia las personas expuestas al sistema de IA:** Las personas deben ser siempre conscientes de que están interactuando con un sistema de IA y/o de que están sujetas a sus resultados de una manera que sea legal y proporcional al caso de uso específico. La información sobre transparencia debe ser significativa, adecuada al contexto, coherente con el estado de la técnica y accesible para personas con discapacidad. Las personas afectadas deben tener la capacidad de comprender y, si es necesario, cuestionar el resultado y las decisiones relacionadas con este. Los representantes de los trabajadores deben ser informados sobre el uso de sistemas de IA en la gestión de empleados. Según el caso de uso y el sistema de IA, el responsable del despliegue debe establecer mecanismos de queja transparentes y accesibles que respeten los derechos específicos y prever soluciones para las personas afectadas de manera ilícita por los sistemas de IA.
- **Transparencia hacia el público en general:** Cuando se utilizan sistemas de IA de alto riesgo en nombre de autoridades, el responsable del despliegue debe registrarlo en una base de datos pública accesible de la UE<sup>42</sup>, conforme a los Artículos 49 y 71 del Reglamento de IA de la UE. Para aumentar la transparencia y la confianza pública en el uso de la IA en los servicios de seguridad, y si se considera adecuado y seguro en el caso de uso específico, los responsables del despliegue pueden registrar voluntariamente cualquier uso de IA de alto riesgo, incluso si no lo están utilizando en nombre de una autoridad.
- **Transparencia hacia las autoridades:** Los responsables del despliegue deben poner la documentación de IA a disposición de las autoridades competentes para su inspección y para garantizar

el cumplimiento de los requisitos legales. Los responsables del despliegue de sistemas de identificación biométrica remota deben presentar informes anuales a las autoridades de vigilancia del mercado y de protección de datos pertinentes.

- **Explicabilidad:** Es fundamental que los responsables del despliegue estén en condiciones de explicar la finalidad prevista de la recopilación de datos a las personas afectadas y de proporcionar información clara y sencilla sobre cómo se alcanzaron las decisiones de la IA, en proporción al caso de uso y respetando la propiedad intelectual, la privacidad y la seguridad. Con este fin, los responsables del despliegue, si es necesario, deberán solicitar al desarrollador que proporcione tarjetas de modelo u orientación legible por humanos sobre cómo toma decisiones el sistema de IA.

**Los responsables del despliegue deben promover la comprensión entre el público y los legisladores sobre el uso de la IA en los servicios de seguridad.** Esto se puede lograr promoviendo esta Carta.



#### EVALUACIÓN DEL IMPACTO SOBRE LOS DERECHOS FUNDAMENTALES

Las Evaluaciones del Impacto sobre los Derechos Fundamentales constituyen una obligación legal para los responsables del despliegue de IA de alto riesgo según el Artículo 27 del Reglamento de IA de la UE

**Además de la evaluación de impacto de protección de datos obligatoria según el artículo 25 del RGPD, los responsables del despliegue de IA de alto riesgo que sean autoridades públicas o que presten servicios en nombre de autoridades públicas deben realizar una Evaluación del Impacto sobre los Derechos Fundamentales** conforme al Artículo 27 del Reglamento de IA de la UE antes de usar un sistema de IA de alto riesgo por primera vez. Dicha evaluación debe cubrir:

- una descripción de los procesos del responsable del despliegue en los cuales se utilizará el sistema de IA de alto riesgo en línea con su finalidad prevista;
- una descripción del período y la frecuencia de uso previstos del sistema de IA de alto riesgo;
- las categorías de personas que probablemente se verán afectadas por su uso en el contexto específico;
- los riesgos específicos de daño que probablemente tengan repercusiones sobre las personas afectadas;

<sup>42</sup> Esta base de datos de la UE está regulada según el Artículo 71 del Reglamento de IA de la UE. La información que debe ser introducida por los responsables del despliegue de sistemas de IA se detalla en el Anexo VIII. La base de datos será establecida y gestionada por la Comisión Europea en el transcurso de 2026.

- una descripción de las medidas de supervisión humana conforme a las instrucciones de uso;
- medidas de gestión de riesgos, incluidas gobernanza interna y mecanismos de queja.

Los responsables del despliegue de sistemas de IA de alto riesgo que presten servicios en nombre de autoridades públicas deben notificar a las autoridades nacionales el resultado de esta evaluación y repetirla si consideran que alguno de estos elementos no está actualizado durante el uso. Los responsables del despliegue que no desplieguen sistemas de IA de alto riesgo en nombre de autoridades públicas también deberían considerar realizar dicha evaluación si tienen razones para creer que su caso de uso podría tener impacto sobre derechos fundamentales, aunque sean improbable. La Oficina Europea de IA puede desarrollar directrices para ayudar a los responsables del despliegue a cumplir con sus obligaciones legales.

Según el caso de uso, los responsables del despliegue pueden consultar a grupos de partes interesadas afectadas sobre tales Evaluaciones del Impacto sobre los Derechos Fundamentales.



#### DILIGENCIA DEBIDA

**Los responsables del despliegue de sistemas de IA deben adoptar políticas de diligencia debida al adquirir sistemas de IA:**

- verificar que el sistema de IA se haya entrenado con conjuntos de datos de alta calidad, diversos y representativos;
- confirmar la conformidad del sistema de IA con los requisitos de ciberseguridad pertinentes, al menos aquellos establecidos en la normativa aplicable, como el Reglamento de IA de la UE y la Ley de Resiliencia Cibernética de la UE;
- utilizar únicamente sistemas de IA que sean transparentes en sus procesos de toma de decisiones e incluyan instrucciones de uso adecuadas<sup>43</sup> que permitan, entre otras cosas, una comprensión fácil de las finalidades previstas del sistema y de las medidas necesarias de supervisión humana; el nivel de precisión, incluyendo sus métricas, solidez y ciberseguridad; así como las circunstancias y usos indebidos previsibles que puedan conducir a riesgos para los derechos fundamentales.

Los proveedores de sistemas de IA de alto riesgo deben registrar sus productos en la base de datos de la UE mencionada en el Artículo 71 del Reglamento de IA de la UE. Los responsables del despliegue solo deben utilizar sistemas de alto riesgo que hayan sido debidamente registrados.



#### INVOLUCRAR A LOS TRABAJADORES EN LA INTEGRACIÓN DE LA IA EN LOS SERVICIOS

**Además de las obligaciones legales de informar a los trabajadores sobre el uso de IA en el lugar de trabajo, el responsable del despliegue debe involucrar activamente a los profesionales de seguridad en el uso de sistemas de IA en los servicios.**

Esto podría incluir actividades de sensibilización, como seminarios, retransmisiones por internet y otro material informativo, para proporcionar transparencia sobre qué sistemas de IA se utilizan y por qué y cómo se pretende utilizarlos. Como parte de las medidas de supervisión humana y en función de cada caso de uso, los trabajadores deben recibir información adecuada sobre lo que se puede y no se puede esperar del sistema, para evitar abrumarlos y fomentar la confianza en la tecnología. Los beneficios del análisis de riesgos con IA deben alcanzar a cada empleado, por ejemplo, compartiendo estadísticas y recomendaciones sobre salud y seguridad operativas.

Los responsables del despliegue pueden establecer puntos de contacto específicos donde los trabajadores puedan plantear preocupaciones éticas sobre el funcionamiento y el uso de ciertos sistemas de IA, protegidos según la legislación laboral pertinente y, posiblemente, a través de un comité de ética o revisión interna.



#### EN CASO DE DUDA: CONTACTE CON LAS AUTORIDADES COMPETENTES

**Los códigos de conducta internos y las políticas de IA deben prever que los responsables del despliegue trabajen activamente con las autoridades competentes en caso de dudas sobre la certeza legal y los requisitos establecidos en esta Carta.** Además, si el responsable del despliegue tiene razones para considerar que el uso de los sistemas de IA puede presentar algún riesgo material o inmaterial para las personas afectadas, deberá informar al proveedor del sistema y a la autoridad de vigilancia del mercado correspondiente, y suspender el despliegue del sistema. En caso de incidente con un sistema de IA de alto riesgo, se debe informar a las autoridades competentes.

**“La Carta Europea aconseja que los responsables del despliegue desarrollen una política de gobernanza de la IA”**

<sup>43</sup> Para sistemas de IA de alto riesgo que cumplan con las disposiciones del Reglamento de IA de la UE según el Artículo 13.

## Capítulo IV: Lista de comprobación

El Reglamento de IA de la UE comenzará a aplicarse de forma escalonada y la mayoría de sus disposiciones tendrán efecto a partir del 2 de agosto de 2026. Sin embargo, gran parte de la implantación y el cumplimiento del Reglamento de IA de la UE depende de las Directrices que publique la Oficina Europea de IA de la Comisión Europea, de las Normas que ha de desarrollar CEN/CENELEC y del marco de aplicación que establezcan las autoridades nacionales.

Si ya está utilizando sistemas de IA en sus servicios o planea hacerlo, hay formas de adelantarse a estos requisitos y utilizar esta Carta para establecer marcos de gobernanza de la IA que garanticen el uso ético y responsable de la IA en sus servicios.

Aquí dispone de una lista de comprobación que puede ayudarle:

- #1 **Establezca un equipo interno de gobernanza y liderazgo en IA**, con procesos y responsabilidades en el marco de un planteamiento multilateral. 
- #2 **Identifique los posibles sistemas de IA en cuestión**, así como su uso y finalidad prevista en su oferta de servicios. 
- #3 **Conozca los marcos legales y las normas aplicables a su caso de uso** y confirme los plazos de cumplimiento. 
- #4 **Evalúe el posible perfil de riesgo de su sistema de IA y el caso de uso**, las obligaciones legales respectivas y el valor añadido de usar el sistema de IA en el caso de uso específico. 
- #5 **Involucre a sus autoridades nacionales y/o expertos legales** y confirme su evaluación interna. 
- #6 **Inspírese en esta Carta y construya un código de conducta interno.** 
- #7 **Adquiera su sistema de IA siguiendo un planteamiento de diligencia debida** y capacite a su equipo de liderazgo en IA. 
- #8 **Realice una evaluación de riesgos y establezca un proceso de gestión de riesgos para cada caso de uso individual.** 
- #9 **Prepare medidas adecuadas para cada caso de uso individual** conforme a los valores y requisitos establecidos en esta Carta, y capacite a su personal en consecuencia si es necesario. 
- #10 **Revise continuamente su gobernanza de la IA, monitoree el entorno regulatorio y los incidentes relacionados con IA de alto riesgo** e involúcrese con la Oficina Europea de IA, los organismos reguladores de su país, los organismos de normalización, las asociaciones de la industria y la comunidad de IA para mantenerse informado sobre las últimas tendencias, directrices, normas y novedades legales. 

# Anexo: Repositorio de directrices y normas útiles

## → Textos legales de la UE:

- ♦ Texto legal del Reglamento de IA de la UE: Reglamento (UE) 2024/1689:  
<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32024R1689>

## → Orientaciones de la UE:

- ♦ Siga a la Oficina Europea de IA:  
<https://digital-strategy.ec.europa.eu/en/policies/ai-office>
- ♦ Siga el Pacto de IA de la UE:  
<https://digital-strategy.ec.europa.eu/en/policies/ai-pact>
- ♦ Siga a la Alianza Europea de IA:  
<https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance>
- ♦ Directrices de la UE sobre IA fiable:  
<https://digital-strategy.ec.europa.eu/es/library/ethics-guidelines-trustworthy-ai>
- ♦ Centro Común de Investigación de la UE: “Principios rectores para abordar los requisitos de ciberseguridad para sistemas de IA de alto riesgo”:  
<https://op.europa.eu/es/publication-detail/-/publication/7d0a4007-51dd-11ee-9220-01aa75ed71a1/language-es>
- ♦ Lista de autoevaluación de la UE para IA fiable:  
<https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>

## → Orientaciones internacionales:

- ♦ Definición de un sistema de IA por la OCDE:  
<https://oecd.ai/en/wonk/ai-system-definition-update>
- ♦ Centro de Recursos de IA de la Asociación Internacional de Profesionales de la Privacidad (IAPP):  
<https://iapp.org/>
- ♦ Portafolio del Reino Unido de técnicas de seguridad de IA:  
<https://www.gov.uk/ai-assurance-techniques>
- ♦ Marco de Gestión de Riesgos de IA del Instituto Nacional de Estándares y Tecnología de EE. UU.:  
<https://www.nist.gov/itl/ai-risk-management-framework>

## → Orientaciones para la industria de la seguridad:

- ♦ Asociación Británica de la Industria de la Seguridad (BSIA): Reconocimiento Facial Automatizado – Guía para un uso ético y legal:  
[https://www.bsia.co.uk/zappfiles/bsia-front/public-guides/form\\_347\\_automated\\_facial%20recognition\\_a\\_guide\\_to\\_ethical\\_and\\_legal\\_use-compressed.pdf](https://www.bsia.co.uk/zappfiles/bsia-front/public-guides/form_347_automated_facial%20recognition_a_guide_to_ethical_and_legal_use-compressed.pdf)
- ♦ CoESS & Euralarm: Directrices de ciberseguridad para la industria de la seguridad:  
<https://www.coess.eu>



→ **Normas europeas:**

- ◆ Siga al Comité Técnico Conjunto 21 de CEN-CENELEC sobre “Inteligencia Artificial” :  
<https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/>

→ **Normas internacionales:**

- ◆ ISO/IEC 5339:2024 “Tecnología de la información – Inteligencia artificial – Directrices para aplicaciones de IA”:  
<https://www.iso.org/standard/81120.html>
- ◆ ISO/IEC TS 8200:2024 “Tecnología de la información – Inteligencia artificial – Controlabilidad de sistemas de inteligencia artificial automatizados”:  
<https://www.iso.org/standard/83012.html>
- ◆ ISO/IEC 22989:2022 “Tecnología de la información – Inteligencia artificial – Conceptos y terminología de inteligencia artificial”:  
<https://www.iso.org/standard/74296.html>
- ◆ ISO/IEC 23894 “Inteligencia Artificial – Directrices sobre Gestión de Riesgos”:  
<https://www.iso.org/standard/77304.html>
- ◆ ISO/IEC TR 24028:2020 “Tecnología de la información – Inteligencia artificial – Visión general de la fiabilidad en inteligencia artificial” :  
<https://www.iso.org/standard/77608.html>
- ◆ ISO/IEC TR 24030:2024 “Tecnología de la información – Inteligencia artificial – Casos de uso”:  
<https://www.iso.org/standard/84144.html>
- ◆ ISO/IEC TR 24368:2022 “Tecnología de la información – Inteligencia artificial – Visión general de preocupaciones éticas y sociales”:  
<https://www.iso.org/standard/78507.html>
- ◆ ISO/IEC TR 27563:2023 “Seguridad y privacidad en casos de uso de inteligencia artificial – Mejores prácticas”:  
<https://www.iso.org/standard/80396.html>
- ◆ ISO 30434:2023 “Gestión de recursos humanos – Asignación de la fuerza laboral”:  
<https://www.iso.org/standard/68711.html>
- ◆ ISO/IEC 38507:2022 “Tecnología de la información – Gobernanza de TI – Implicaciones de gobernanza del uso de la inteligencia artificial por las organizaciones”:  
<https://www.iso.org/standard/56641.html>
- ◆ ISO/IEC 42001 “Sistema de Gestión de Inteligencia Artificial”:  
<https://www.iso.org/standard/81230.html>



Actuando como la voz de la industria de la **seguridad**

Confederation of European Security Services

**Los servicios de seguridad privada en Europa ofrecen una amplia gama de servicios esenciales, tanto para clientes privados como públicos, que abarcan desde instalaciones de infraestructuras críticas hasta espacios públicos y cadenas de suministro.**

**coess.eu**

**Confederation of European Security Services**

Avenue des Arts 56

B-1000 Brussels

Belgium