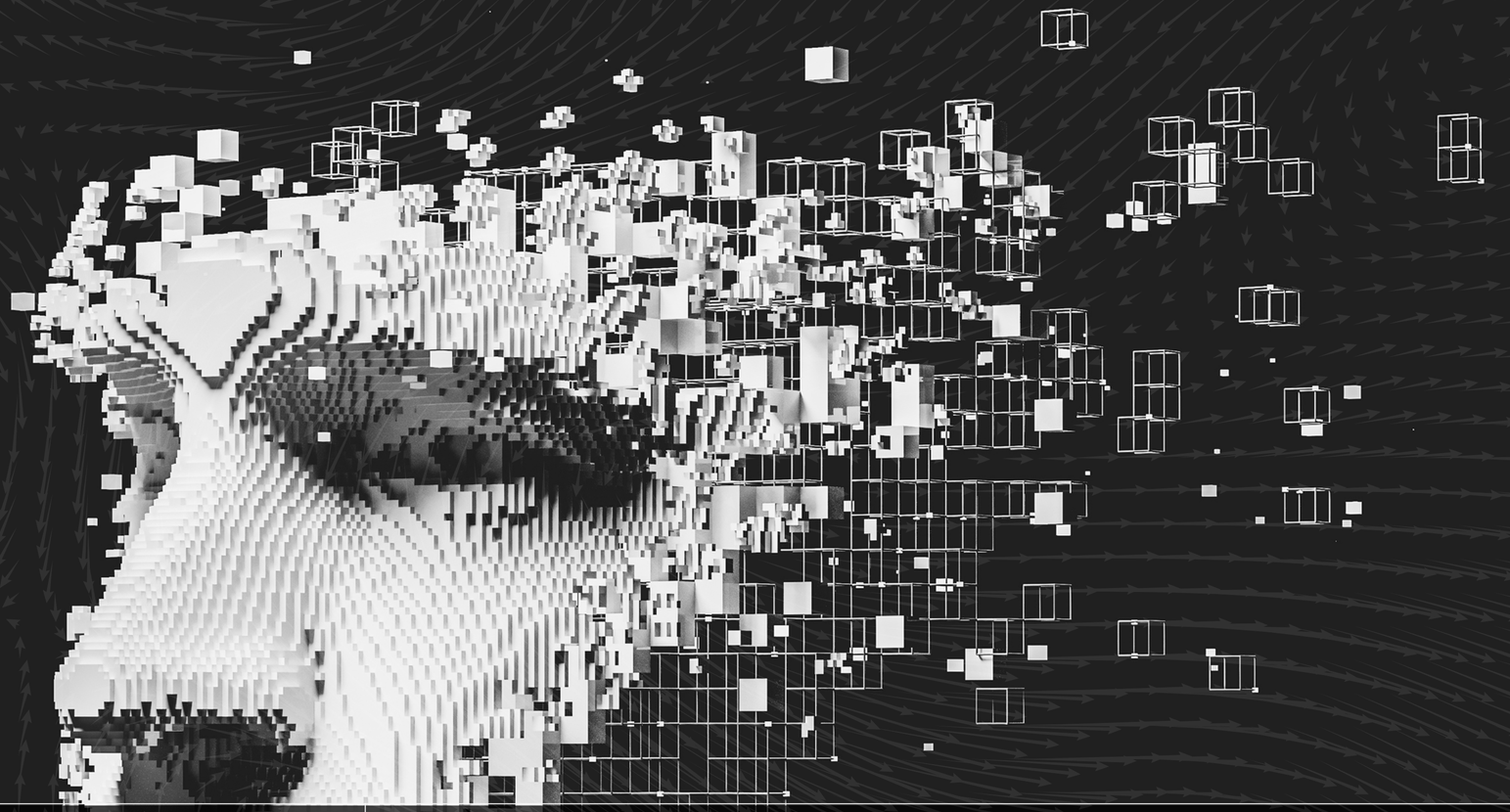
FUNDACIÓN ESYS



S E M I N A R I O

UNA **ESTRATEGIA NACIONAL** DE **INTELIGENCIA ARTIFICIAL** QUE INCORPORE **ELEMENTOS CLAVE** DE **SEGURIDAD**

SEMINARIO FUNDACIÓN ESYS

24 SEPTIEMBRE 2020

Í N D I C E


ESTRATEGIA ESPAÑOLA
EN
INTELIGENCIA ARTIFICIAL

IA

La **Inteligencia Artificial (IA)** es una **nueva forma de analizar, trabajar, comunicarse**, que va a **transformar** (ya lo está haciendo) la **economía y la sociedad** como parte del **proceso de transición digital** en que están inmersos **todos los países**.

Desde el punto de vista económico, la **Inteligencia Artificial** se está convirtiendo en un **elemento decisivo para la competitividad** de las empresas. Su aprovechamiento e incorporación en las cadenas de valor de los diferentes sectores económicos, y en los diferentes procesos de las compañías **va a condicionar la capacidad de las empresas para competir en los mercados globales**. La **maduración acelerada y simultánea** de varias tecnologías está generado un **cambio disruptivo** que es necesario gestionar.

Entre estas tecnologías podemos mencionar la **Inteligencia Artificial**, el **acceso y análisis de datos**, los **sensores biónicos**, la **robótica**, las **comunicaciones inalámbricas de banda ancha** y la **supercomputación**. La **Inteligencia Artificial** es sin duda una de las **tecnologías con mayor capacidad de disrupción**. Son varios los factores habilitadores que podemos identificar como causantes de la emergencia de la disrupción tecnológica asociada a la **Inteligencia Artificial**:

COMPUTACIÓN UBICUA DE ALTAS PRESTACIONES

ALGORITMOS DE APRENDIZAJE (REDES NEURONALES)

PROCESAMIENTO DE GRANDES VOLÚMENES DE DATOS

Uno de los aspectos que más puede limitar el desarrollo de las diferentes tecnologías, y en particular de la Inteligencia Artificial es la **ausencia o carencia del talento suficiente**. Se estima que **faltarán más de 1.8 millones de profesionales en el área de seguridad** en los próximos 5 años. La misma carencia se prevé en áreas como la **Inteligencia Artificial** o el **Big Data**.

La **Inteligencia Artificial** se ha convertido en una tecnología de impacto transversal que está acelerando y va a acelerar aún más, tendencias en el ecosistema digital, tanto positivas (competitividad y bienestar) como negativas (ciberataques). Esto crea **riesgos y desafíos únicos**.

En el contexto de esta nueva realidad, España, al igual que el resto de los países de la Unión Europea, **debe presentar a lo largo del año 2020 su estrategia en Inteligencia Artificial**. La estrategia tendrá que considerar la forma como España puede incorporarse a esta disrupción tecnológica, y como puede **impulsarse su desarrollo y adopción** desde las administraciones públicas. Pero la estrategia también tendrá que considerar que esta nueva realidad requiere un **marco regulatorio** consensuado, y anclado en el **principio de precaución**.

En la estrategia **España Digital 2025**, presentada por el gobierno el pasado **23 de Julio**, se incide tanto en los **aspectos de ciberseguridad como de Inteligencia Artificial**, señalando específicamente como objetivos:

Reforzar la capacidad española en **Ciberseguridad,** consolidando su posición como uno de los polos europeos de capacidad empresarial.

Favorecer el tránsito hacia una **economía del dato,** garantizando la seguridad y privacidad y aprovechando las oportunidades que ofrece la **Inteligencia Artificial.**

Como primera medida, en el eje del **plan relacionado con la economía del dato y la inteligencia artificial**, el plan recogía la elaboración de una **Estrategia Nacional de Inteligencia Artificial** con el objetivo de situar a España en la línea de los países líderes en la investigación y uso de una **IA confiable** al servicio del desarrollo económico y social.

Esta estrategia se concibe como un **compromiso** entre la **ciudadanía española**, la **iniciativa privada** y el **sector público**, **alineada con los principios europeos**, respetuosa con los valores compartidos y que ayude a mejorar.

- La **productividad** del **sector privado**
- Las **condiciones de vida** de las **personas**
- La **prestación más eficiente** de **servicios públicos**
- **Resolver** algunos de los **grandes retos** a los que se enfrenta **nuestra sociedad** actual, como el **medio ambiente**, la **movilidad** o el **envejecimiento**

Este documento pretende aportar algunos elementos, reflexiones e ideas sobre la relación entre **Seguridad** e **Inteligencia Artificial**, para que puedan tomarse en consideración en la elaboración de esta estrategia nacional en Inteligencia Artificial.

Las propuestas y reflexiones recogidas en este documento son el fruto del debate mantenido con expertos de la administración española, del ámbito académico y del entorno empresarial, durante el seminario organizado por la Fundación ESYS, celebrado el 24 de septiembre de 2020.

LA RELACIÓN ENTRE **SEGURIDAD** E **INTELIGENCIA ARTIFICIAL**

La Inteligencia Artificial se ha convertido en una tecnología transversal que se incorpora en muchos de los sistemas y aplicaciones que utiliza cualquier compañía. Es por ello por lo que los aspectos de seguridad van a ser **especialmente relevantes en el diseño y utilización de la inteligencia artificial**. De acuerdo con la opinión expresada por el experto *Bruce Schneier*, *"nuestros coches, nuestros dispositivos médicos y nuestros electrodomésticos son ahora ordenadores con cosas adjuntas a ellos. Su nevera es un ordenador que mantiene las cosas frías y el microondas es un computador que las calienta. Su coche es un ordenador con cuatro ruedas y un motor. Los ordenadores ya no son solo una pantalla que encendemos y miramos, y ese es el gran cambio. Lo que era la seguridad informática, en su propio ámbito por separado, ahora es la seguridad de todo".*

Igualmente, si consideramos la **IA**, como un **elemento clave en la automatización de la toma de decisiones**, son varios los niveles de ayuda para la toma de decisión apoyadas en el uso masivo de datos y algoritmos de IA ejecutados en sistemas de computación especiales:

01 El **humano toma todas las decisiones** sin asistencia de computadora.
02 El **ordenador proporciona** un conjunto completo de **alternativas para elección humana**.
03 El **ordenador presenta** un **rango** seleccionado de **alternativas**.
04 El **ordenador sugiere una alternativa**.
05 El **ordenador ejecuta** una decisión **si el humano la aprueba**.
06 El **ordenador ejecuta** una decisión **permitiendo el veto humano** en un tiempo restringido.
07 El **ordenador ejecuta** una acción e **informa** de su decisión **a un humano**.
08 El **ordenador ejecuta** una acción e **informa de ella si es requerida**.
09 El **ordenador ejecuta** una acción e **informa a un humano si lo considera apropiado**.
10 El **ordenador ejecuta** sus acciones **ignorando al humano**.

Cada uno de estos niveles tendrá **diferentes implicaciones en el ámbito de seguridad**, especialmente cuando superamos la frontera de los **niveles de automatización controlados por el ser humano** (niveles 1 a 4), y pasamos a los **niveles de automatización controlados por la máquina** (7 a 10).

Cuanto mayor sea el control de la máquina en la toma de decisión, mayores serán las implicaciones en los aspectos de seguridad.

En este contexto, son varias las perspectivas que pueden utilizarse para analizar la relación entre seguridad e **Inteligencia Artificial**, entre las que podemos identificar tres especialmente relevantes:

Inteligencia Artificial para la Seguridad

Inteligencia Artificial como una nueva amenaza de Seguridad

Seguridad para la **Inteligencia Artificial**

Inteligencia Artificial para la Seguridad

Utilización de la **Inteligencia Artificial** como una tecnología que mejora las prestaciones de las herramientas y sistemas de ciberseguridad. Es ésta un área de rápido desarrollo en el que la **IA** puede potenciar las capacidades de ciberseguridad en áreas tales como:

Detección de intrusiones
Descubrimiento de vulnerabilidades en el código
Detección del fraude
Hacking ético
Detección de Malware
Inteligencia de Amenazas
SOC Inteligentes

Inteligencia Artificial como una nueva amenaza de Seguridad

Al igual que la **IA** puede ayudar a potenciar la ciberseguridad, igualmente también puede utilizarse como una nueva amenaza. La **IA** ha pasado a incorporarse en las tecnologías utilizadas en todos los ciber-ataques, en una gama que abarca desde las ciber-guerras, el ciber-espionaje, el ciber-terrorismo, el ciber-crimen, a la más simple ciber-malicia.

En todas estas áreas la **IA** puede ayudar a explotar vulnerabilidades conocidas, descubrir vulnerabilidades desconocidas o crear nuevas vulnerabilidades. La complejidad por tanto crece y se incrementa por la aportación que puede realizar la Inteligencia artificial en todas las ciberamenazas. Una de las áreas actualmente más conocida es la de *Deep Fake*, o noticias falsas.

Diversos analistas ya consideran como las noticias falsas puede dañar la credibilidad de las empresas, y cómo el riesgo de este fenómeno se ha visto incrementado e impulsado por el uso de la **Inteligencia Artificial**. Igualmente debe mencionarse la pérdida de confianza de ciudadanos y empresas en el uso de determinadas tecnologías, derivada de estas nuevas ciberamenazas, lo que puede retrasar el proceso de transición digital.

Seguridad para la **Inteligencia Artificial**

La **IA**, como nueva tecnología, y dado su carácter transversal, amplía la superficie de ataque, y por tanto requiere medidas específicas para garantizar la robustez, resiliencia y seguridad de los sistemas que la incorporan. Son muchas las tácticas de ataque que se está utilizando contra sistemas que incorporan inteligencia artificial, que abarcan desde al acceso a los datos, hasta la contaminación o manipulación de los mismos.

Será la perspectiva de **Seguridad para la Inteligencia Artificial** la que será abordada en mayor detalle en este documento. Esta es un área que ya ha sido abordada por la Comisión Europea, en el marco de la definición de la **Estrategia Europea para la Inteligencia Artificial**, y que deberá ser igualmente abordada en el contexto de la **Estrategia nacional española de Inteligencia Artificial**.

Seguridad para la **Inteligencia Artificial**

Para mitigar estos nuevos ataques va a ser preciso invertir en todo el ciclo de desarrollo de la **IA** en ámbitos muy diferentes:

Investigación en amenazas a la IA

Diseño de Sistemas de IA seguros y justos:

- Seguridad desde el diseño
- Privacidad desde el diseño y por defecto
- Imparcialidad desde el diseño
- Explicabilidad desde el diseño

Pruebas de los sistemas de IA seguros y justos

Operación de los sistemas de IA seguros y justos

Compartición de Base de Conocimiento de ataques a sistemas de IA

Análisis forense de ataques realizados

Compartición de la información de los sistemas de IA

EL MARCO EUROPEO PARA LA **SEGURIDAD** EN LA INTELIGENCIA **ARTIFICIAL**

Desde el año 2014, la Comisión Europea ha venido trabajando para facilitar el desarrollo de una economía digital apoyada en el uso inteligente de los datos. Entre los pasos más relevantes pueden destacarse el **Reglamento** sobre la **libre circulación de datos no personales**, **la norma sobre ciberseguridad**, **la Directiva sobre los datos abiertos** y el **Reglamento General de Protección de Datos**. En 2018, la Comisión presentó por primera vez una **estrategia de Inteligencia Artificial (IA)** y acordó un **plan coordinado** con los Estados miembros.

Con la elección de una nueva **Comisión Europea en el año 2019** se fijaron **entre sus prioridades para el período 2019-2024 lograr una Europa preparada para la era Digital**. Así lo señaló en su **discurso**, la presidenta de la Comisión *Ursula von der Leyen*, que subrayó la necesidad de que Europa lidere la transición hacia un nuevo mundo digital. En ese contexto, anunció el inicio del debate sobre una **inteligencia artificial centrada en las personas**. En palabras de la propia comisaria: *"Ya sea el cultivo en una agricultura de precisión, un diagnóstico médico más preciso, o una conducción autónoma segura, la inteligencia artificial nos abrirá nuevos mundos. Pero este mundo también necesita reglas. Queremos un conjunto de reglas que sitúen a las personas en el centro. Los algoritmos no deben ser una caja negra y debe haber reglas claras si algo sale mal. La Comisión propondrá una ley en este sentido el próximo año."*

De acuerdo con este objetivo, la Comisión Europea definió en abril de 2019 las Directrices Éticas en el uso **Inteligencia Artificial**. En este documento la Comisión pretendía promover una discusión sobre un marco global en el que Europa pretende desarrollar una **IA** adaptada a los valores éticos europeos.

Para ello **definió siete requisitos esenciales** para lograr una **inteligencia artificial confiable**:

1. **Supervisión humana**: debe de ser supervisada por seres humanos, con las apropiadas medidas de contingencia.
2. **Robustez y seguridad:** los sistemas deben ser «resistentes» y «resilientes» ante eventuales intentos de manipulaciones o de pirateo y dotarse de planes de contingencia.
3. **Privacidad y control de los datos:** se debe de garantizar la privacidad de los datos de los ciudadanos en todo el ciclo vital de la inteligencia artificial.
4. **Transparencia**: la **IA** debe de ser transparente, lo que supone poder reconstruir cómo y por qué se comporta de una determinada manera y quienes interactúen con esos sistemas deben de saber que se trata de inteligencia artificial, así como qué personas son sus responsables.
5. **Diversidad, no discriminación y equidad**: la inteligencia artificial debe tener en cuenta la diversidad social desde su desarrollo para garantizar que los algoritmos en que se base no tengan sesgos discriminatorios directos o indirectos.
6. **Bienestar social y ambiental**: el desarrollo tecnológico debe tener en cuenta su impacto social y medioambiental de forma que sea sostenible y ecológicamente responsable.
7. **Responsabilidad**: la inteligencia artificial y sus resultados deben **rendir cuentas ante auditores** externos e internos.

El requisito 2 aborda específicamente los **aspectos de seguridad en la inteligencia artificial**. La fiabilidad de la inteligencia artificial requiere que los algoritmos sean suficientemente seguros, fiables y sólidos para resolver errores o incoherencias durante todas las fases del ciclo de vida útil de los sistemas de inteligencia artificial, así como protegerse frente a posibles ataques o manipulaciones.

Este aspecto abre un nuevo campo en la relación entre **Seguridad** e **Inteligencia Artificial**. Son muchos los aspectos que deben abordarse, entre los cuales pueden señalarse:

Esquemas de Certificación – Garantías de Seguridad

Relación Seguridad y Transparencia - Trazabilidad

Relación Seguridad y Responsabilidad - Rendición cuentas

Todas estas áreas deberían de alguna forma tenerse en cuenta en la elaboración de la nueva estrategia nacional en **Inteligencia Artificial**. Con el objetivo de desarrollar unas directrices para el cumplimiento de estos principios éticos, la Comisión Europea constituyó un grupo de expertos de alto nivel (*High Level Expert Group on AI - AI HLEG*), que elaboraron un documento inicial de valoración y evaluación para lograr una **IA** confiable (**AI assessment list).**

En junio de 2019 la **Comisión Europea** lanzó una **fase piloto** en la que **han participado más de 350 empresas**, que han revisado y valorado las directrices recogidas en el documento elaborado en el grupo de expertos. La Fase del Piloto se cerró el 1 de diciembre 2019, y tras este proceso, el **AI HLEG** se comprometió a publicar un nuevo documento **en Julio 2020 (actualización del AI assessment list).** La versión revisada se **presentó el 17 de Julio.**

El documento pretende servir de guía para todas las empresas que están trabajando en el desarrollo, implementación y despliegue de sistemas que incorporan **IA**, para poder validar que es una **IA** confiable. De nuevo, estos elementos deberán tenerse en cuenta a la hora de elaborar la nueva estrategia en **Inteligencia Artificial**.

CONSECUENCIAS **GEOPOLÍTICAS** DE LA INTELIGENCIA **ARTIFICIAL**

Parece claro que la **IA** se ha **convertido en un elemento decisivo** para la competitividad de las empresas. Con esta consideración, a nadie puede sorprender que esta nueva tecnología se haya convertido igualmente en un **aspecto crítico de la batalla tecnológica y geopolítica que libran** las grandes potencias tecnológicas del mundo, **Estados Unidos y China**.

Como se ha señalado anteriormente, la **IA** se basa en diferentes componentes, entre los que se encuentran los **sensores,** los **sistemas de comunicación**, los **ordenadores**, las **aplicaciones** o los **algoritmos**. Todos estos elementos tienen importancia estratégica en tanto en cuanto su disponibilidad puede verse restringida, tanto desde el punto de vista de su fabricación, como de su capacidad de utilización.

Si analizamos la **situación de disponibilidad** de los diferentes componentes, encontramos diferencias notables, que apuntan a **consecuencias geopolíticas**:

Sensores	Diseños en Estados Unidos y fabricación sudeste asiático.
Sistemas de comunicación	La tecnología 5G cuenta con fabricantes asiáticos y europeos; el despliegue de red está siendo variable, con España situada en buena posición.
Ordenadores	A falta de la disponibilidad de la computación cuántica, la capacidad de computación está muy extendida.
Aplicaciones y algoritmos	Aplicaciones y algoritmos: en gran parte en empresas privadas de Estados Unidos o gobiernos como China y Rusia, en grado menor en muchas empresas de todo el mundo, incluida España.
Capacidad de utilización	Abierta, solo restringida por la formación de los usuarios.

En relación con el hardware específico para Inteligencia Artificial, la situación es preocupante en lo que respecta a la fabricación, dominada por la empresa TSMC, la mayor empresa fabricante de semiconductores del mundo, con sede en Taiwán. **La capacidad de fabricación de CI de alta densidad está muy concentrada en Asia (China, Corea del Sur, Japón y Taiwán). El diseño de CI para IA sigue dominado por Estados Unidos**:

Apple	Ya es responsable de un quinto de las ventas de la mayor empresa de fabricación, **TSMC**, y contrata más de la mitad de su capacidad de **7nm**.
Google	Fabrica su **chip de IA TPU** en **TSMC** con tecnología de **27nm**.
Nvidia	Diseña sus **chips de procesamiento gráfico (GPU)** en Estados Unidos, pero los fabrica **TSMC**.

En este contexto, la **situación de la Unión Europea es preocupante** porque **no dispone de capacidad de fabricación de circuitos integrados (CI) de IA masivos con resoluciones inferiores a 10nm**. No cabe duda de que la relevancia estratégica y las repercusiones geopolíticas de la IA crecerán en la próxima década. Esto plantea algunos retos para la UE, e igualmente para España, que tendrán que ser considerados en el marco de la Estrategia nacional de Inteligencia Artificial:

- **Dependencia de componentes hardware para IA** (ej.: circuitos integrados)
- **Debilidad de plataformas cognitivas horizontales europeas**
  Robótica inteligente
  Industrial
- **Robots acompañantes**
- **Déficit de recursos humanos**
- **Inversiones públicas reducidas**
- **Regulación adecuada: equilibrio para evitar infra y sobre regulación**


INTELIGENCIA **ARTIFICIAL**
SEGURIDAD Y **DEFENSA**

La **inteligencia artificial** se ha incorporado como una nueva tecnología al servicio de la Defensa. Esta tecnología, **asociada a otras tecnologías** como la **robótica**, la **cibernética** o las **telecomunicaciones**, ya ha empezado a utilizarse para desarrollar **capacidades militares**.

Como en cualquier otro ámbito, el **uso de esta tecnología plantea consideraciones éticas**, que van en gran medida ligadas al ámbito de la seguridad. Aun cuando estas consideraciones son aplicables a todos los sistemas de defensa, sin duda su consideración será más relevante en los sistemas que tienen la capacidad de producir muerte y destrucción, como los sistemas de armas autónomos letales. En este sentido, la problemática es similar a la ya considerada sobre el grado de autonomía que tiene una **IA** en la toma de decisiones. En el ámbito militar esto se traduce en si podemos dejar que una **IA** dirija el empleo de los sistemas de armas, particularmente los **Sistemas de Armas Autónomos Letales (SALAS)**, tomando decisiones de forma totalmente autónoma sobre el uso de la fuerza letal, en el complejo campo de batalla del presente y del futuro, independientemente del ser humano.

En el **ámbito de la defensa** se han identificado **principios éticos para el diseño, desarrollo, despliegue y usos éticos de capacidades militares habilitadas por la IA** que son **muy similares** a los principios éticos identificados por la **Comisión Europea para el uso de la IA**. En concreto el departamento de Defensa americano notificó los siguientes principios:

Responsabilidad **Equidad** **Identificabilidad** **Fiabilidad**

Desde el punto de vista de la seguridad y la defensa, la **estrategia nacional de Inteligencia Artificial debería tener en consideración los siguientes aspectos**:

- **Alinear** la financiación con los **Programas Europeos** que disponen de financiación orientada a la **IA** como, por ejemplo, el **Programa Marco de I+D+I H2020** o el **futuro Horizonte Europa**; el **Programa Life**, el **Programa Europa Digital (DEP)** o el **Programa Europeo de Desarrollo Industrial en materia de Defensa (EDIDP)** o el futuro **Fondo Europeo de Defensa (EDF)**.

- **Promover la explotación de sinergias** entre la **investigación civil y la investigación en defensa**, aprovechando el Protocolo General de Actuación vigente entre el **MINISDEF** y **MICIU**, **CDTI** y **AEI**.

- Abordar la **incorporación de la IA** en **sensores**, **plataformas**, **sistemas de mando** y **control**, etc., utilizados en las misiones asignadas.
  Esta segunda dimensión es la más compleja técnicamente y la que exige un mayor esfuerzo inversor y tiene un carácter estratégico para España por dos razones:

  - Por las **mejoras que puede proporcionar a la operatividad de las Fuerzas Armadas**, redundando en una mayor seguridad para el país.
  - Por ser la **dimensión que permite la capacitación del tejido tecnológico nacional** (centros tecnológicos y empresas), y que posibilita que los productos diseñados y fabricados lleguen un mercado muy exigente, lo que incrementa el número de oportunidades de crecimiento e internacionalización al tratarse de retos tecnológicos comunes a otros sectores y al resto de Fuerzas Armadas de otros países.

España trabaja en el ámbito de defensa de forma coordinada con la UE y OTAN y dentro de un marco ético y legal en la aplicación de la **IA** a los sistemas de armas. **La IA, como elemento esencial rector de los sistemas de arma autónomos letales, plantea problemas éticos.** En gran medida, si deja de haber un "control humano significativo" en el uso de sistemas de armas autónomos letales, siempre tendrá que haber una trazabilidad y capacidad de atribución a un ser humano en las decisiones que impliquen el uso de la fuerza letal. Si no es así, habrá cambiado la naturaleza de la guerra y ya no será un fenómeno humano sino un fenómeno entre máquinas.

PROPUESTAS
FUNDACIÓN ESYS

PLANTEAMIENTO GENERAL DE LA PROPUESTA

España debe tener contar con una **estrategia de IA propia**, aunque sea dentro del marco de las directrices y estrategia de la UE. Las iniciativas europeas han ido en gran parte dirigidas a la regulación de la IA y a el establecimiento de principios éticos.

Existe una estrategia europea de desarrollo e impulso de la IA que aún debe concretarse, y debe plasmarse en una apuesta económica de financiación acorde al reto que supone la IA para todos los países. Las grandes empresas españolas son ya usuarios de la IA como factor determinante de su supervivencia a medio plazo. Las empresas españolas y el Gobierno necesitan, por tanto, **utilizar la IA de forma ineludible**. Y es en esta implantación y utilización crecientes de la IA en las empresas, en las que desde la Fundación ESYS queremos llamar la atención sobre la **necesidad de tener en cuenta la Seguridad como un componente esencial**.

Ciudadanos, administraciones y empresas se van a ver impactados por la Inteligencia Artificial, y por tanto todos ellos deberían tener un rol dentro de la Estrategia nacional de Inteligencia Artificial. La labor de **concienciación mediante la comunicación estratégica** de los beneficios y los riesgos asociados al uso de la Inteligencia Artificial será un factor crítico para el éxito da la estrategia nacional en Inteligencia Artificial. Los aspectos de concienciación y comunicación deben por tanto formar también parte de la estrategia y deben poner a la Seguridad en su foco. Entre los aspectos más relevantes que limitan el desarrollo de la Inteligencia Artificial en España y en Europa debe destacarse la **carencia de profesionales especializados** en esta área. Su remedio es complejo a corto plazo, y es por ello por lo que debería constituir una de las prioridades de la estrategia española. Y estos profesionales deberían incorporarse con la perspectiva de la Seguridad grabada en su formación y sensibilidad.

España debe centrar sus esfuerzos, y la dotación de recursos en aquellas áreas donde aún pueda lograr una posición de relevancia, y en aquellas otras consideradas estratégicas para adquirir un nivel adecuado de independencia tecnológica.

Dadas las barreras existentes (por posiciones ya ganadas o por capacidades técnicas) en el acceso a los diferentes componentes de la IA **se proponen tres componentes sobre los que actuar de forma prioritaria**:

Despliegue de sistemas de comunicación seguros

Aplicaciones y algoritmos en los que su seguridad intrínseca sea un valor distintivo

Capacidad de utilización

Propuestas para la estrategia nacional de Inteligencia Artificial

En este contexto, la **Fundación ESYS** plantea las siguientes propuestas básicas en relación con la Estrategia nacional de Inteligencia Artificial:

Apoyar el despliegue de Sistemas de Comunicación: apoyando a la extensión de la red de fibra y al despliegue de las redes 5G, con exigencias de certificaciones y de elección de componentes acordes con las necesidades de seguridad exigibles desde la UE.

Apoyar el desarrollo y especialización en aplicaciones y algoritmos de IA: asistir a las empresas españolas, orientando las subvenciones de I+D+i en estas áreas. En particular el uso de la compra Pública Innovadora centrada en el área de la seguridad aplicada a la inteligencia artificial puede tener un impacto muy relevante.

Promover el uso de la IA en todos los ámbitos empresariales: apoyo, incluso fiscal, a la utilización de la IA en los procesos de las empresas, unido a la concienciación de la seguridad en su uso.

Gestionar la dependencia tecnológica: intensificación de la ingeniería inversa para el análisis de las compras tecnológicas, ya sea desde la Administración o a través de empresas privadas contratadas por el Gobierno, muy especialmente para contrarrestar las vulnerabilidades embebidas en los equipos.

Crear, atraer y retener el talento para superar la carencia de especialistas: Esta situación puede abordarse con un plan específico universitario, de formación profesional y escolar, para la promoción y obtención de profesionales en todos los segmentos: usuarios, analistas, diseñadores de algoritmos, operadores, Ingeniería inversa, etc., que ya están siendo necesarios para la ciberseguridad en general.

Promover y gestionar las políticas de seguridad en la Inteligencia Artificial: La seguridad debe constituir en un elemento esencial en el diseño de cualquier estrategia de Inteligencia Artificial. La guía para el cumplimiento de los principios éticos elaborada por el grupo de expertos de alto nivel en Inteligencia Artificial es un punto de partida, que puede proporcionar elementos clave para la estrategia española. La robustez y resiliencia de los sistemas de Inteligencia Artificial debe constituirse en una prioridad básica.

Promover acciones de concienciación de ciudadanos, empresas y administraciones sobre los beneficios y riesgos de la Inteligencia Artificial, mediante campañas de comunicación estratégicas: Dado que ciudadanos, empresas y administraciones se verán impactados por el uso de la inteligencia artificial, la estrategia nacional debería cuidar también la labor de concienciación en todos los ámbitos sobre los diferentes agentes. La labor de concienciación debe cubrir las oportunidades y el sentido de urgencia, pero también debe abordar los nuevos riesgos inherentes al uso de la inteligencia artificial, especialmente los relacionados con la seguridad.

Propuestas para impulsar y acelerar el desarrollo de la IA en España

Para **impulsar y acelerar el desarrollo de la IA en España**, se proponen una serie de líneas de acción específicas:

A

Abordar un estudio que determine las **principales aplicaciones que pueden beneficiarse de la introducción de la IA en las administraciones públicas**, y de los riesgos y vulnerabilidades que conllevan, incidiendo en la disponibilidad de datos para entrenamiento de los sistemas. El ámbito de defensa puede ser uno de los relevantes, pero igualmente debe abordarse para otros sectores económicos.

B

Promover la **recopilación y adecuación de los datos disponibles** en el ámbito público (y privado) en aquellos casos en los que sean insuficientes para ser explotados por sistemas inteligentes, prestando especial interés a la seguridad de los mismos.

C

De forma coordinada entre todas las administraciones públicas, **favorecer el aprovechamiento por el tejido tecnológico nacional de todos los instrumentos existentes de los Planes Estatales de I+D+I**, en particular los dirigidos a Compra Pública Innovadora, para desarrollar soluciones tecnológicas seguras para las administraciones públicas (ej. en el ámbito de defensa), aportando éstas su conocimiento como usuarios finales, así como los datos para el entrenamiento de los sistemas inteligentes.

D

Favorecer el conocimiento del tejido tecnológico nacional de las **oportunidades europeas e internacionales en el ámbito de la I+D+i**, de forma que se logren importantes niveles de participación nacional en estos programas, mejorando su capacitación tecnológica en el uso de la IA en defensa.

Aspectos específicos de la propuesta en el ámbito de la seguridad para la IA

La **seguridad merece especial atención en el diseño de la estrategia nacional en inteligencia artificial**. Los sistemas que incorporan inteligencia artificial son **sistemas complejos que dificultan aún más la mitigación de riesgos y la protección frente a ciberataques**. La guía preparada por la Comisión Europea para asegurar el cumplimiento de los principios éticos en las empresas muestra la complejidad del reto. Las muchas preguntas que plantea, y la difícil respuesta a muchas de ellas en la mayoría de las empresas hace necesario proporcionar más ayuda a las empresas para asegurar que los sistemas de **IA** están suficientemente protegidos.

Es preciso invertir en todo el ciclo de desarrollo de la **IA** en ámbitos muy diferentes:

Investigación en amenazas a la IA

Diseño de Sistemas de IA seguros y justos:

- Seguridad desde el diseño
- Privacidad desde el diseño y por defecto
- Imparcialidad desde el diseño
- Trazabilidad (y capacidad de explicación) desde el diseño

Pruebas de los sistemas de AI seguros y justos

Operación de los sistemas de AI seguros y justos

Compartición de Base de Conocimiento de ataques a sistemas de IA

Análisis forense de ataques realizados

Compartición de la información de los sistemas de IA

Todos estos aspectos deberían estar contemplados en la estrategia nacional de IA, con **especial foco en ayudar a todas las compañías en poder implementar de forma efectiva los principios éticos definidos a nivel europeo**, y muy en particular el principio 2 que señala a la robustez y resiliencia de los sistemas.

Como proceso que es, la **IA** va a requerir una metodología que recoja todos los aspectos relacionados (usabilidad, utilidad, ética, privacidad, sesgo, fiabilidad, robustez…), no sólo el desempeño. Creando técnicas y métodos que faciliten el diseño, desarrollo, validación y despliegue de sistemas prácticos basados en **Inteligencia Artificial**, con un enfoque multicriterio **"3Q"**: **calidad del dato**, **calidad del modelo** y **calidad del resultado**. Este aspecto debería incorporarse en la estrategia de **IA**.

En general, la estrategia española debe ser lo más concreta posible, contando con la seguridad como elemento diferencial internacional, y trascender de las directrices y las intenciones a la disposición de fondos y planes concretos de actuación.

aena endesa PROSEGUR RED ELÉCTRICA DE ESPAÑA Telefónica

SEMINARIO FUNDACIÓN ESYS

24 SEPTIEMBRE 2020

FUNDACIÓN ESYS

FUNDACIÓN ESYS EMPRESA, SEGURIDAD Y SOCIEDAD

www.fundacionesys.com