3ª EDICIÓN

Observatorio de Derecho Digital IE - ECIJA

Informe Primera Sesión

Gobernanza y Cumplimiento Normativo en la Era de la IA: Informe sobre el Impacto y Gestión en los Departamentos Legales

Diciembre de 2024

www.ie.edu/odigitallaw

ie UNIVERSITY ECIJA

Prólogo

En los últimos años, la Inteligencia Artificial (IA) ha transformado de manera radical la forma en la que las empresas y las instituciones operan, innovan y se relacionan con la sociedad.

Esta revolución tecnológica no solo ha traído consigo oportunidades significativas, sino también desafíos sin precedentes, especialmente en lo que respecta al cumplimiento normativo y a la gobernanza responsable de la IA.

Este Informe, fruto de la colaboración entre grandes empresas y expertos en el ámbito de la tecnología y la regulación, se adentra en el complejo, pero crucial tema del gobierno de la IA.

El Informe aborda aspectos clave como la Política de Uso de la IA, el estado actual de las regulaciones aplicables y la distribución de roles y competencias necesarios para una gestión eficiente y ética de esta tecnología.

En un contexto en el que las implicaciones de la IA afectan tanto a la competitividad empresarial como al bienestar de la sociedad, es fundamental que las organizaciones cuenten con un marco sólido de gobernanza. Esto no solo implica garantizar el cumplimiento de la normativa vigente, sino anticiparse a nuevas regulaciones y recomendaciones, fomentar la transparencia y promover una implementación ética que respalde la confianza de los usuarios y los consumidores.

El presente Informe no solo ofrece un diagnóstico del estado actual del gobierno de la IA en las organizaciones, sino que también brinda perspectivas y recomendaciones prácticas para quienes tienen la responsabilidad de adaptarse a este nuevo marco. El Informe recoge las mejores prácticas identificadas a nivel corporativo, así como reflexiones sobre cómo adoptar los marcos normativos a los vertiginosos avances tecnológicos.

Este esfuerzo conjunto representa una hoja de ruta para avanzar hacia un modelo de gobernanza de la IA que sea robusto, adaptable y alineado con los valores legales y éticos de la sociedad.

Estamos convencidos de que este Informe aportará una perspectiva valiosa para fortalecer la gobernanza corporativa y el cumplimiento normativo en torno a la IA, ayudando a las organizaciones a alinear sus estrategias con los nuevos marcos regulatorios.

¿Una inteligencia artificial que te ayude a cumplir con la normativa? ¿Y si este prólogo ya lo hizo?

Prólogo creado por IA "ChatGPT"

1. Introducción

El desarrollo y uso de la IA han suscitado una creciente preocupación en torno a la necesidad de establecer un marco normativo que garantice su implementación responsable y segura. El Reglamento de Inteligencia Artificial de la Unión Europea (UE) 2024/1689 marca un hito al abordar aspectos clave como las políticas de uso, la definición de roles y competencias, y la gobernanza del uso de esta tecnología en las organizaciones.

Este informe aborda las discusiones relativas a los elementos fundamentales del Reglamento, ofreciendo una visión práctica para entender cómo las empresas deben adaptar sus estructuras de cumplimiento y reforzar su gobernanza interna para garantizar el respeto a los principios éticos y legales que rigen el uso de la IA.

La entrada en vigor del Reglamento de Inteligencia Artificial representa un paso decisivo hacia un marco normativo uniforme que aborda los retos asociados al desarrollo y uso de esta tecnología en la Unión Europea.

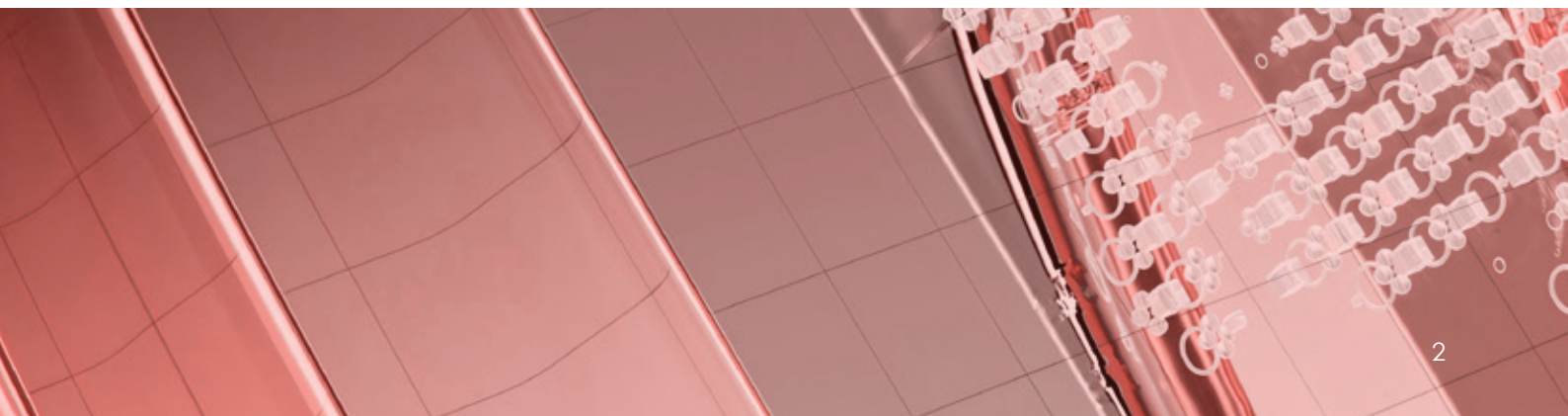
El Reglamento, basado en un enfoque de gestión del riesgo (artículo 9), establece determinadas obligaciones para los distintos operadores de la cadena de valor; desde los proveedores hasta los responsables del despliegue de los sistemas de IA. Entre sus disposiciones, destacan los requisitos de gobernanza interna que obligan a las organizaciones a adoptar políticas de uso responsables y asegurar supervisión humana en sistemas de alto riesgo (artículos 13 y 14).

El Reglamento también introduce mecanismos para la gestión y evaluación de riesgos asociados a la IA (artículo 23), promoviendo la transparencia y la rendición de cuentas mediante la creación de roles específicos, como el del 'responsable del despliegue' (artículo 26).

Además, la Oficina Europea de Inteligencia Artificial supervisará la correcta implementación de estas normas (artículo 62), fortaleciendo un enfoque coordinado a nivel europeo para garantizar la protección de derechos fundamentales, fomentar una adopción ética de la IA en todos los sectores y fortalecer el mercado único digital europeo.

Este Informe proporciona una guía práctica para entender cómo las empresas están integrando estos requisitos en sus estructuras de cumplimiento, abordando tanto la gestión de riesgos como la necesidad de un enfoque proactivo en la gobernanza de la IA.

En un entorno donde la innovación avanza más rápido que la regulación, el cumplimiento normativo no solo se configura como una necesidad, sino como un reto estratégico que definirá la capacidad de las organizaciones para gestionar riesgos, garantizar el respeto a los derechos fundamentales y operar de manera ética y sostenible en la era de la IA.



2. Estado del desarrollo de políticas corporativas de uso IA

En la actualidad, la gran mayoría de las empresas se encuentra en una fase inicial en lo que respecta al desarrollo e implementación de políticas corporativas específicas para el uso de la IA en el seno de sus organizaciones. Aunque muchas organizaciones han empezado a explorar las implicaciones de la IA y a integrar sus principios básicos en sus operaciones, aún son pocos los que han formalizado y aprobado políticas y procedimientos que guíen de manera explícita su aplicación dentro de los marcos establecidos por el Reglamento de Inteligencia Artificial.

No obstante, en esta etapa temprana, el enfoque sigue siendo mayormente genérico. La mayoría ha optado (o está optando) por incorporar los principios corporativos de la organización de forma transversal (transparencia, el rol de los humanos, equidad, seguridad, ética, responsabilidad, privacidad, etc.)

En el análisis de las empresas que han participado, se han apreciado diferentes velocidades de avance en el desarrollo de políticas corporativas relacionadas con la IA, dependiendo de los distintos Sectores de actividad al que pertenecen. Este fenómeno se explica principalmente en función de la dependencia tecnológica de cada Sector en cada uno de los eslabones críticos de su Cadena de Valor.

En sectores como la tecnología y las telecomunicaciones donde la IA juega un papel más relevante en el desarrollo de productos y servicios, se observa un avance más acelerado en la formalización de políticas. Estas empresas, por su proximidad a la innovación tecnológica y la integración de la IA en sus operaciones cotidianas, han desarrollado marcos regulatorios internos más estructurados y específicos para el garantizar un uso responsable y ético de la IA que permita minimizar los riesgos asociados.

Por otro lado, con ciertas diferencias, otros sectores más tradicionales o menos dependientes de la IA, como servicios financieros o *manufacturing,* las políticas de la IA aún están en sus primeras fases de desarrollo. La incorporación de la IA en estos sectores depende en gran medida de la digitalización de sus procesos, lo que implica que las políticas de IA se integran gradualmente dentro de un contexto más amplio de transformación digital.
Respecto del sector asegurador, las políticas corporativas de uso de la IA están avanzando, pero a un ritmo variable. No obstante, la dependencia tecnológica en este sector está más centrada en la recopilación y análisis de datos, lo que requiere un enfoque más cauteloso respecto del cumplimiento normativo en relación con la protección de datos personales.
El sector de la seguridad se enfrenta a un desafío único, ya que la integración de la IA en sus operaciones incluye el uso de tecnologías de alto riesgo, por lo que el avance en políticas es más lento debido a la necesidad de adaptar la tecnología a marcos legales estrictos que protejan los derechos fundamentales.

Sin embargo, nos encontramos en otros sectores donde puede existir una fuerte vinculación del uso de la IA en los procesos operativos de logística o transportes, la evolución de las políticas es aún incipiente. Asimismo, el sector energético apuesta por la innovación y el uso de la IA, enfrentándose a nuevos retos con la IA generativa, a la que se suma el desarrollo del gobierno de la IA generativa. Todo ello sin perjuicio de que el uso de la IA, por lo menos un tipo de IA técnico o predictiva ya se venía utilizando años atrás.

En resumen, aunque en estos sectores se están dando pasos hacia la integración de políticas de IA, la velocidad de adopción está fuertemente influenciada por la naturaleza de las actividades, el grado de digitalización y la necesidad de cumplir con las normativas específicas relacionadas con la privacidad, la seguridad y la protección de datos.

Mientras el reglamento de inteligencia artificial exige políticas claras y solidas para su uso, muchas empresas aún están adaptandose a medida que estas tecnologías transforman sus estructuras internas.

3. Otros aspectos destacados en el cumplimiento normativo y gestión responsable de la IA

En el marco del cumplimiento normativo y la gestión responsable de la IA, las grandes empresas han puesto de manifiesto la urgencia e importancia de abordar y gestionar los riesgos asociados al uso de esta tecnología. Este enfoque responde a la creciente accesibilidad de herramientas de IA, que pueden ser utilizadas por cualquier empleado con acceso a una licencia, lo que aumenta la posibilidad de usos indebidos o no alineados con las políticas corporativas de la organización. Todos destacan la necesidad de conocer qué está ocurriendo dentro de la compañía, en especial, relativo al control del uso de información confidencial.

La rápida aparición de *early adopters* corporativos ha acelerado la implementación parcial de licencias de inteligencia artificial en diversas funciones del negocio. Este fenómeno ha permitido a las empresas explorar nuevas posibilidades y mejorar su eficiencia operativa, pero también ha puesto de relieve la necesidad urgente de establecer controles claros y efectivos desde las etapas iniciales. La adopción temprana de estas herramientas exige no solo un enfoque estratégico para su uso, sino también la incorporación de mecanismos de supervisión y gobernanza que garanticen el cumplimiento normativo, minimicen riesgos y alineen estas tecnologías con los objetivos éticos y operativos de la organización.

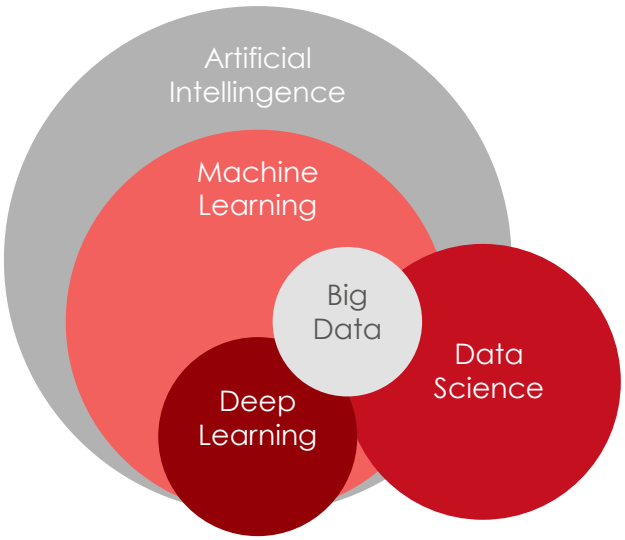
Como consecuencia, se han comenzado a realizar *assessments* detallados de sus capacidades internas relacionadas con esta tecnología. Estas evaluaciones tienen como objetivo identificar las competencias ya adquiridas, así como las áreas que requieren mejoras o ajustes para garantizar el cumplimiento del Reglamento de IA. Este proceso permite a las organizaciones adaptarse a las nuevas exigencias normativas, así como convivir con entorno regulatorio en evolución y asegurar que el uso de la IA sea seguro, ético y alineado con los estándares legales y operativos.

Esta recopilación de información interna requiere coordinación interdepartamental, mediante la creación de grupos de trabajo multidisciplinares incorporando las funciones de:

- Estrategia
- Riesgos
- Compliance
- Tecnologías de la Información
- Asesoría Jurídica
- Otros *(dependiendo de la actividad de la Compañía)*

Como resultado de estos internal assessments, se están generando registros de todos los sistemas de IA con los que se está trabajando en las diferentes áreas de la organización. Un foco clave en estos análisis es la distinción entre IA Generative AI vs General AI. Mientras que la IA Generativa se centra en la creación de contenido nuevo a partir de datos existentes, la IA General se basa en tecnologías de *machine learning,* diseñadas para desarrollar capacidades más amplias y versátiles que emulan habilidades humanas complejas, como el razonamiento y la adaptación autónoma a contextos diversos.

Esta diferenciación es crucial para entender las implicaciones éticas, normativas y operativas de cada tipo de IA, así como para identificar los riesgos específicos que conlleva su adopción. Las empresas están adaptando sus capacidades internas y estableciendo marcos de gobernanza específicos para garantizar que cada tipo de IA se utilice de manera responsable y en alineación con los requisitos del nuevo reglamento de IA.



Para alinear estos esfuerzos, muchas empresas están desarrollando e implementando herramientas específicas para la gestión interna de los distintos aspectos de la IA. Estas plataformas no solo permiten monitorizar y supervisar el uso de la IA, sino que también integran mecanismos para la gestión responsable como la evaluación ética, el cumplimiento normativo y el análisis de riesgos. Al centralizar estos procesos, las organizaciones pueden garantizar una gestión más responsable de la IA, fomentando la transparencia, el control y la alineación con los marcos regulatorios emergentes.

Para garantizar una gestión responsable y efectiva de la inteligencia artificial, muchas organizaciones están creando comités internos que integran perfiles diversos. Estos comités combinan la perspectiva técnica de expertos en IA y *data science* con la sensibilidad ética y social de profesionales provenientes de las humanidades, como filósofos, sociólogos y juristas. El equilibrio ideal de estos equipos incluye especialistas en cumplimiento normativo, gestores de riesgos, negocio y líderes tecnológicos, asegurando un enfoque integral en la toma de decisiones.

A nivel internacional, los grandes grupos están adoptando una jerarquía clara para gestionar estos aspectos, con roles específicos como "IA Champions" o "Ethical AI Managers", que lideran iniciativas dentro de sus departamentos. En algunos casos, también se establecen funciones en las B&Cs (*business and corporate divisions*) como *AI Governance Leads o AI Compliance Officers,* responsables de supervisar la alineación entre las políticas internas y las normativas globales. Esta estructura busca establecer un liderazgo claro en la adopción y supervisión de la IA, promoviendo una gestión alineada con las mejores prácticas y estándares internacionales.

Como parte de los aspectos clave del cumplimiento normativo y la gestión responsable de la inteligencia artificial, la formación y la comunicación interna se consolidan como pilares fundamentales. La formación permite a los empleados comprender no solo las capacidades y limitaciones de las tecnologías de IA, sino también los riesgos asociados y las normativas aplicables. Las empresas están apostando por programas educativos adaptados a diferentes niveles y roles, desde talleres prácticos para usuarios operativos hasta sesiones estratégicas para líderes y gestores.

De forma complementaria, la comunicación interna juega un papel crucial en la construcción de una cultura organizativa que priorice el uso ético y responsable de la IA. Las iniciativas incluyen la difusión de guías prácticas, la creación de canales para reportar inquietudes o incidentes relacionados con la IA y la promoción de valores corporativos que refuercen el compromiso con la transparencia y la gobernanza. Estas acciones no solo fomentan un entorno de confianza y colaboración, sino que también aseguran que todos los niveles de la organización estén alineados con los objetivos y retos del emergente panorama normativo de la IA.

La gestión responsable de la IA no es solo una cuestion técnica, sino un compromiso ético y estratégico

Toxicity
Toxic, obscene, or otherwise inappropriate outputs.

Polarit:
Unfair positive or negative attitudes to certain individuals or groups.

Discrimination
Model performance is less robust for certain social groups.

Human-Computer Interactions
Over-reliance on the outputs of AI due to perceived sentience or blind trust in an automated system.

Disinformation
Presenting factually incorrect answers or information.

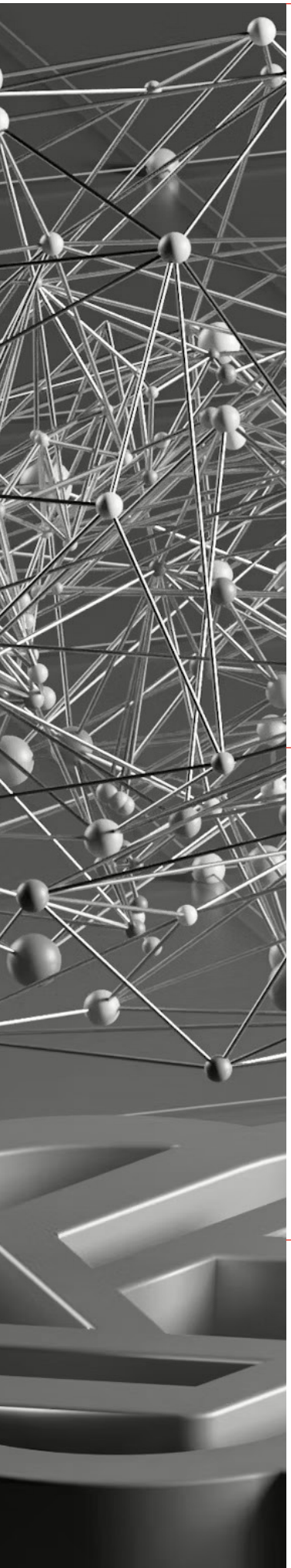
Data Privacy
Input data shared back to 3rd-party model providers and possibly shared as future outputs to non-authorized users.

Model Security
Ability for a user to circumvent security protocols intended to prevent social-technical harms or gain access to unauthorized data.

Copyright Infringements
Redistribution of copyrighted material, presented as original content.

https://www.nist.gov/news-events/news/2023/01/nist-risk-management-framework-aims-improve- trustworthiness-artificial# Source: Data Iku

4. Entrando en el detalle de su implementación



1. Gestión de riesgos en el uso de la IA

Las grandes empresas han identificado como prioridad la adopción de mecanismos para evaluar y mitigar los riesgos asociados a la IA. Entre las medidas implementadas destacan:

- Según lo indicado en la sección anterior, en relación con el resultado del **assessment interno,** el punto de arranque es determinar las áreas internas de impacto.
- **Mapeos de riesgos:** El mapeo de todos los modelos de IA que estén siendo utilizados dentro de la organización hará posible la creación de un registro interno con el listado de dichos modelos, sus características, su impacto y la identificación del riesgo asociado.
- **Evaluaciones de impacto** (AI Impact Assessments): una vez identificados todos los riesgos, procederemos a su categorización y a su posterior priorización en función del impacto.
- **Metodología de evaluación:** a partir de aquí, debería desarrollarse una metodología de evaluación del impacto que mayoritariamente asemejan a la de Protección de Datos (protección de la Privacidad), de cara a la evaluación de los componentes de las IAs. Ello igualmente vinculado a la afección a esta tipología de riesgo.
- **Integración de principios éticos:** La implementación práctica de principios como transparencia, equidad y responsabilidad se traduce en métricas específicas y controles automatizados
- **Control ex ante a la puesta en marcha**. Se recomienda el testeo interno de todos los modelos de IA, a diferentes escalas, antes de autorizar su implementación.

2. Coordinación interdepartamental

La transversalidad de la IA exige la colaboración entre múltiples áreas organizativas para garantizar una gestión integral.

- Creación de comités interdepartamentales: Estos órganos reúnen representantes de compliance, TI, legal, recursos humanos y operaciones para alinear estrategias. Actualmente, existen fórmulas diversas, aunque mayoritariamente nos encontramos con que las empresas optan por crear o integrar el Comité de Privacidad & AI (como órgano de segundo nivel) compuesto por equipos multidisciplinares, y estableciendo los niveles de aprobación en función del riesgo identificado.
- En el caso de que la organización dispusiera de sedes en diferentes localizaciones, se recomienda la creación de Oficinas IA en cada una de ellas al efecto y coordinadas con el Comité de Privacidad & AI.
- Flujos de trabajo compartidos: Establecimiento de procesos para la comunicación fluida entre departamentos y la toma de decisiones informada.

3. Organización interna y mecanismos de gobernanza

La implementación de mecanismos internos específicos y políticas para el uso y gobernanza de la IA es un paso esencial para garantizar el cumplimiento normativo:

- Creación de órganos de supervisión interna: Equipos o comités responsables de la implementación, seguimiento y actualización de las políticas de IA.

- Roles especializados: Las empresas han comenzado a incorporar figuras como el "AI Compliance Officer" o responsables de gobernanza tecnológica, asegurando que exista un punto focal para estas cuestiones.

Con toda la información recopilada y la estructura creada para la gestión de las IAs, estaremos en disposición de poner en marcha su Gobernanza mediante la identificación de los touchpoints con las políticas internas vigentes: decidiendo a qué stakeholder(s) se le asigna la responsabilidad. Se destaca:

- Políticas internas sobre el uso responsable de la IA: Documentos que establecen reglas claras, limitaciones y requisitos de cumplimiento adaptados al marco regulatorio aplicable.
- Reportes internos regulares: Informes que detallen el estado de la implementación y los resultados obtenidos en la gestión de riesgos.

4. Formación, comunicación, y sensibilizaciones internas

La comunicación efectiva en torno al cumplimiento normativo en IA es crucial para alinear a toda la organización con sus objetivos éticos y regulatorios.

- Programas de formación continua: Capacitación en ética, regulaciones aplicables y riesgos tecnológicos, dirigida tanto a equipos técnicos como no técnicos.
- Campañas internas de sensibilización: Destinadas a destacar la importancia del cumplimiento en el uso de la IA y sus implicaciones para la reputación corporativa.
- Guías de uso para terceros: Extensión de las políticas internas a proveedores y socios, asegurando un enfoque homogéneo en toda la cadena de valor.

En todo caso, la implementación de Formación interna se ajustará siempre en función de las necesidades detectadas.

5. Seguimiento, auditoría y mejora continua

El seguimiento, la auditoría y la mejora continua son elementos clave para garantizar la efectividad y sostenibilidad del cumplimiento normativo en gobernanza de la IA. Las empresas deben implementar sistemas de monitorización continua que permitan identificar desviaciones, evaluar riesgos emergentes y garantizar el alineamiento con políticas internas y marcos regulatorios. Este seguimiento suele apoyarse en indicadores clave de desempeño (KPIs) y herramientas tecnológicas que facilitan la detección de anomalías o sesgos.

- Monitorización continua de los sistemas de IA: Implementación de herramientas automatizadas para la detección de comportamientos anómalos, sesgos emergentes o fallos de funcionamiento.
- Indicadores clave de desempeño (KPIs): Desarrollo de métricas específicas que permitan evaluar el cumplimiento de objetivos éticos y regulatorios, tales como niveles de transparencia, precisión y equidad.

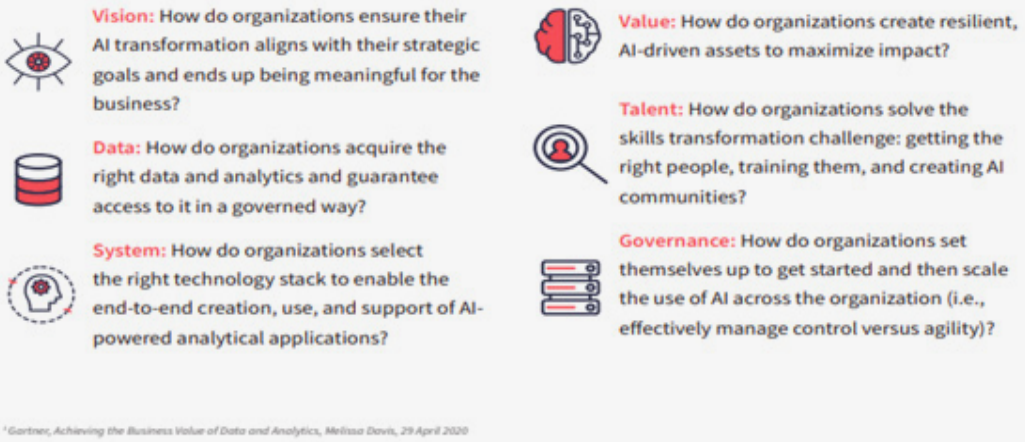
Las auditorías, tanto internas como externas, son esenciales para verificar el cumplimiento de las normativas y fortalecer la confianza. Estas revisiones no solo se centran en los procesos corporativos, sino también en aspectos técnicos como la robustez de los algoritmos y la seguridad de los datos. Además, el análisis de resultados de las auditorías sirve como base para

procesos de mejora continua, permitiendo ajustar políticas y estrategias en función de nuevos riesgos, avances tecnológicos o cambios normativos.

Se destaca a título de ejemplo revisión de la modelo llevada a cabo por parte del BCE: riesgos, trazabilidad, identificación de sesgos, control de errores, supervisión, etc. seguimiento, la auditoría y la mejora continua son componentes esenciales en la implementación de un sistema de cumplimiento normativo eficaz para la gobernanza de la inteligencia artificial (IA). Estos procesos permiten evaluar la efectividad de las políticas implementadas, identificar áreas de mejora y garantizar la adaptabilidad frente a un entorno tecnológico y regulatorio en constante evolución.

6. Transparencia

Finalmente, la transparencia juega un papel crucial. La elaboración de reportes accesibles y la divulgación de los resultados relevantes a partes interesadas, como reguladores y socios, refuerzan la confianza y el compromiso ético de las organizaciones. Estos esfuerzos, combinados con la adopción de estándares internacionales y certificaciones, aseguran una gobernanza adaptativa y resiliente en el uso de la IA.



[1] Gartner, Achieving the Business Value of Data and Analytics, Melissa Davis, 29 April 2020

En resumen, las organizaciones participantes han avanzado significativamente en la implementación de mecanismos de cumplimiento normativo en la gobernanza de la IA. Estos esfuerzos, si bien variados, se caracterizan por un enfoque holístico que combina políticas claras, estructuras internas sólidas y una constante revisión de riesgos y estrategias. Estos elementos son indispensables para construir una cultura organizativa comprometida con el uso ético y responsable de la IA.

5. Creación de roles

La implementación del Reglamento de Inteligencia Artificial exige a las organizaciones no solo adaptar sus sistemas y procesos, sino también estructurar sus equipos para garantizar el cumplimiento efectivo y sostenible en el tiempo. Este desafío demanda la creación de roles específicos y la identificación de stakeholders críticos que actúen como garantes del cumplimiento normativo, integrando perspectivas jurídicas, de privacidad y de seguridad corporativa.

En este sentido, es fundamental que las organizaciones promuevan un enfoque multidisciplinar, fomentando la colaboración entre áreas clave como la asesoría legal, los equipos de Compliance, los responsables de protección de datos y los especialistas en ciberseguridad, entre otros.

Además, como se ha comentado anteriormente, el establecimiento de grupos de trabajo transversales permite abordar de manera integral las implicaciones del reglamento en los procesos de desarrollo e implementación de sistemas de IA.

La transversalidad del impacto de la IA dentro de la organización deberá ser tenida en cuenta, considerando criterios de Eficiencia, para priorizar los eslabones críticos de nuestra Cadena de Valor desde el principio de cara a poder cumplir los requerimientos a largo plazo.

Por supuesto, la IA deberá reducir el tiempo requerido por la gestión documental, garantizando un entorno seguro, por lo que, de nuevo, la Formación y la sensibilización interna serán clave.

El horizonte temporal para el cumplimiento requiere un enfoque ágil y coordinado, asegurando que cada rol cumpla con sus responsabilidades específicas y que las sinergias entre disciplinas potencien el gobierno efectivo de la IA dentro de la organización.

Llegados a este punto, se revela necesaria la aparición de la figura del 'Responsable de IA'; figura que se erige como un pilar central en el marco del cumplimiento del Reglamento de Inteligencia Artificial, asumiendo un rol estratégico y operativo dentro de la organización, cuyo perfil deberá reunir las siguientes características generales:

- Conocimiento técnico y normativo: sólida comprensión de los sistemas de IA, su desarrollo y funcionamiento, así como profundo conocimiento de legislación aplicable, como el Reglamento de Inteligencia Artificial, privacidad y derechos fundamentales.

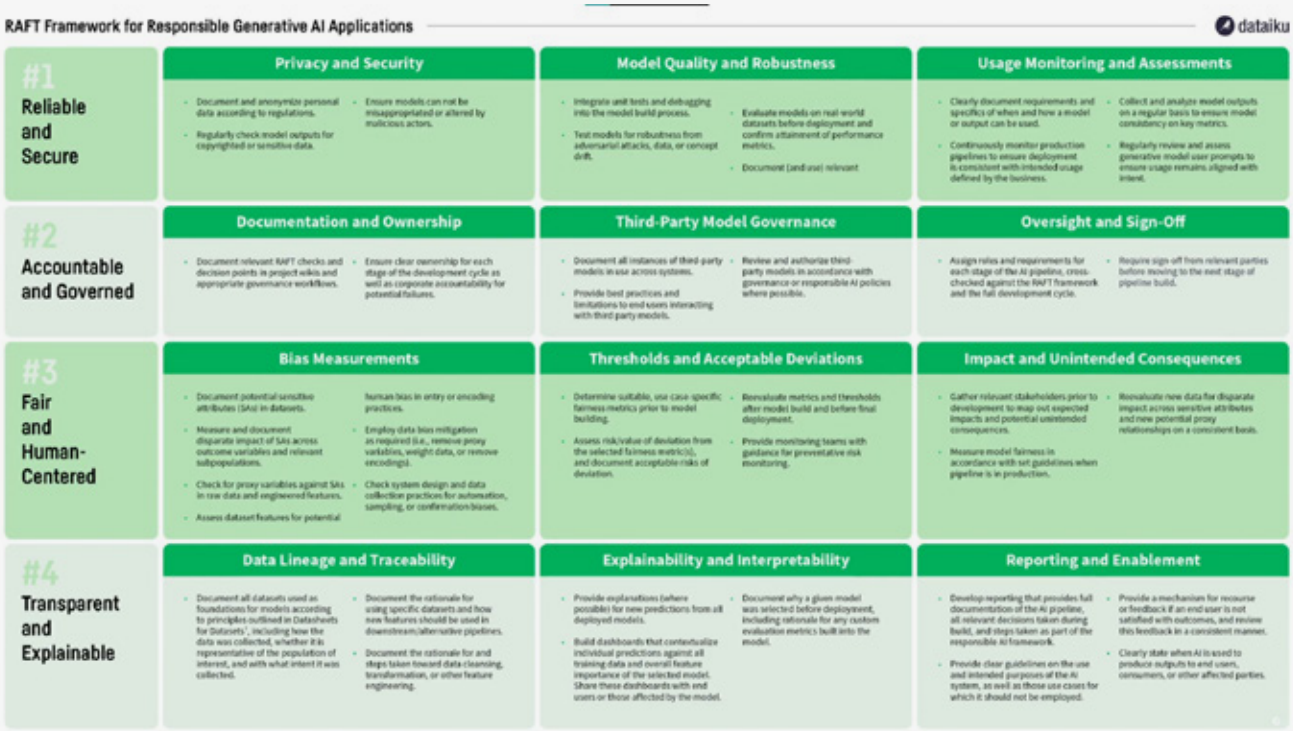
- Liderazgo y coordinación: capacidad para liderar equipos multidisciplinares (jurídico, privacidad, seguridad, TI), así como habilidad para gestionar proyectos complejos relacionados con el cumplimiento y la gobernanza de la IA.

- Visión estratégica: alinea el uso de la IA con los objetivos éticos, normativos y de negocio de la organización, así como fomentar una cultura de innovación responsable y sostenible. Asimismo, ha de tener la capacidad para poder definir el impacto en la estrategia corporativa mediante el análisis del dimensionamiento de la cobertura de responsabilidades para poder definir la estructura que será necesaria para este nuevo rol.

- Supervisión y evaluación: responsable de realizar evaluaciones de riesgos de los sistemas de IA, supervisión de auditorías internas y aplicación de medidas correctivas. Para ello, debido a la transversalidad del impacto aludido con anterioridad, con Privacy, CDO, DPO, y CTO, para poder identificar el impacto de los riesgos. Es importante que tenga un control y evitar la dispersión interna de modelos de IA.

- Transparencia y comunicación: actúa como punto de contacto con organismos reguladores y stakeholders externos, promueve la transparencia interna y externa sobre el uso y el impacto de la IA.

- Formación: fomentar la construcción de una Cultura Corporativa alineada con las necesidades detectadas. Para ello, aparte del lanzamiento de iniciativas de Formación interna, deberá liderar la utilización de Guías de Uso para los empleados.



Source: Data Iku

Este perfil, por tanto, requiere una visión integral que no solo aborde los aspectos técnicos y legales, sino también los estratégicos, asegurando que la IA sea un motor de innovación responsable y sostenible para la organización.

Para superar esta Fase Inicial, detallada en el presente documento, se deberá llevar a cabo una revisión del estado de las cosas en 2025.

6. Hacia la actualización e interpretación de guías y recomendaciones prácticas

La Unión Europea se posiciona como líder mundial en la regulación de la inteligencia artificial, marcando el camino con iniciativas legislativas pioneras y una visión clara hacia el desarrollo ético y responsable de esta tecnología. Las empresas están atentas a la publicación de guías prácticas, recomendaciones y circulares que faciliten la interpretación e implementación del marco normativo establecido por la Unión Europea y otras autoridades internacionales.

Mientras estas guías se formalizan, los comités internos de gobernanza deben asumir un rol estratégico como interlocutores únicos en la gestión de los proyectos relacionados con la IA. Téngase en cuenta que las multinacionales están exportando las políticas de regulación europeas a aquellos mercados donde aún no hay regulación.

Mientras esperamos a la publicación de las Guías, el Comité(s) de IA deberá:

- **Interlocutor único:** Los comités internos de IA deben actuar como punto de referencia central para la gestión de proyectos relacionados con inteligencia artificial, facilitando la alineación entre departamentos.
- **Identificación de requisitos normativos:** Su presencia en reuniones clave asegura una comprensión clara de los cumplimientos obligatorios y la anticipación a las exigencias regulatorias.
- **Elaboración de aspectos clave:** Estos comités son responsables de estructurar guías internas que incluyan los aspectos esenciales del cumplimiento normativo en cada proyecto.
- **Sinergia con la estrategia comercial:** Garantizan que las políticas de gobernanza y las estrategias empresariales vayan de la mano, transformando el cumplimiento normativo en una ventaja competitiva con el objetivo de ir de la mano con el Área de Estrategia Comercial para estar preparados de cara a los next steps: la adaptación a la nueva Regulación / Requerimientos, y a diferentes velocidades según el impacto que tenga en las operaciones de la compañía.

TABLE 1: MAPPING OF AI RMF TAXONOMY TO AI POLICY DOCUMENTS

AI RMF	OECD AI Recommendation	EU AI Act (Proposed)	EO 13960
Valid and reliable	Robustness	Technical Robustness	Purposeful and performance driven Accurate, reliable, and effective Regularly monitored
Safe	Safety	Safety	Safe
Fair and bias is managed	Human-centered values and fairness	Non-discrimination Diversity and fairness Data governance	Lawful and respectful of our Nation's values
Secure and Resilient	Security	Security & Resilience	Secure & Resilient
Transparent and accountable	Transparency and responsible disclosure Accountability	Transparency Accountability Human Agency and oversight	Transparent Accountable Lawful and respectful of our Nation's values Responsible and traceable Regularly monitored
Explainable and Interpretable	Explainability		Understandable by subject matter experts, users, and other, as appropiate
Privacy-enhanced	Human values; Respect for human rights	Privacy Data governance	Lawful and respectful of our Nation's values

Source : NIST AI RMF V2

7. Implantación de los proyectos

Enablers supporting every phase

Technology stack Provisioning the environment and tooling to optimize workflows	**Compliance, security, and risk** Establishing processes, governance, and tooling to control the AI system	**Assetization** Creating reusable components to increase efficiency and reduce risk	**People** Ensuring the right talent mix and operating model to execute best practices across the AI life cycle

Source: McKinsey

Los principales criterios clave para la implantación de proyectos de gobernanza de la IA son:

1. Asignación de presupuesto: Por un lado, evaluar los recursos necesarios para cumplir con los requisitos normativos y éticos, integrando el cumplimiento como una inversión estratégica en lugar de un coste adicional, así como priorizar recursos en función del nivel de riesgo, criticidad y beneficios potenciales de los sistemas de IA implementados.
2. Priorización por riesgos y criticidad del negocio: Identificar los casos de uso más críticos para el negocio y aquellos que representen mayores riesgos legales, éticos o reputacionales. Concentrar los esfuerzos iniciales en sistemas de IA con impacto directo en clientes, empleados o reguladores.
3. Impacto organizativo interno: Asegurar la colaboración interdepartamental, integrando áreas clave como legal, TI, compliance y operaciones en todas las fases del proyecto, así como considerar los cambios organizativos necesarios, como la creación de roles específicos (p.ej., AI Compliance Officer) o comités internos.
4. Criterios geográficos y regulatorios: Adaptar las políticas y la implementación a las normativas locales y regionales, especialmente en mercados donde se prevén regulaciones más estrictas, como la Unión Europea, y evaluar las diferencias regulatorias entre países para priorizar la adecuación en las geografías más relevantes para la operación de las empresas.
5. Adaptación a la cultura corporativa y sensibilización: Diseñar estrategias que alineen la gobernanza de la IA con los valores de la compañía, generando una cultura de cumplimiento y ética tecnológica, impulsar la formación y la comunicación para que todos los niveles de la organización comprendan y apoyen los objetivos del proyecto.
6. Incorporar estándares internacionales y certificaciones como herramientas para mantener la confianza y la competitividad.

Estos criterios proporcionan un marco práctico y adaptable para que las empresas aborden proyectos de gobernanza de IA, priorizando el cumplimiento normativo sin comprometer su operativa ni sus objetivos estratégicos.

Reliable and Secure	AI systems are built to ensure consistency and reliability across the entire lifecycle. Data and models are secure and privacy-enhacing.
Accountable and Governed	Ownership over each aspect of the AI lifecycle is documented and used to support oversight and control mechanisms.
Fair and Human-Centric	AI systems are built to minimize bias against individuals or groups and support human determination and choice.
Transparent and Explainable	The use of AI is disclosed to end users and explanations for the mothods, parameters and data used in AI systems are provided.

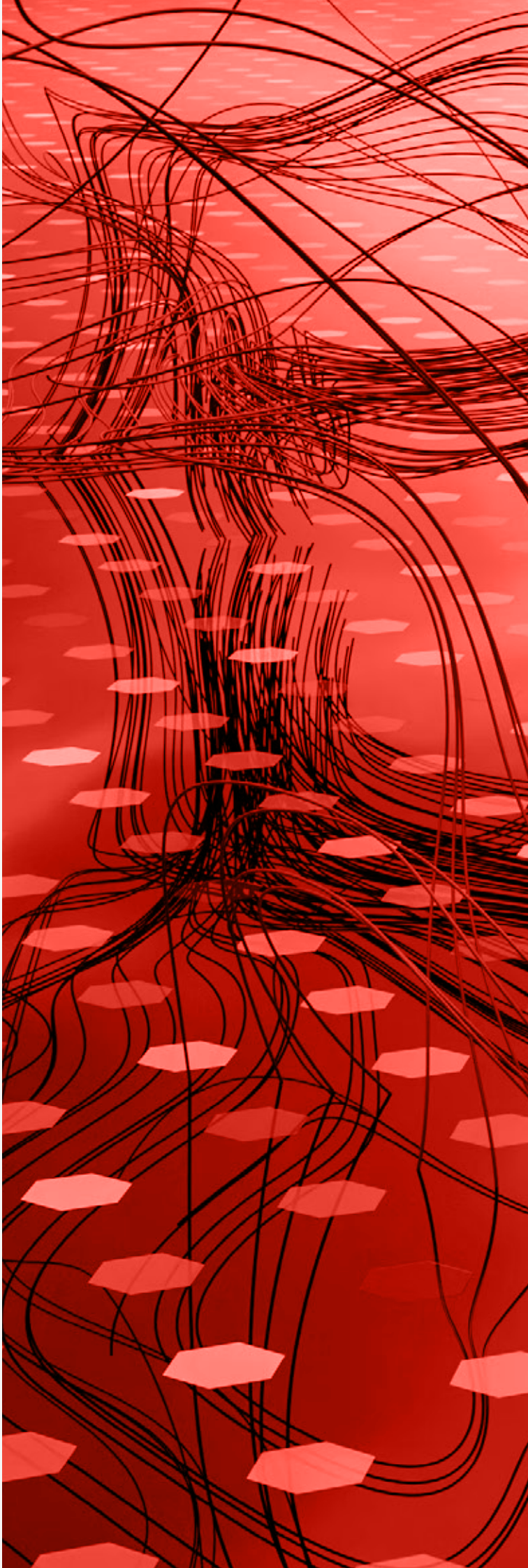
Source: McKinsey

Para finalizar, hay que destacar la opinión generalizada de que la aplicación de la IA aporta beneficios significativos a las organizaciones. La IA tiene el potencial de mejorar la eficacia de los procesos, optimizando tiempos, reduciendo errores y aumentando la productividad en áreas clave. Además, permite a las empresas adquirir nuevas capacidades, como el análisis predictivo, la personalización avanzada y la automatización inteligente, que generan ventajas competitivas en un entorno de mercado dinámico.

Estas tecnologías, implementadas de manera responsable, no solo impulsan la innovación, sino que también fortalecen la confianza de los stakeholders, creando un ecosistema más eficiente y sostenible.

El marco regulatorio no limita la innovación; la impulsa. Al proporcionar directrices claras y promover un uso ético de la IA, las organizaciones pueden desarrollar soluciones más avanzadas y confiables, fortaleciendo la competitividad y abriendo nuevas oportunidades de mercado en un entorno de confianza y sostenibilidad. Aunque la supervisión humana es siempre necesaria, sin duda es un motor para la innovación.

La clave del éxito en la gobernanza de la IA no es solo cumplir con la normativa, sino integrar el cumplimiento como un valor estrategico en la organización.



Agradecimiento

Han participado en el focus group de Compliance & IA del Observatorio IE – ECIJA de Derecho Digital los siguientes profesionales:

Irene Rodríguez Alonso	BBVA
Lucía Conde	Huawei Technologies
Pablo Salas	Iberdrola
Sergio Torné Goncer	ING España y Portugal
Miguel Retana	Mahou
Antonio Muñoz Marcos	Telefónica
Leticia Vitores	Banco Cooperativo
Paloma Esteban	Enagas
Diego Molero	Renfe
Cristina Cañas	Renfe
Martina Hoyos	CEGID
Elena del Tiempo	Microsoft
Celia Figuera	BNP Paribas
Elena Fraile	Iberdrola
Jesús Revaliente	Securitas Direct
Marta Campomanes	EMT Madrid
Rosana Viejo	BANKINTER
Elena Bernal	CAIXABANK
Sofia Serrat	SANTANDER
Chelo Borrás	BANESCO
Guerrero Vallecillo	Telecoming