

Gobierno de la IA

Cumplimiento, control y seguridad para una adopción responsable de la Inteligencia Artificial

La Inteligencia Artificial ya forma parte de la operativa de muchas organizaciones: asistentes generativos, automatización de procesos, modelos predictivos, herramientas integradas en SaaS, soluciones de RR. HH., análisis financiero, atención al cliente o desarrollo de software.

Pero su adopción también introduce nuevos riesgos: uso no autorizado de herramientas, falta de inventario, exposición de datos sensibles, sesgos, ausencia de supervisión humana, decisiones automatizadas sin trazabilidad o dependencia de proveedores externos.



Gobierna la IA. Reduce riesgos. Acelera la innovación con confianza.

Además, el marco regulatorio ya exige pasar de un uso experimental de la IA a un modelo gobernado, documentado y auditable. El Reglamento Europeo de Inteligencia Artificial establece obligaciones para sistemas de IA según su nivel de riesgo, con sanciones que pueden alcanzar hasta **35 millones de euros o el 7% del volumen de negocio mundial anual** en determinados incumplimientos.

Con el servicio de **Gobierno de la IA de Excelia**, ayudamos a las organizaciones a identificar, clasificar, controlar y supervisar sus sistemas de IA, alineando su uso con el Reglamento (UE) 2024/1689, ISO/IEC 42001, NIST AI RMF y las mejores prácticas de ciberseguridad aplicada a IA.

De la adopción de IA al control real

Muchas empresas ya están usando IA, pero no siempre saben:

- Qué sistemas de IA existen realmente en la organización.
- Cuáles son las herramientas que usan los empleados fuera de los canales aprobados.
- Datos que se están introduciendo en modelos generativos.
- Qué sistemas pueden considerarse de alto riesgo.
- Cuáles son las obligaciones que aplican como proveedor, integrador o responsable del despliegue.
- Evidencias que deben conservar ante una auditoría o revisión regulatoria.
- Cómo formar a los equipos para un uso seguro, responsable y conforme.



Cómo convertir el uso de IA en un sistema seguro y trazable

El servicio de Gobierno de la IA proporciona un marco operativo para gestionar la IA de forma segura, trazable y alineada con la regulación.

Diseñamos e implantamos una Oficina de Gobierno de IA que actúa como punto de control entre negocio, tecnología, ciberseguridad, legal, DPO, riesgos y dirección. Su objetivo es que la organización pueda adoptar IA con velocidad, pero sin perder control.

El servicio cubre tres grandes bloques:

1. Descubrimiento, clasificación y diagnóstico

Identificamos los sistemas de IA existentes, incluyendo herramientas aprobadas, soluciones integradas en SaaS, desarrollos internos y posibles usos de Shadow AI. Cada sistema se clasifica por nivel de riesgo y se analiza su rol regulatorio: proveedor, deployer/responsable del despliegue, integrador o usuario interno.

Incluye

- Inventario de sistemas de IA.
- Clasificación de riesgo por sistema.
- Identificación de usos prohibidos, alto riesgo, transparencia o riesgo mínimo.
- Mapa de exposición regulatoria.
- Gap analysis frente a EU AI Act, ISO/IEC 42001 y NIST AI RMF.

2. Framework de gobierno y cumplimiento

Definimos el marco documental, organizativo y operativo necesario para controlar el ciclo de vida de la IA. Trabajamos sobre un framework propio, **AI Governance Minimum Set**, formado por 12 controles de gobierno y 4 controles de capa de aplicación, mapeados contra EU AI Act, ISO/IEC 42001 y NIST AI RMF.

Incluye

- Política corporativa de uso aceptable de IA.
- Código ético y buenas prácticas.
- Registro de sistemas de IA.
- Procedimiento de evaluación predespliegue.
- Evaluación de riesgos por sistema.
- Gobierno y calidad de datos.
- Supervisión humana y transparencia.
- Documentación técnica y repositorio de evidencias.
- Procedimiento de incidentes de IA.
- Modelo de reporting a dirección.



3. Operación, control y mejora continua

La gobernanza de la IA no termina con una política. Necesita seguimiento, evidencias y revisión periódica. Por eso, planteamos un modelo operativo con revisión mensual de controles, KPIs medibles, comité operativo, reporting ejecutivo y evolución continua del marco de gobierno.

Incluye

- Seguimiento de riesgos abiertos, mitigados y aceptados.
- Revisión de sistemas nuevos o modificados.
- Control de evidencias.
- Reporting periódico.
- Vigilancia regulatoria.
- Soporte a auditoría ISO/IEC 42001.
- Mejora continua del sistema de gestión de IA.



Roadmap de implantación

Planteamos un recorrido progresivo que permite empezar por el diagnóstico y avanzar hacia una operación continua de la IA.

Fase 1

Assessment

Inventario de sistemas de IA, clasificación de riesgos, identificación de roles regulatorios, análisis de brechas y plan de acción priorizado.

Fase 2

Implantación

Desarrollo del marco normativo, políticas, registros, evaluación de riesgos, controles de supervisión humana, transparencia, calidad de datos e integración con sistemas de gestión existentes.

Fase 3

Operación

Revisión mensual de controles, gestión de incidentes, reporting ejecutivo, vigilancia regulatoria, repositorio de evidencias y preparación para auditoría ISO/IEC 42001.

Beneficios clave

Cumplimiento demostrable

Convierte las obligaciones regulatorias en controles, evidencias y procedimientos verificables.

Reducción del riesgo operativo y reputacional

Ayuda a prevenir incidentes derivados de fugas de datos, sesgos, decisiones automatizadas opacas o falta de supervisión.

Preparación para ISO/IEC 42001

Facilita la evolución hacia un Sistema de Gestión de IA estructurado y auditable.

Visibilidad sobre el uso real de IA

Permite identificar sistemas, herramientas, proveedores y usos no autorizados dentro de la organización.

Integración con ciberseguridad y compliance

Alinea gobierno de IA, SGSI, privacidad, DPO, legal, riesgos, SOC y dirección.

Acompañamiento experto

Combinamos capacidades de gobierno, riesgo, cumplimiento, ciberseguridad, operaciones y seguridad ofensiva aplicada a IA.

Servicios incluidos

- AI Discovery & Classification.
- AI Gap Analysis & Roadmap.
- AI Governance Framework.
- Conformity Assessment.
- ISO/IEC 42001 Readiness.
- FRIA / DPIA integrada.
- AI Literacy & Training.
- AI Third-Party Risk Management.
- Gobierno de proveedores de IA.
- Repositorio de evidencias.
- Reporting ejecutivo.
- Vigilancia regulatoria
- Soporte a comités de gobierno.
- Integración con controles de ciberseguridad.



Por qué Excelia

Enfoque end-to-end

Integramos cumplimiento, riesgo, ciberseguridad y operación continua en un único modelo de Gobierno de la IA.

Experiencia tecnológica y regulatoria

Combinamos conocimiento normativo, ciberseguridad, Cloud, datos, gestión de riesgos y transformación digital.

Framework propio

Trabajamos con un modelo de controles orientado a evidencias, KPIs y seguimiento continuo.

Integración con estructuras existentes

La Oficina de Gobierno de IA puede integrarse con SGSI, DPO, CISO, comités de riesgos, legal, IT, seguridad y áreas de negocio.

Presencia internacional

Excelia cuenta con más de 25 años de experiencia, oficinas propias en 9 países y presencia en más de 50 mercados.

