El reto de la Inteligencia Artificial en la Era Digital. Innovación, ética y responsabilidad.

AENOR

¿Qué está sucediendo?

- En 2028, la IA representará el **29% del gasto corporativo**.
- Hasta 2027 los CIO y proveedores de servicios de TI esperan **destinar el 50%** de recursos de I+D para inversiones de TI en **Inteligencia Artificial y automatización**.

*"Todas las aplicaciones y **servicios** serán más inteligentes..., pero asegúrese de **no ser redundante**".*

Presidente de IDC, Crawford Del Prete.

Los datos: su impacto en la sociedad.

El dato es un activo muy **valioso**:

- **Toma de decisiones** de manera oportuna y segura.
- **Mejora los procesos** de producción.
- Crea ó mejora **modelos de negocio, productos o servicios**.

*“El amplio potencial de las **tecnologías y los Sistemas de Información** que les dan soporta”.*

El dato es un **recurso estratégico**, considerando:

- la **ética** y la defensa de los **derechos digitales**.
- Incremento del **valor** en la gestión y almacenamiento de los **datos**.
- la inteligencia de los datos dando paso al momento actual: la **inteligencia artificial**.

¿Y cómo podemos **mitigar** los riesgos en la Tecnologías?
¿Podemos **gestionar riesgos** en la IA?¿**Hay solución**?

AENOR

Ecosistema Digital de AENOR: soluciones a los riesgos tecnológicos

Cuestiones a considerar por el Comité de Direccion y del CIO en la actual era digital

¿Está integrado mi plan de TIC con mi plan estratégico de compañía?

¿Estoy preparado para dar servicios de TI?

¿Son los datos fiables para hacer BI - IA?

¿Se conocen y gestionan los ciberriesgos y las ciberamenazas que puedan afectar a mi organización?

Riesgos en Continuidad de Negocio (ISO 22301)

- Desaparición de la empresa. Después de un desastre natural, o provocado, o negligencia. Pandemias
- No existe resiliencia ante un desastre o incidentes graves
- No se identifican procesos y/o proveedores críticos.

Riesgos en Ciberseguridad y Cloud (ISO 27001 - ISO 27701 - ENS - 27017/27018)

- Perdida de integridad en la información.
- Pérdida de Disponibilidad/contingencia (ciberresiliencia)
- Suplantación de identidad/Mal uso de roles.

Riesgos en Servicios TI (ISO 20000-1)

- Pérdida de Disponibilidad/contingencia (ciberresiliencia)
- Servicios de TI no definidos, sin compromiso
- Incumplimiento de los SLAs (Acuerdos de nivel de servicio).

AENOR

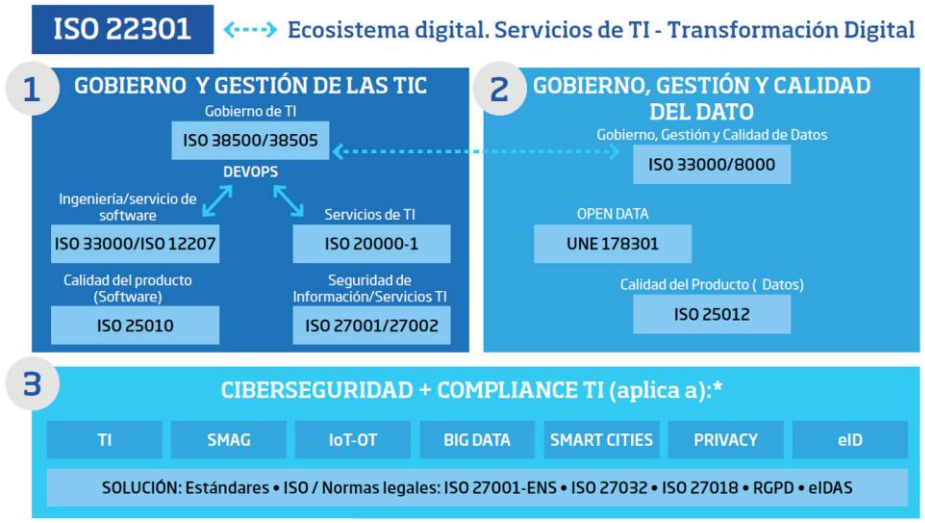
Diseño de soluciones basadas en consenso internacional para IA

INTELIGENCIA ARTIFICIAL

WORLD ECONOMIC FORUM

La confianza es la piedra angular de la Ley de Inteligencia Artificial de la UE - De esto se trata

5 abr 2023



Fuente: AENOR TIC

NORMAS ISO SOBRE IA / CONSENSO INTERNACIONAL

- **ISO/IEC 22989:2022 -** Artificial intelligence concepts and terminology
- **ISO/ IEC 42001** – Artificial Intelligence Management System
- **ISO/IEC 23894:2023 -** Guidance on risk management
- **ISO/IEC 23053** -Framework for Artificial Intelligence(AI) Systems Using Machine Learning (ML)
- **ISO/IEC TR 24368 –** Aspectos Sociales y Éticos en la IA.

Calidad del Software (algoritmos)&Data

- Procesos (ISO 12207 / ISO 5338).
- Producto (ISO 25010 / ISO 25012 / ISO 25059).

AENOR

ISO/IEC 42001 – Gestión de IA

OBJETIVO.

Garantizar que los sistemas, productos y servicios de IA se desarrollan, implantan y utilizan sean:

Fiables: capaces de realizar sus tareas de forma precisa y consistente. Que sean coherentes e íntegras. (IA generativa)

Transparentes: comprensibles y explicables para los usuarios y las partes interesadas. (IA explicativa).

Responsables: utilizados de forma que se minimice el riesgo de daños o perjuicios a las personas o al entorno.

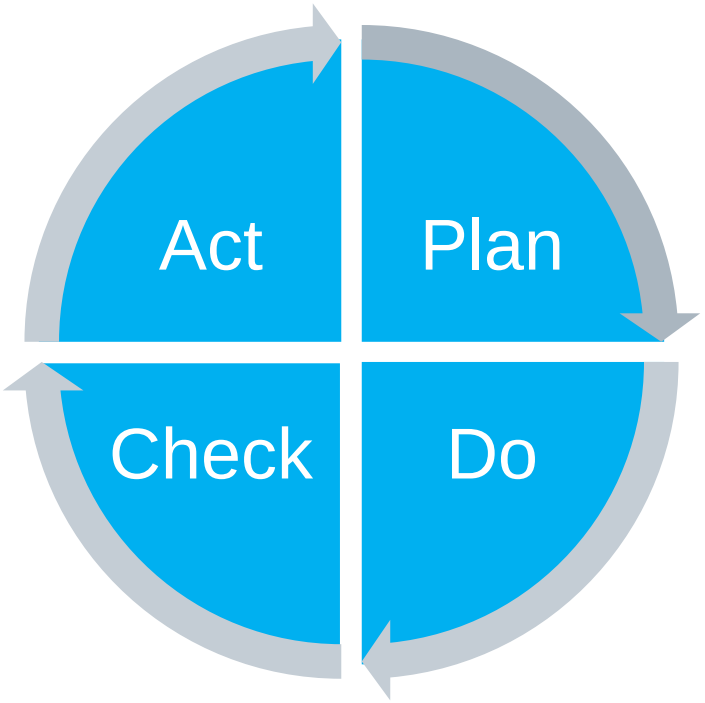
AENOR

Gestión de la Inteligencia Artificial – ISO/IEC 42001 (SGIA)

OBJETIVO

Garantizar que los sistemas, productos y servicios de IA se desarrollan, implantan y utilizan de forma fiable, transparente y responsable.

Ciclo de Mejora Continua - PDCA



- 4. CONTEXTO DE LA ORGANIZACIÓN
- 5. LIDERAZGO
- 6. PLANIFICACION
- 7. SOPORTE
- 8. OPERACIÓN
- 9. EVALUACIÓN DEL DESEMPEÑO
- 10. MEJORA

ANEXOS

ANEXO A. OBJETIVOS DE CONTROL Y CONTROLES
A1. GENERAL
A2. POLITICAS RELACIONADAS CON LA IA
A3. ORGANIZACIÓN INTERNA
A4. RECURSOS PARA SISTEMAS DE IA
A5. EVALUACION DE IMPACTO EN SISTEMAS IA
A6. CICLO DE VIDA DE UN SISTEMA IA
A7. DATOS PARA SISTEMAS IA
A8. INFORMACION PARA LAS PARTES INTERESADA DE SISTEMAS IA
A9. USO DE SISTEMAS IA
A10. RELACION DE TERCERAS PARTES Y CLIENTES
ANEXO B. GUIA DE IMPLANTACION PARA CONTROLES DE IA
ANEXO C. OBJETIVOS Y POTENCIALES FUENTES DE RIESGO EN IA
ANEXO D. USO DE UN SGIA EN DISTINTOS AMBITOS O SECTORES

Gestión ética de la Inteligencia Artificial – ISO/IEC 42001 + ISO/IEC TR 24368

ISO/IEC 42001 – Sistema de Gestión de la IA

Elementos clave:

- **Inventario** de los sistemas de IA (casos de uso)
- Políticas y **Código Ético** en Sistemas de IA
- Mapa de **Riesgos** del Sistema de IA
- Definición de **órganos y mecanismos de control** que minoran los riesgos del Sistema IA
- Gestión de toda la **cadena de valor** de la IA

ISO/IEC TR 24368 – Aspectos Sociales y Éticos en la IA

Principios sociales y éticos

(resumen: 7 de 14):

- Diseño centrado en los valores humanos
- Equidad y no discriminación
- Privacidad y seguridad
- Transparencia y *explicabilidad*
- Supervisión humana
- Responsabilidad

Ej. casos de uso en:

- *Chatbots (At. Cliente)*
- Vehículos autónomos
- *Credit scoring* / Cribado de talento
- Análisis de comportamientos / sentimientos
- Procesos jurídicos

RIA – Reglamento (Europeo) de Inteligencia Artificial

Marco Jurídico y aplicabilidad

Proporciona un marco jurídico uniforme, basado en riesgos pare el desarrollo y uso de sistemas de IA en la UE:

- Promueve una IA **fiable y centrada** en la integridad del ser humano.
- Garantiza la **libre circulación** transfronteriza de mercancías y servicios basados en la IA.
- **AESIA** asume un rol similar a la AEPD en materia de modelos y sistemas de IA.

Tipología IA:

- Sistemas de IA.
- Sistemas de IA de propósito general.
- Modelos de IA de propósito general.

Roles en IA

- Proveedor.
- Responsable del despliegue.
- Distribuidor.
- Importador.
- Representante autorizado.
- Fabricante.

Nivel de Riesgo (Sistemas de IA)

- Prohibidos / Inaceptables.
- Alto Riesgo.
- Limitado.
- Mínimo.

Riesgos en IA

Reglamento Europeo de IA

CASOS DE USO (No exhaustivo)	RIESGOS	CONSECUENCIAS
▪ Identificación biométrica en tiempo real ▪ Puntuación por comportamiento social ▪ …	**Riesgo inaceptable**	PROHIBICIÓN
▪ Acceso al empleo (“sesgo en recruiting”) ▪ Aplicación de la ley y vigilancia penitenciaria ▪ …	**Riesgo alto**	OBLIGACIÓN DE REGISTRO Y VERIFICACIÓN INDEPENDIENTE DE LA CONFORMIDAD
▪ Atención al cliente (Chatbots) ▪ Contenido generado por IA / Deepfakes ▪ …	**Riesgo limitado**	OBLIGACIÓN DE TRANSPARENCIA
▪ Desarrollo de software ▪ Filtros de emails/spam ▪ …	**Riesgo mínimo**	SIN OBLIGACIONES PARTICULARES

Ciberseguridad / Privacidad

* Fuente: Comisión Europea

Estas directrices exigen la gestión de los riesgos desde 2/2/25,

AENOR

Conclusiones

GarantIAs a través de estándares internacionales, alineados al Reglamento Europeo de IA

Ante los escenarios y desafíos como lo es la inteligencia artificial, la normas/estándares, permitirán:

1. disponer de una herramienta muy potente para la **gestión adecuada** de los **sistemas, productos y servicios** de IA.
2. basada en la gestión de **riesgos, aplicación de controles y mejora continua**.
3. garantizando **fiabilidad, transparencia y responsabilidad,** con ética y seguridad.

Así, las organizaciones que incorporen en su **estrategia la IA**, deberán:

- Considerar a sus *stakeholders*, sus objetivos, y el **difícil equilibrio entre:** innovar, riesgos y beneficios.
- Concienciar y capacitar a los empleados, determinando **posibles nuevas habilidades** y conocimientos.
- Invertir en la formación de los empleados para aprovechar el potencial de esta tecnología: que **no sea una amenaza** sino una oportunidad. **Productividad y eficiencia.**
- Adoptar un enfoque **responsable y ético**, con garantías de (ciber) seguridad y privacidad.

Gracias

Boris Delgado Riss. CISA, CISM
Director de Industria y TIC
AENOR
bdelgado@aenor.com

AENOR