



Compliance Officers

INTELIGENCIA ARTIFICIAL EN LA FRONTERA CON LA INTEGRIDAD

Iván Martínez López
imartinez@worldcomplianceassociation.com

25 sept 2024

www.worldcomplianceassociation.com

The ABC's of COMPLIANCE MONSTERS!



CORRUPCIÓN



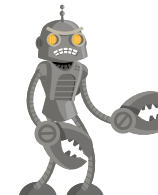
SOBORNO



TRÁFICO DE
INFLUENCIAS



COLUSIÓN



INTELIGENCIA
ARTIFICIAL



MARCO
REGULATORIO



FRAUDE
INTERNO



TRIBUTARIO



PRÁCTICAS
ANTICOMPETITIVAS



CONFLICTO DE
INTERESES



PRIVACIDAD Y
DATOS PERSONALES



CIBER
SEGURIDAD



DERECHOS DE LOS
CONSUMIDORES



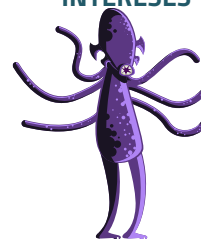
EQUIDAD



RESPONSABILIDAD
PENAL



SEGURIDAD



PROPIEDAD
INTELLECTUAL



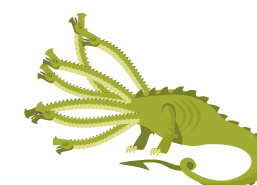
SOCIAL



DERECHOS
LABORALES



LAVADO DE DINERO



MEDIO
AMBIENTE

Riesgos emergentes... la Inteligencia Artificial



elEconomista.es

MERCADOS Y COTIZACIONES

IBEX 35

M.CONTINUO

EMPRESAS

ECONOMÍA

VIVIENDA

OPINIÓN

MÁS LEÍDAS

Tecnología

Estafa maestra con Inteligencia Artificial: suplantan al CEO y varios empleados en una videollamada para robar cientos de millones

* Todas las personas que aparecieron en la llamada en realidad eran bots impulsados por IA

* A pesar de conocer a las personas, no supo distinguir que no eran reales



Riesgos emergentes... la Inteligencia Artificial



LA VANGUARDIA

Economía

BOJILLO / DINERO / FINANZAS PERSONALES / EMPRENDEDORES / INNOVACIÓN / LEGAL / CONSORCIO

EL USO DE LAS NUEVAS TECNOLOGÍAS

Competencia usa la IA para perseguir cárteles en las licitaciones públicas

- Su nueva herramienta ya explora contratos del Estado y las comunidades autónomas



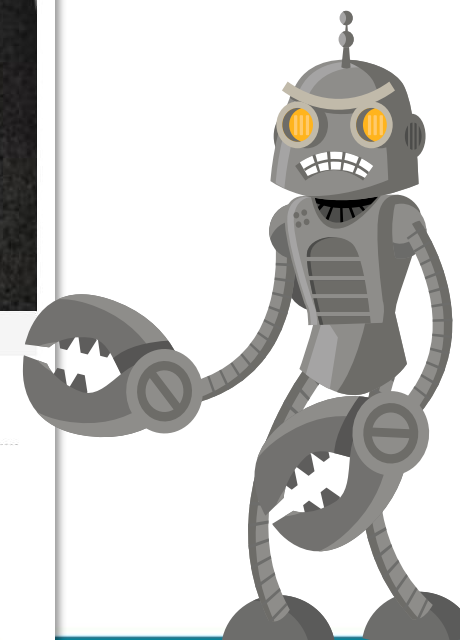
Sede de la CNMC, en Madrid (Emilia Gutiérrez)



Iñaki de las Heras
Madrid

21/09/2024 06:00 | Actualizado a 21/09/2024 09:42

La Comisión Nacional de los Mercados y la Competencia (CNMC) está recurriendo a la inteligencia artificial para rastrear todas las licitaciones públicas del Estado, las comunidades autónomas y los ayuntamientos con el objetivo de detectar patrones sospechosos y posibles casos de colusión.



“ Compliance tendrá la responsabilidad de asegurar que los sistemas de IA cumplan con estándares éticos, de transparencia, de seguridad y privacidad”



EU AI Act (Reglamento (UE) 2024/1689)



¿Es mi sistema un "sistema de IA" según la Ley de IA de la UE?

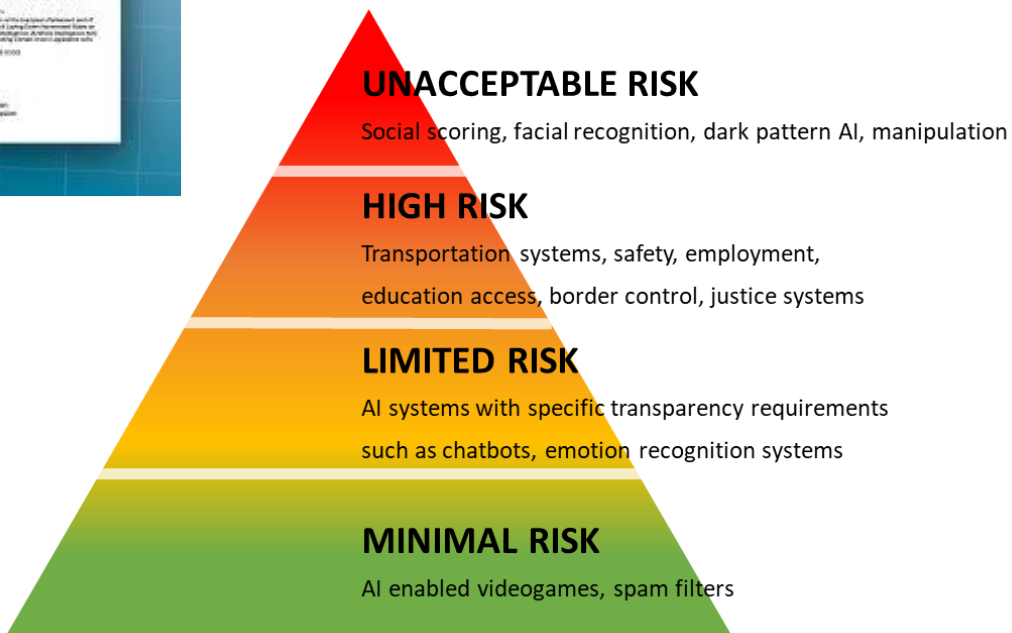
<https://artificialintelligenceact.eu/assessment/eu-ai-act-compliance-checker/>



- 01 La Ley de IA de la UE es vista como un referente global en cuanto a la regulación de la inteligencia artificial. Establece un marco integral para **equilibrar la innovación tecnológica con la protección de los derechos de los ciudadanos**, posicionando a la UE como líder en la regulación ética de la IA. Además, se espera que inspire legislaciones similares en otras regiones del mundo.
- 02 Este enfoque preventivo y **basado en riesgos** marca un hito importante en la relación entre la tecnología avanzada y la legislación, con el objetivo de construir un entorno seguro y confiable para el despliegue de IA.
- 03 El área de compliance relacionada con la inteligencia artificial (IA) está emergiendo como una de las más prometedoras a medida que entran en vigor regulaciones como la Ley de IA de la Unión Europea (AI Act) y otros marcos normativos a nivel global. Las oportunidades en materia de compliance para empresas e instituciones que operan en el campo de la IA son variadas y crecientes, especialmente debido a la necesidad de asegurar que los **sistemas de IA cumplan con estándares éticos, de transparencia, privacidad y de seguridad**.

Un sistema de inteligencia artificial (sistema IA) se define como: Un sistema basado en máquinas diseñado para operar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras su despliegue y que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales.

EU AI Act (Reglamento (UE) 2024/1689)



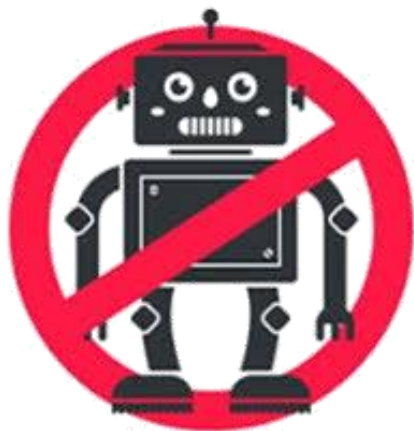
- ➔ **Riesgo inaceptable:** Se prohíben los sistemas de IA que presenten un riesgo significativo para los derechos fundamentales y la seguridad de las personas. Ejemplos incluyen el uso de IA para manipular el comportamiento humano o sistemas de vigilancia masiva con IA.
- ➔ **Alto riesgo:** Se incluyen en esta categoría los sistemas de IA que impactan áreas críticas como infraestructuras, educación, empleo, servicios financieros, y acceso a la justicia. Estos sistemas estarán sujetos a estrictos controles, auditorías, y requisitos de transparencia.
- ➔ **Riesgo limitado:** Se incluyen aquí los sistemas de IA que interactúan con los usuarios, como chatbots. Estos deben cumplir con ciertas obligaciones de transparencia para que los usuarios sepan que están interactuando con una IA.
- ➔ **Riesgo mínimo o nulo:** En esta categoría caen las aplicaciones de IA con bajo impacto, como los filtros de spam. No están sujetas a regulación estricta, pero deben seguir ciertas buenas prácticas.



EU AI Act (Reglamento (UE) 2024/1689)

SISTEMAS PROHIBIDOS

1. **Despliegue de técnicas subliminales, manipuladoras o engañosas** para distorsionar el comportamiento y perjudicar la toma de decisiones con conocimiento de causa, causando un daño significativo.
2. **Explotar las vulnerabilidades** relacionadas con la edad, la discapacidad o las circunstancias socioeconómicas para distorsionar el comportamiento, causando daños significativos.
3. **Sistemas de categorización biométrica que infieran atributos sensibles** (raza, opiniones políticas, afiliación sindical, creencias religiosas o filosóficas, vida sexual u orientación sexual), excepto el etiquetado o filtrado de conjuntos de datos biométricos adquiridos legalmente o cuando las fuerzas de seguridad categoricen datos biométricos.
4. **Puntuación social**, es decir, evaluar o clasificar a individuos o grupos basándose en comportamientos sociales o rasgos personales, causando un trato perjudicial o desfavorable a esas personas.
5. **Evaluar el riesgo de que un individuo cometa delitos penales** basándose únicamente en perfiles o rasgos de personalidad, excepto cuando se utilice para aumentar las evaluaciones humanas basadas en hechos objetivos y verificables directamente relacionados con la actividad delictiva.
6. **Compilación de bases de datos de reconocimiento facial** mediante el raspado no selectivo de imágenes faciales de Internet o de grabaciones de CCTV.
7. **Inferir emociones en lugares de trabajo o centros educativos**, salvo por razones médicas o de seguridad.
8. **Identificación biométrica remota** (RBI) "en tiempo real" en espacios de acceso público para las fuerzas de seguridad excepto: búsqueda de personas desaparecidas, víctimas de secuestros y personas víctimas de la trata de seres humanos o la explotación sexual; prevenir una amenaza sustancial e inminente para la vida, o un ataque terrorista previsible; o identificar a sospechosos de delitos graves (por ejemplo, asesinato, violación, robo a mano armada, tráfico de estupefacientes y armas ilegales, delincuencia organizada y delitos contra el medio ambiente, etc.).





EU AI Act (Reglamento (UE) 2024/1689)

REQUISITOS PARA SISTEMAS DE ALTO RIESGO

Los desarrolladores de IA de alto riesgo deben seguir criterios estrictos antes de comercializar sus productos en la UE, como:

- **Establecer un sistema de gestión de riesgos a lo largo del ciclo de vida del sistema de IA de alto riesgo;**
- **Llevar a cabo la gobernanza de los datos, garantizando que los conjuntos de datos de formación, validación y prueba sean pertinentes, suficientemente representativos y, en la medida de lo posible, estén libres de errores y completos de acuerdo con la finalidad prevista.**
- **Elaborar documentación técnica para demostrar la conformidad y facilitar a las autoridades la información necesaria para evaluar dicha conformidad.**
- **Diseñar su sistema de Inteligencia Artificial de alto riesgo para que pueda registrar automáticamente los eventos relevantes para identificar los riesgos a nivel nacional y las modificaciones sustanciales a lo largo del ciclo de vida del sistema.**
- **Proporcionar instrucciones de uso a los encargados de la implantación posterior para permitir el cumplimiento por parte de estos últimos.**
- **Diseñar su sistema de IA de alto riesgo para permitir a los desplegados aplicar la supervisión humana.**
- **Diseñar su sistema de IA de alto riesgo para alcanzar los niveles adecuados de precisión, solidez y ciberseguridad.**
- **Establecer un sistema de gestión de la calidad para garantizar el cumplimiento.**

TRANSPARENCIA Y DERECHOS DEL USUARIO

- **Los usuarios deben ser informados si están interactuando con un sistema de IA.**
- **Se prohíben ciertos usos de IA que comprometan la privacidad o que no respeten los derechos humanos, como el reconocimiento facial en espacios públicos sin una base legal clara.**

- **Multas administrativas:**
 - Hasta el 6% de los ingresos anuales globales: En caso de infracciones graves, como la implementación y uso de IA prohibida o el incumplimiento de los requisitos de alto riesgo.
 - Hasta el 4% de los ingresos anuales globales: En caso de falta de cooperación con las autoridades competentes o incumplimiento de las obligaciones relacionadas con los sistemas de IA de alto riesgo.
 - Hasta 2% de los ingresos anuales globales: Para infracciones menos graves, como no reportar correctamente los incidentes a las autoridades o no llevar a cabo las evaluaciones de conformidad.
- **Órdenes de suspensión o prohibición:** Las autoridades pueden ordenar la suspensión temporal o permanente del uso de ciertos sistemas de IA hasta que se rectifique el incumplimiento.
- **Retirada del mercado:** Los productos y servicios de IA que violen las disposiciones del reglamento podrían ser retirados del mercado europeo.

Objetivos para el compliance Officer en materia de gestión de la IA

Responsabilidad

Experiencia
en IA

Disponibilidad
y calidad de los
datos de
entrenamiento
y prueba

Impacto
ambiental

Equidad

Mantenibilidad

Equidad

Privacidad

Robustez

Seguridad

Transparencia y
explicabilidad

Gestión de la IA en organizaciones

- ➔ **Requisitos y orientación** para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de IA (inteligencia artificial) dentro del contexto de una organización.
- ➔ **Destinado a** ser utilizado por una organización que proporciona o utiliza productos o servicios que utilizan sistemas de IA manera responsable para lograr sus objetivos y cumplir con los requisitos aplicables.

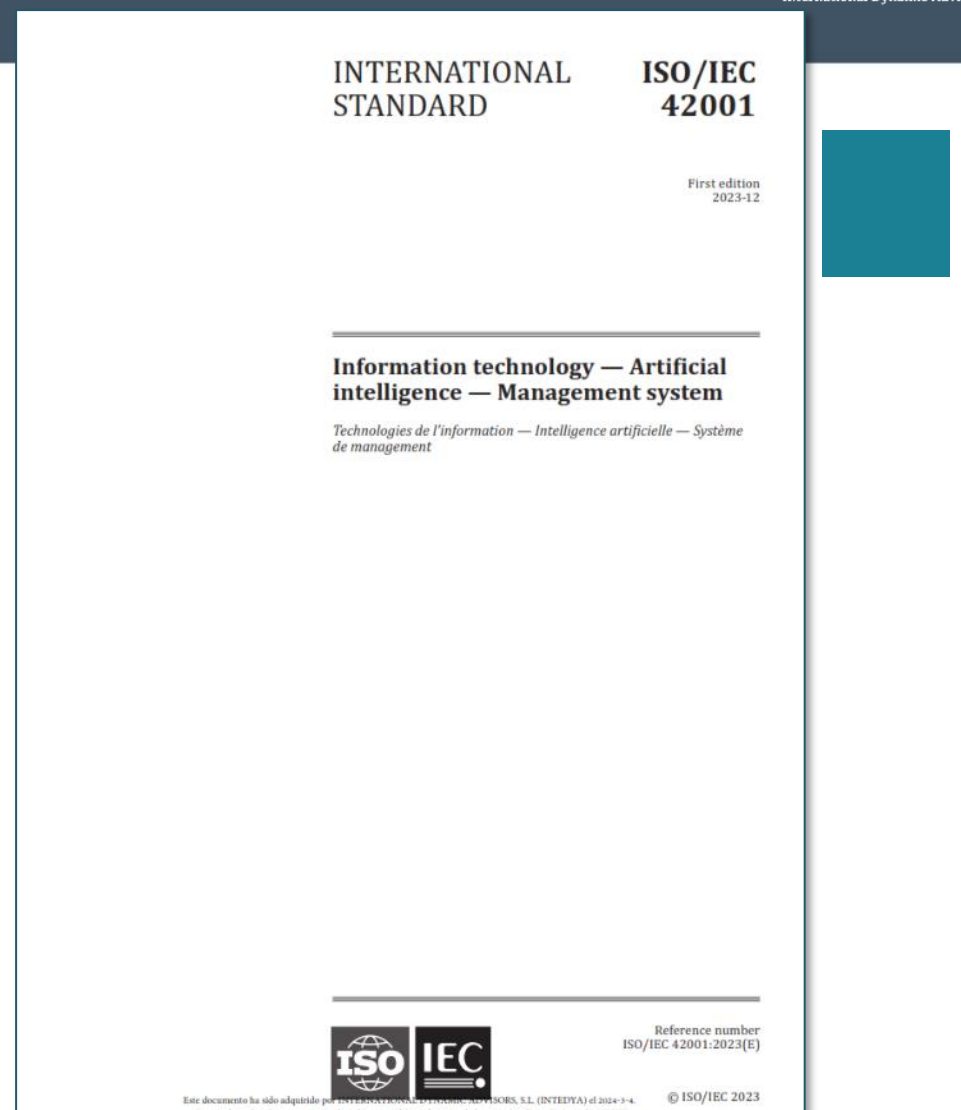
Estructura de Alto Nivel

+

Norma Tipo A

+

ANEXOS



Gestión de la IA en organizaciones

INTERNATIONAL
STANDARD

ISO/IEC
42001

First edition
2023-12

Information technology — Artificial intelligence — Management system

Technologies de l'information — Intelligence artificielle — Système
de management

ANEXO A: Objetivos de control y controles



Reference number
ISO/IEC 42001:2023(E)

Este documento ha sido adquirido por INTERNACIONAL COMPLIANCE ASSOCIATION, S.L. (INTEDYA) el 2024-3-4.
Este puede utilizarse en un sistema de control interno, de gestión, de cumplimiento de la legislación o de otro tipo.

© ISO/IEC 2023

A.2 Políticas relacionadas con la IA

Objetivo: Proporcionar dirección de gestión y soporte para los sistemas de IA de acuerdo con los requisitos del negocio.

	Tema	Control
A.2.2	Política de IA	La organización deberá documentar una política para el desarrollo o uso de sistemas de IA.
A.2.3	Alineación con otras políticas organizacionales	La organización deberá determinar dónde otras políticas pueden verse afectadas o aplicarse a los objetivos de la organización con respecto a los sistemas de IA.
A.2.4	Revisión de la política de IA	La política de IA se revisará a intervalos planificados o adicionalmente según sea necesario para garantizar su idoneidad, adecuación y eficacia continuas.

A.3 Organización interna

Objetivo: Establecer responsabilidad dentro de la organización para defender su enfoque responsable para la implementación, operación y gestión de los sistemas de IA.

	Tema	Control
A.3.2	Roles y responsabilidades de la IA	Las funciones y responsabilidades de la IA se definirán y asignarán de acuerdo con las necesidades de la organización.
A.3.3	Informe de inquietudes	La organización deberá definir e implementar un proceso para informar inquietudes sobre el papel de la organización con respecto a un sistema de IA a lo largo de su ciclo de vida.

A.4 Recursos para sistemas de IA

Objetivo: Garantizar que la organización rinda cuentas de los recursos (incluidos los componentes y activos del sistema de IA) del sistema de IA para comprender y abordar completamente los riesgos e impactos.

	Tema	Control
A.4.2	Documentación de recursos	La organización debe identificar y documentar los recursos relevantes necesarios para las actividades en determinadas etapas del ciclo de vida del sistema de IA y otras actividades relacionadas con la IA relevantes para la organización.
A.4.3	Recursos de datos	Como parte de la identificación de recursos, la organización deberá documentar información sobre los recursos de datos utilizados para el sistema de IA.
A.4.4	Recursos de herramientas	Como parte de la identificación de recursos, la organización deberá documentar información sobre los recursos de herramientas utilizados para el sistema de IA.

Gestión de la IA en organizaciones

A.4.5	Sistema y recursos informáticos	Como parte de la identificación de recursos, la organización deberá documentar información sobre el sistema y los recursos informáticos utilizados para el sistema de IA.
A.4.6	Recursos humanos	Como parte de la identificación de recursos, la organización deberá documentar información sobre los recursos humanos y sus competencias utilizadas para el desarrollo, implementación, operación, gestión de cambios, mantenimiento, transferencia y desmantelamiento, así como la verificación e integración del sistema de IA.
A.5 Evaluación de los impactos de los sistemas de IA		
Objetivo: Evaluar los impactos del sistema de IA en individuos o grupos de individuos, o ambos, y en las sociedades afectadas por el sistema de IA a lo largo de su ciclo de vida.		
	Tema	Control
A.5.2	Proceso de evaluación del impacto del sistema de IA	La organización deberá establecer un proceso para evaluar las posibles consecuencias para individuos o grupos de individuos, o ambos, y sociedades que pueden resultar del sistema de IA a lo largo de su ciclo de vida.
A.5.3	Documentación de evaluaciones de impacto del sistema de IA	La organización deberá documentar los resultados de las evaluaciones de impacto del sistema de IA y conservar los resultados durante un período definido.
A.5.4	Evaluación del impacto del sistema de IA en individuos o grupos de individuos	La organización deberá evaluar y documentar los impactos potenciales de los sistemas de IA en individuos o grupos de individuos a lo largo del ciclo de vida del sistema.
A.5.5	Evaluación de los impactos sociales de los sistemas de IA	La organización deberá evaluar y documentar los posibles impactos sociales de sus sistemas de IA a lo largo de su ciclo de vida.
A.6 Ciclo de vida del sistema de IA		
A.6.1 Orientación de gestión para el desarrollo de sistemas de IA		
Objetivo: Garantizar que la organización identifique y documente objetivos e implemente procesos para el diseño y desarrollo responsable		
	Tema	Control
	Objetivos para el desarrollo responsable del sistema de IA	La organización deberá identificar y documentar objetivos para guiar el desarrollo responsable de los sistemas de IA, y tomar esos objetivos en cuenta e integrar medidas para lograrlos en el ciclo de vida del desarrollo.
	Procesos para el diseño y desarrollo responsable de sistemas de IA	La organización deberá definir y documentar los procesos específicos para el diseño y desarrollo responsable del sistema de IA.
A.7 Datos para sistemas de IA		
Objetivo: Garantizar que la organización comprenda el papel y los impactos de los datos en los sistemas de IA en la aplicación y el desarrollo, suministro o uso de sistemas de IA a lo largo de sus ciclos de vida.		
	Tema	Control
A.7.2	Datos para el desarrollo y mejora del sistema de IA	La organización deberá definir, documentar e implementar procesos de gestión de datos relacionados con el desarrollo de sistemas de IA.
A.7.3	Adquisición de datos	La organización deberá determinar y documentar los detalles sobre la adquisición y selección de los datos utilizados en los sistemas de IA.
A.7.4	Calidad de los datos para los sistemas de IA	La organización debe definir y documentar los requisitos para la calidad de los datos y garantizar que los datos utilizados para desarrollar y operar el sistema de IA cumplan esos requisitos.
A.7.5	Procedencia de los datos	La organización deberá definir y documentar un proceso para registrar la procedencia de los datos utilizados en sus sistemas de IA durante los ciclos de vida de los datos y del sistema de IA.
A.7.6	Preparación de datos	La organización debe definir y documentar sus criterios para seleccionar la preparación de datos y los métodos de preparación de datos que se utilizarán.
A.8 Información para las partes interesadas de los sistemas de IA		
Objetivo: Garantizar que las partes interesadas relevantes tengan la información necesaria para comprender y evaluar los riesgos y sus impactos (tanto positivos como negativos).		
	Tema	Control
A.8.2	Documentación del sistema e información para los usuarios.	La organización deberá determinar y proporcionar la información necesaria a los usuarios del sistema de IA.
A.8.3	Informes externos	La organización deberá proporcionar capacidades para que las partes interesadas informen sobre los impactos adversos del sistema de IA.
A.8.4	Comunicación de incidencias	La organización deberá determinar y documentar un plan para comunicar incidentes a los usuarios del sistema de IA.
A.8.5	Información para las partes interesadas	La organización deberá determinar y documentar sus obligaciones de reportar información sobre el sistema de IA a las partes interesadas.
A.9 Uso de sistemas de IA		
Objetivo: Garantizar que la organización utilice los sistemas de IA de manera responsable y según las políticas organizacionales.		
	Tema	Control
A.9.2	Procesos para el uso responsable de la IA	La organización debe definir y documentar los procesos para el uso responsable de los sistemas de IA.
A.9.3	Objetivos para el uso responsable de la IA	La organización debe identificar y documentar objetivos para guiar el uso responsable de los sistemas de IA.

A.6.2.6	Operación y monitoreo del sistema de IA	La organización deberá definir y documentar los elementos necesarios para el funcionamiento continuo del sistema de IA. Como mínimo, esto debería incluir monitoreo, reparaciones, actualizaciones y soporte del sistema y del rendimiento.
A.6.2.7	Documentación técnica del sistema de IA	La organización debe determinar qué técnicas del sistema de IA se necesita documentación técnica para cada categoría relevante de partes interesadas, como usuarios, socios, autoridades de supervisión, y proporcionarles la documentación técnica en la forma adecuada.
A.6.2.8	Registro del sistema de IA de registros de eventos	La organización deberá determinar en qué fases del ciclo de vida del sistema de IA, se debe habilitar el mantenimiento de registros de eventos, pero como mínimo cuando el sistema de IA está en uso.
A.7 Datos para sistemas de IA		
Objetivo: Garantizar que la organización comprenda el papel y los impactos de los datos en los sistemas de IA en la aplicación y el desarrollo, suministro o uso de sistemas de IA a lo largo de sus ciclos de vida.		
	Tema	Control
A.7.2	Datos para el desarrollo y mejora del sistema de IA	La organización deberá definir, documentar e implementar procesos de gestión de datos relacionados con el desarrollo de sistemas de IA.
A.7.3	Adquisición de datos	La organización deberá determinar y documentar los detalles sobre la adquisición y selección de los datos utilizados en los sistemas de IA.
A.7.4	Calidad de los datos para los sistemas de IA	La organización debe definir y documentar los requisitos para la calidad de los datos y garantizar que los datos utilizados para desarrollar y operar el sistema de IA cumplan esos requisitos.
A.7.5	Procedencia de los datos	La organización deberá definir y documentar un proceso para registrar la procedencia de los datos utilizados en sus sistemas de IA durante los ciclos de vida de los datos y del sistema de IA.
A.7.6	Preparación de datos	La organización debe definir y documentar sus criterios para seleccionar la preparación de datos y los métodos de preparación de datos que se utilizarán.
A.8 Información para las partes interesadas de los sistemas de IA		
Objetivo: Garantizar que las partes interesadas relevantes tengan la información necesaria para comprender y evaluar los riesgos y sus impactos (tanto positivos como negativos).		
	Tema	Control
A.8.2	Documentación del sistema e información para los usuarios.	La organización deberá determinar y proporcionar la información necesaria a los usuarios del sistema de IA.
A.8.3	Informes externos	La organización deberá proporcionar capacidades para que las partes interesadas informen sobre los impactos adversos del sistema de IA.
A.8.4	Comunicación de incidencias	La organización deberá determinar y documentar un plan para comunicar incidentes a los usuarios del sistema de IA.
A.8.5	Información para las partes interesadas	La organización deberá determinar y documentar sus obligaciones de reportar información sobre el sistema de IA a las partes interesadas.
A.9 Uso de sistemas de IA		
Objetivo: Garantizar que la organización utilice los sistemas de IA de manera responsable y según las políticas organizacionales.		
	Tema	Control
A.9.2	Procesos para el uso responsable de la IA	La organización debe definir y documentar los procesos para el uso responsable de los sistemas de IA.
A.9.3	Objetivos para el uso responsable de la IA	La organización debe identificar y documentar objetivos para guiar el uso responsable de los sistemas de IA.

Gestión de la IA en organizaciones

A.9.4	Uso previsto del sistema de IA	La organización deberá garantizar que el sistema de IA se utilice de acuerdo con los usos previstos del sistema de IA y la documentación que lo acompaña.
A.10 Relaciones con terceros y clientes		
Objetivo: Garantizar que la organización comprenda sus responsabilidades y siga siendo responsable, y que los riesgos se distribuyan adecuadamente cuando terceros estén involucrados en cualquier etapa del ciclo de vida del sistema de IA.		
	Tema	Control
A.10.2	Asignar responsabilidades	La organización deberá garantizar que las responsabilidades dentro del ciclo de vida de su sistema de IA se distribuyan entre la organización, sus socios, proveedores, clientes y terceros.
A.10.3	Proveedores	La organización debe establecer un proceso para garantizar que el uso de los servicios, productos o materiales proporcionados por los proveedores se alinee con el enfoque de la organización para el desarrollo y uso responsable de los sistemas de IA.
A.10.4	Clientes	La organización debe garantizar que su enfoque responsable para el desarrollo y uso de sistemas de IA considere las expectativas y necesidades de sus clientes.



ANEXOS B: Guía de implementación de controles

ANEXO C: Posibles objetivos organizacionales relacionados con la IA y fuentes de riesgo

ANEXO D: Uso del sistema de gestión de IA en todos los dominios o sectores

Gestión de Riesgos en materia de inteligencia artificial

- ➔ Proporciona orientación sobre cómo las organizaciones que desarrollan producen, implementan o utilizan productos, sistemas y servicios que utilizan inteligencia artificial (IA) pueden gestionar los riesgos específicamente relacionados con la IA.
- ➔ La guía también tiene como objetivo ayudar a las organizaciones a integrar la gestión de riesgos en sus actividades y funciones relacionadas con la IA. Además, describe los procesos para la implementación e integración efectiva de la gestión de riesgos de la IA..

Complemento ISO 31000

+

Norma Tipo B

+

ANEXOS A: Objetivos

ANEXO B: Fuentes de riesgo

ANEXO C: Gestión de riesgos y ciclo de vida del sistema de IA



Conductas de riesgo a “mapear”

01. Uso indebido de datos

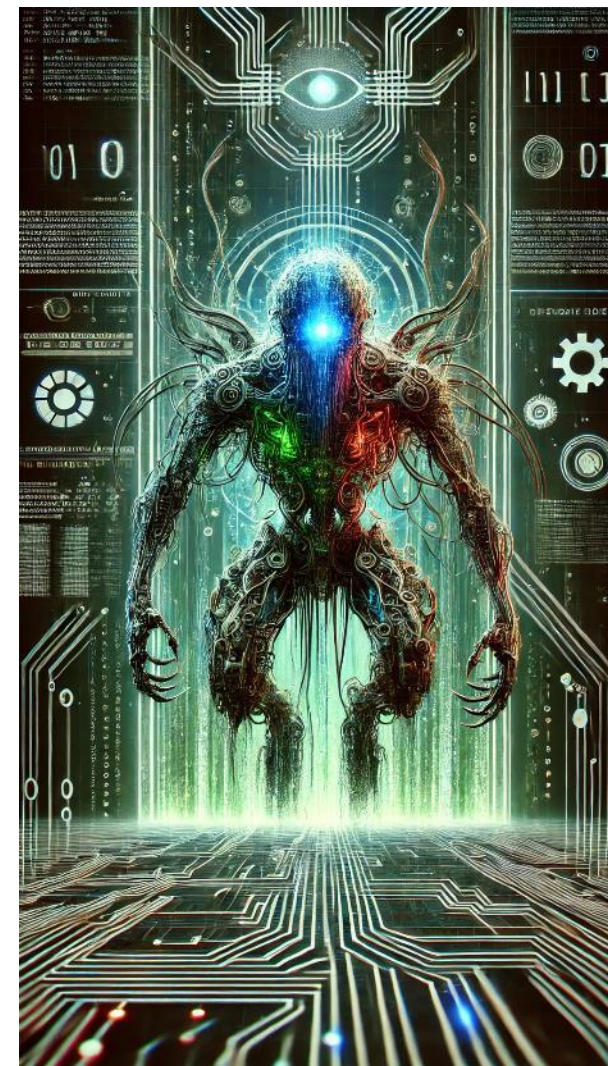
- **Acceso no autorizado:** Acceso a datos sensibles o confidenciales sin el permiso adecuado.
- **Uso de datos personales sin consentimiento:** Utilización de datos personales en modelos de IA sin cumplir con las normativas de protección de datos, como el GDPR.
- **Falsificación o manipulación de datos:** Alteración de datos de entrenamiento para obtener resultados deseados o falsificados.

02. Desarrollo y uso de sistemas de IA sin controles éticos

- **Sesgos algorítmicos:** Uso de IA sin verificar sesgos en los algoritmos, lo que puede llevar a discriminación o resultados injustos.
- **Despliegue de IA prohibida o no regulada:** Uso de sistemas de IA que están restringidos o prohibidos por las regulaciones.
- **Implementación de IA de alto riesgo sin pruebas de seguridad:** Uso de IA en áreas críticas (salud, transporte, finanzas) sin realizar auditorías de seguridad o pruebas adecuadas.

03. Manipulación o alteración de los resultados de la IA

- **Manipulación de salidas de IA:** Ajustar los resultados de la IA para obtener beneficios personales o corporativos a corto plazo, sin tener en cuenta los impactos a largo plazo.
- **Ignorar o suprimir alertas de riesgo:** Desactivar o ignorar sistemas de alerta que advierten sobre errores, posibles fallos o riesgos éticos.



Conductas de riesgo a “mapear”

4. Falta de transparencia y rendición de cuentas

- **Ocultamiento de errores:** No informar o encubrir fallos o errores de la IA que puedan afectar a la empresa o a los clientes.
- **No documentar adecuadamente los procesos:** Falta de documentación de cómo la IA toma decisiones, dificultando el seguimiento y auditoría interna.

5. Uso no autorizado de herramientas de IA externas

- **Uso de herramientas IA no aprobadas:** Empleados que utilizan sistemas o aplicaciones de IA sin la aprobación o supervisión de la empresa, lo que puede exponer a la organización a vulnerabilidades de seguridad.
- **Uso de IA en actividades ilegales:** Aplicar IA para actividades no éticas o ilegales, como espionaje corporativo, fraudes, o manipulación de mercados.

6. No seguir políticas internas de IA

- **Desatender las políticas de la empresa sobre IA:** Ignorar los protocolos y directrices corporativas para el desarrollo y uso de IA.
- **Uso de IA sin supervisión humana:** Implementar sistemas de IA críticos sin el monitoreo o intervención humana necesarios.

7. Riesgo de ciberseguridad

- **Integración insegura de IA:** Conectar sistemas de IA a infraestructuras sin las medidas de ciberseguridad necesarias, lo que puede ser explotado por ciberdelincuentes.
- **Uso negligente de datos y modelos IA compartidos públicamente:** Emplear datos y modelos sin verificar su origen o seguridad, lo que puede comprometer la seguridad de la empresa.







» Oportunidades «

- **Monitoreo de correos electrónicos** para detectar posibles violaciones de políticas internas (p. ej., uso de lenguaje inapropiado, envío de información confidencial).
- **Análisis de transacciones financieras en tiempo real** para identificar comportamientos sospechosos o actividades fraudulentas.
- **Escaneo de contratos** para verificar automáticamente cláusulas de cumplimiento normativo.
- **Control del acceso a sistemas sensibles** basándose en patrones de comportamiento de los usuarios.
- **Auditoría de registros de empleados** para asegurar que todos han completado la capacitación en cumplimiento y ética.
- **Monitoreo del uso de dispositivos y redes** para detectar el uso inapropiado de recursos tecnológicos.
- **Validación automática de terceros** (proveedores o clientes) contra listas de sanciones internacionales.
- **Escaneo de archivos compartidos en plataformas de trabajo** colaborativo para detectar datos personales o información confidencial mal protegida.
- **Automatización del proceso de denuncias internas** para asegurar que las quejas de los empleados sobre comportamientos no éticos sean recibidas y gestionadas adecuadamente.
- **Revisión automática de facturas** para detectar pagos duplicados o facturación incorrecta.
- **Monitoreo de redes sociales de empleados y socios** para asegurar que no se publiquen comentarios que puedan comprometer la reputación de la empresa.
- **Revisión de los términos de uso de software y licencias** para verificar que la empresa está utilizando software dentro de los límites legales.
- **Escaneo de informes financieros** para identificar automáticamente discrepancias o anomalías que puedan implicar fraude.
- **Control de acceso físico a áreas restringidas** mediante sistemas de reconocimiento facial o autenticación biométrica.
- **Evaluación automática de riesgos de proveedores** basándose en su historial de cumplimiento y noticias sobre incidentes.
- **Detección de patrones de comunicación inusuales** en chats corporativos que podrían indicar actividades no éticas.
- **Monitoreo de la entrega de productos** para asegurar que se cumple con los requisitos legales de etiquetado y calidad.
- **Supervisión de la gestión de residuos y emisiones** para asegurar el cumplimiento de las normativas ambientales.



» Oportunidades en materia de CORRUPCIÓN «

- **Monitoreo de pagos inusuales:** La IA puede analizar patrones de pagos para identificar transacciones que no coinciden con las políticas de la empresa o que parecen inusuales, como pagos repetitivos o montos elevados a terceros.
- **Verificación de proveedores y socios comerciales:** Utilizar IA para realizar una due diligence automatizada, revisando antecedentes de terceros y verificando si aparecen en listas de sanciones o vinculaciones con casos de corrupción.
- **Análisis de contratos:** Implementar IA para revisar automáticamente contratos en busca de cláusulas sospechosas que podrían indicar intentos de soborno o acuerdos irregulares.
- **Monitoreo de gastos de representación:** Analizar los reportes de gastos de empleados para identificar posibles pagos irregulares o sobornos disfrazados de gastos de viajes, entretenimiento o regalos.
- **Detección de conflictos de interés:** La IA puede identificar relaciones personales o empresariales no declaradas entre empleados y proveedores, para prevenir que los empleados favorezcan a socios con los que tienen vínculos no reportados.
- **Auditoría automática de aprobaciones:** Verificar si las aprobaciones de contratos, pagos o adquisiciones siguen los procedimientos correctos y no han sido manipuladas por empleados con la intención de cometer corrupción.
- **Control de regalos e incentivos:** IA que monitorea la entrega y recepción de regalos o incentivos para asegurarse de que no superan los límites legales o éticos establecidos por la empresa.
- **Monitoreo de patrones de comunicación:** Utilizar IA para analizar correos electrónicos o mensajes internos que puedan contener señales de comportamiento corrupto, como menciones de favores, influencias o acuerdos bajo la mesa.
- **Supervisión de la adjudicación de contratos:** Implementar sistemas de IA que revisen los procesos de licitación y adjudicación de contratos para detectar irregularidades, como favoritismos, licitaciones amañadas o sobornos.
- **Evaluación de transparencia en donaciones y contribuciones:** La IA puede revisar las donaciones o contribuciones políticas de la empresa para asegurarse de que cumplen con las regulaciones y no esconden actos de corrupción.
- **Detección de conductas colusorias.**

LA VANGUARDIA

Economía

DOLSILO / DINERO / FINANZAS PERSONALES / EMPRENDEDORES / INNOVACIÓN / LEGAL / CONSORCIO DE LA ZONA FRANCA [SUSCRIBETE](#)

CONTROL FINANCIERO

Inteligencia artificial para combatir el blanqueo de dinero

El HSBC es una de las entidades financieras que ha sido sancionada con multas más abultadas por este delito



Sede central de banco HSBC en Fish Market al este de Londres. (Justin Tallis / AFP)

Pilar Blázquez Madrid
10/04/2018 23:05 | Actualizado a 11/04/2018 13:37

[Al minuto](#)

Preocupación máxima por el estado de salud de Julián Muñoz: "Ha empeorado"

HSBC, el mayor banco de Europa, ha sido uno de los que ha

Morgan Stanley implementó IA para analizar millones de correos electrónicos internos en busca de posibles infracciones éticas o violaciones regulatorias. La IA analiza patrones lingüísticos y detecta señales de posible manipulación de mercado o fraude.

Salas de prensa Perspectivas Reportes de investigación Librería multimedia Idioma y región

Mastercard acelera la detección del fraude en tarjetas gracias a la tecnología IA Generativa

22 DE MAYO, 2024 | MIAMI, FL

A medida que los estafadores buscan nuevas formas de explotar la tecnología, Mastercard está utilizando la Inteligencia Artificial (AI) generativa para duplicar la velocidad a la que puede detectar tarjetas potencialmente comprometidas, protegiendo aún más a los tarjetahabientes y reforzando el ecosistema.

Los estafadores roban millones de números de tarjetas de pago a través de spyware, malware y otras prácticas clandestinas como el *skimming* de tarjetas. En un intento por vender estos datos a otros delincuentes, colocan parte de los 16 dígitos de las tarjetas en sitios web ilegales. Mastercard, líder mundial en ciberseguridad, tiene ahora mayores capacidades para predecir la información completa de estas tarjetas comprometidas en su red, lo que permite a los bancos bloquearlas mucho más rápido que antes.

Deutsche Bank moderniza su tecnología de gestión del riesgo crediticio y ahorra más de 10 millones de euros

Un banco de inversión líder lanza un programa de varios años para transformar su capacidad de gestión del riesgo de crédito a escala mundial

Como parte de un programa de transformación empresarial de varios años, Deutsche Bank recurrió a los servicios de GFT para implementar microservicios, rediseñar varias aplicaciones de crédito cruciales para el negocio y actualizar su capacidad de almacenamiento y gestión de datos. Con el programa hoy concluido, se estima que los cambios introducidos permitirán al banco ahorrar más de 10 millones de euros, mejorar drásticamente el cumplimiento normativo y aumentar la productividad en un 10%.

¿Por dónde empezamos?

- 
- 01 Identifica riesgos y oportunidades
 - 02 Establece una política de uso
 - 03 Define responsabilidades
 - 04 Establece medidas de control
 - 05 Formación y toma de conciencia
 - 06 Monitoreo y supervisión
 - 07 Actualízate



Compliance Officers

INTELIGENCIA ARTIFICIAL EN LA FRONTERA CON LA INTEGRIDAD

Iván Martínez López
imartinez@worldcomplianceassociation.com

25 sept 2024

www.worldcomplianceassociation.com