



Instituto de
Auditores Internos
de Argentina



IA y Gobierno de Datos

Nuevos Horizontes para la Auditoría Interna



Carlos García

Socio de Soluciones Tecnológicas

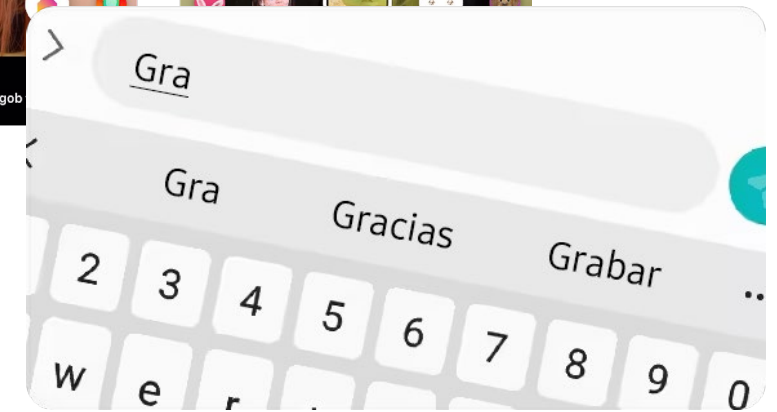
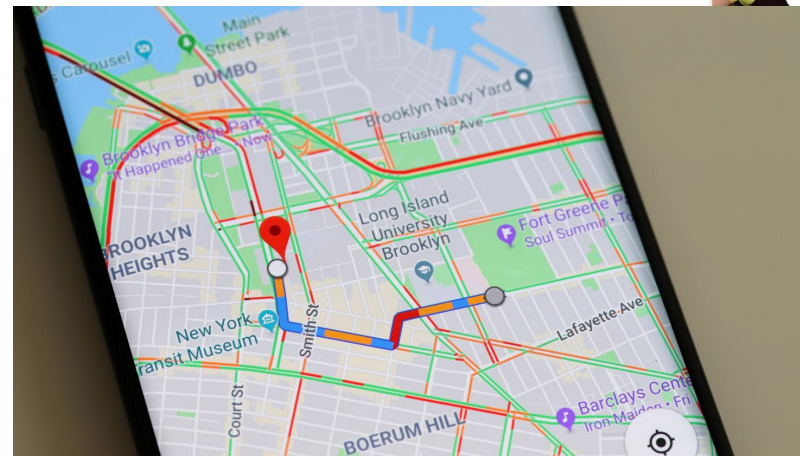
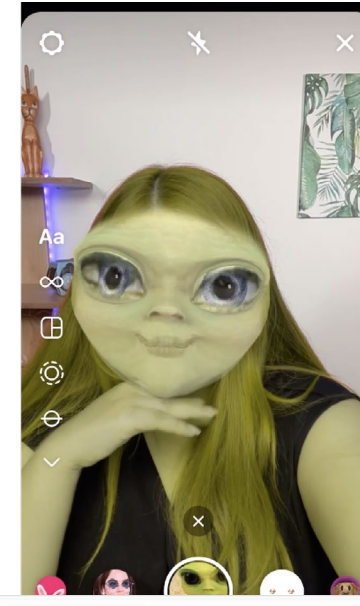
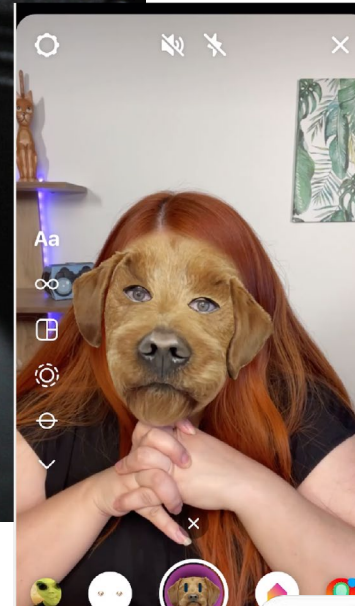
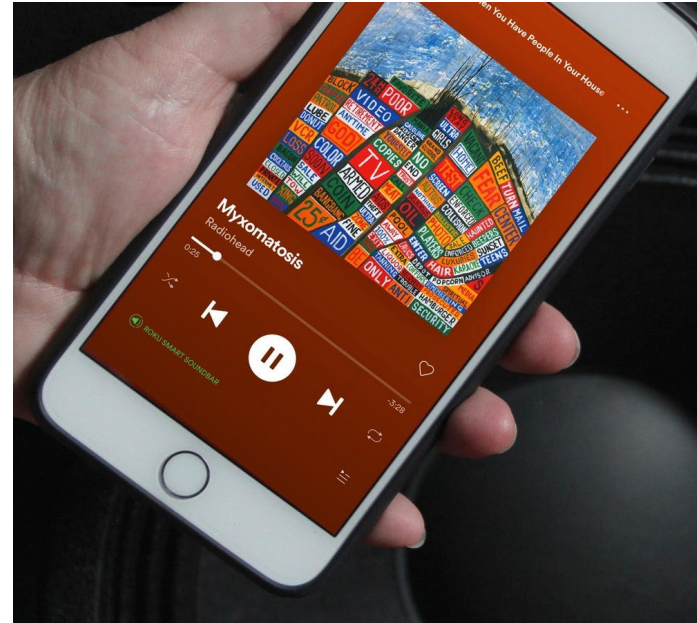
csgarcia@llyasoc.com



Natacha Soledad Represa

Manager Gestión de Datos e IA

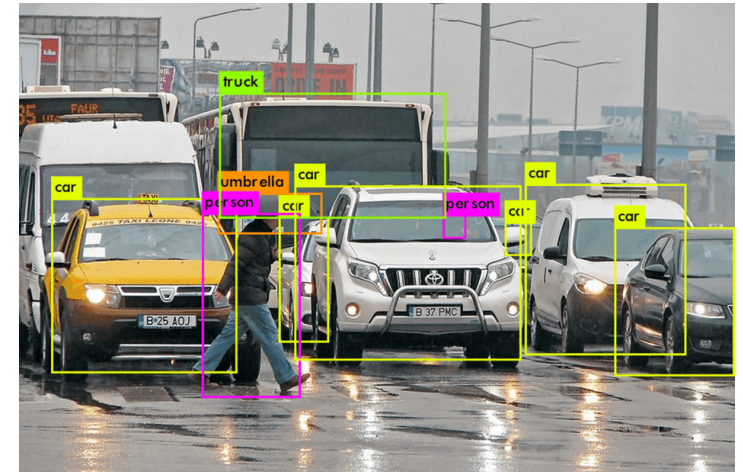
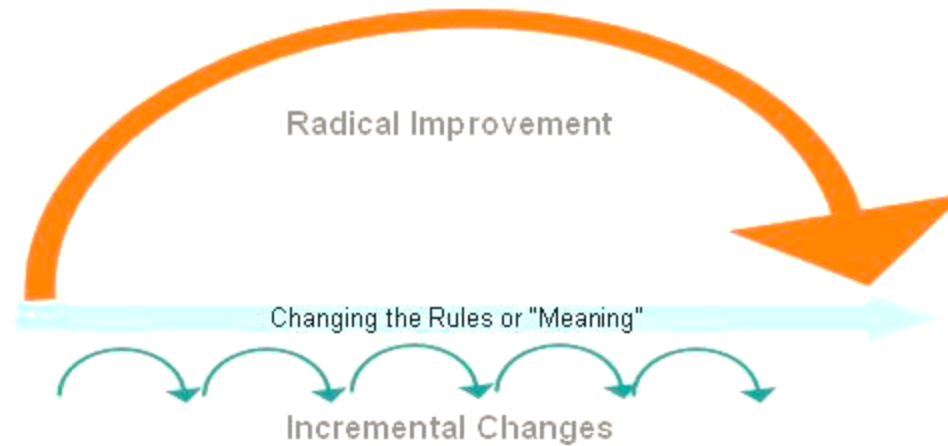
nrepresa@llyasoc.com



Evolución tecnológica



Disrupción tecnológica



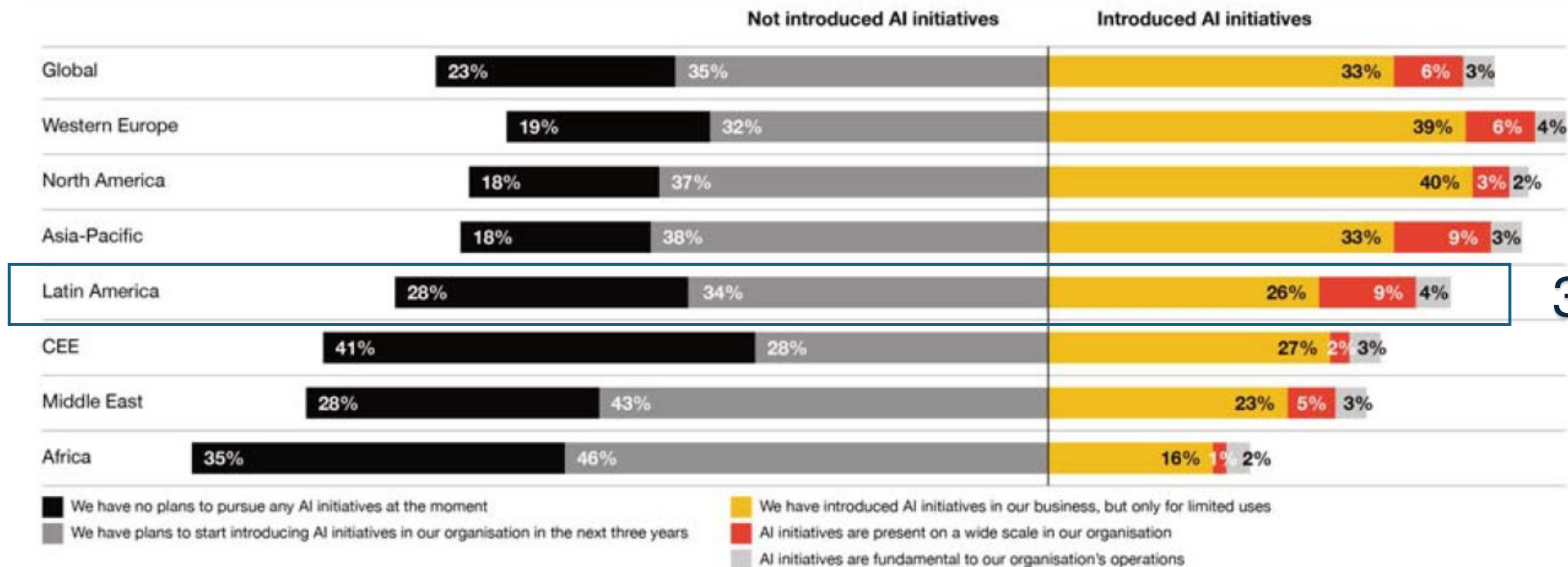


4ta Revolución Industrial

No solo automatizamos tareas repetitivas, **estamos creando sistemas capaces de tomar decisiones complejas.**



PLANES DE DESARROLLO DE INTELIGENCIA ARTIFICIAL



FUENTE: PwC. 22 nd Anual Global Global CEO Survey⁴

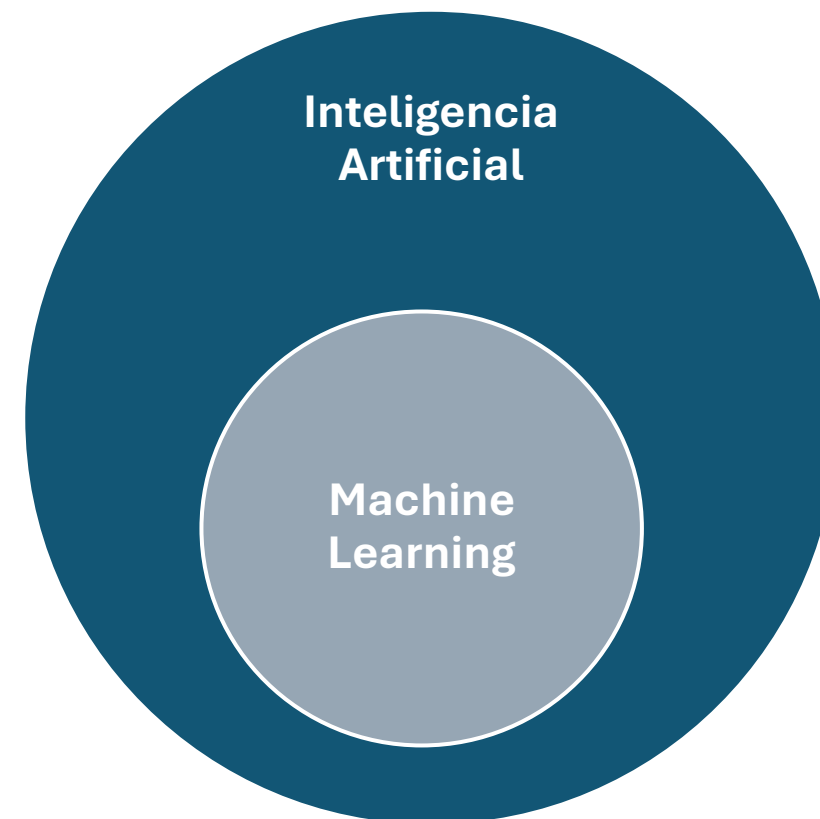
En un contexto de evolución hacia **modelos de negocio cada vez más tecnológicos, la auditoría está obligada a transformarse** para dar respuesta a las nuevas necesidades.

Inteligencia Artificial

IA es la **capacidad de las máquinas de mostrar habilidades y comportamientos “inteligentes”**. Este concepto abarca todo, desde sistemas que realizan tareas simples hasta aquellos que pueden imitar complejas actividades humanas.

Machine Learning (aprendizaje automático)

ML en el conjunto de métodos estadísticos para que las computadoras “aprendan” y mejoren a partir de los datos.



¿Cómo aprende la Inteligencia Artificial?

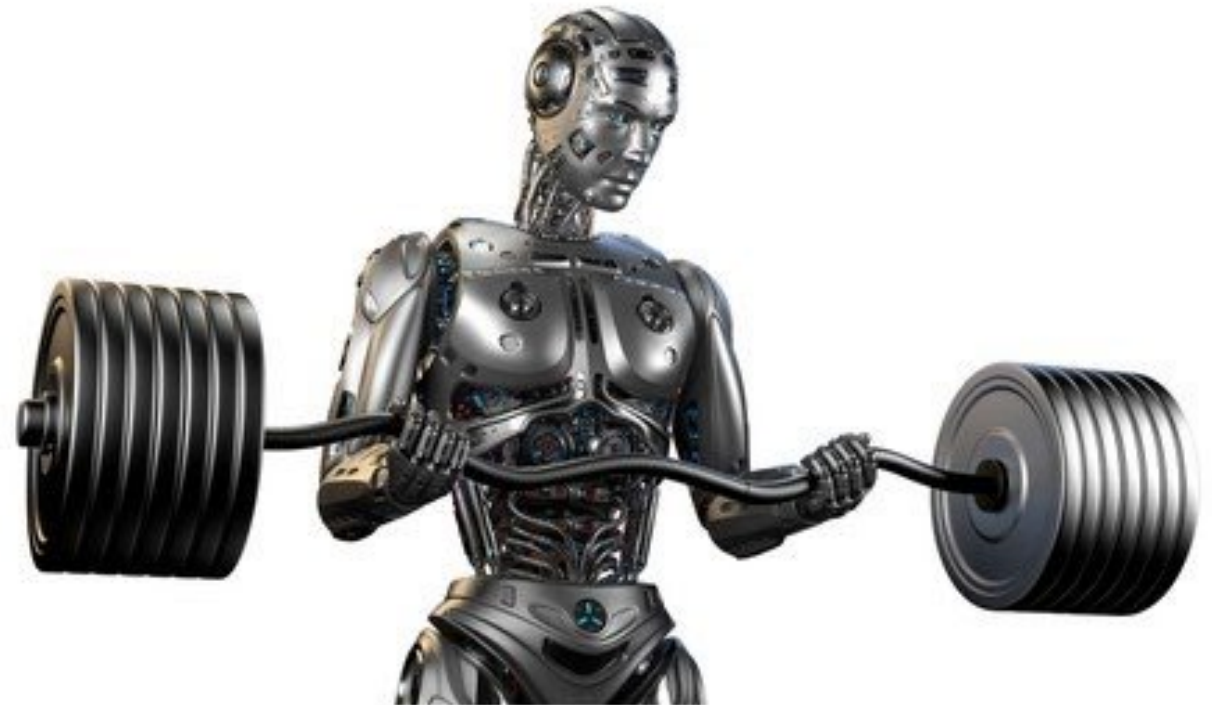
La IA aprende a través del entrenamiento de sus algoritmos.

Los algoritmos son instrucciones programadas que guían el procesamiento de **datos**, permitiendo que las computadoras recuerden patrones, mediante el ajuste de parámetros internos de los algoritmos.



¿Cómo se entrenan los algoritmos?

Para que los algoritmos aprendan hace falta entrenarlos con grandes cantidades de datos. Estos datos deben ser representativos del fenómeno que estamos queriendo modelar.





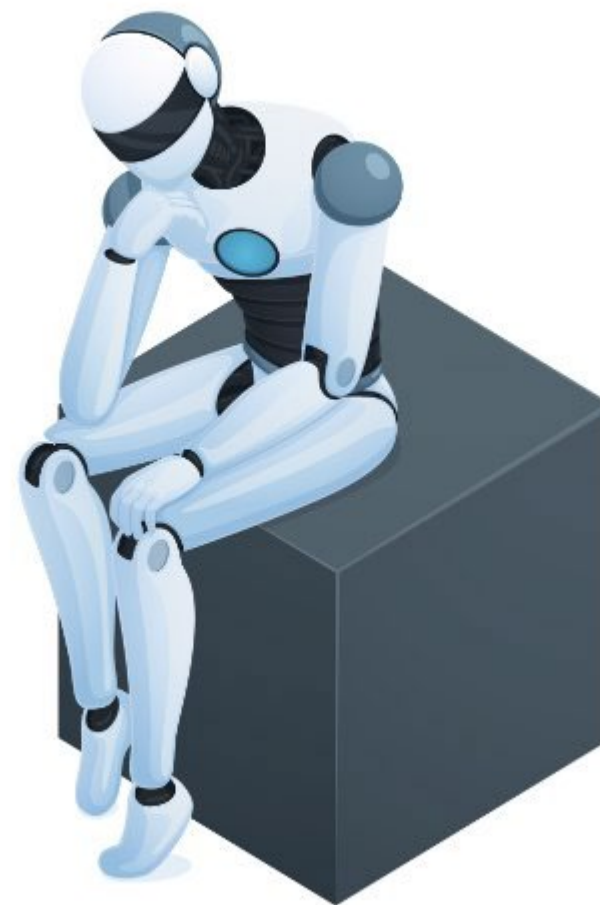
Los métodos de **machine learning** se basan en **algoritmos que aprenden de los datos**.

En el proceso de aprendizaje, se **ajusta el modelo automáticamente** para **mejorar su rendimiento**.

Los algoritmos **encuentran patrones** y aprenden de ellos para **hacer predicciones**.



¿Manzanas?



FORBES > TECH

Google Photos Tags Two African-Americans As Gorillas Through Facial Recognition Software

Maggie Zhang Forbes Staff

I write about technology, innovation, and startups.

Follow



Jul 1, 2015, 01:42pm EDT

TECH

How a computer algorithm caused a grading crisis in British schools

PUBLISHED FRI, AUG 21 2020 7:18 AM EDT | UPDATED FRI, AUG 21 2020 8:45 AM EDT

Sam Shead
@SAM_L_SHEAD

SHARE    

KEY POINTS

- Approximately 39% of A-level results were downgraded by exam regulator Ofqual's algorithm.
- Disadvantaged students were the worst affected as the algorithm copied the inequalities that exist in the U.K.'s education system.
- The U.K. government did a U-turn on the grading method as students went on protest.

¿Cuál es el nivel de riesgo de esta disrupción digital?

Riesgo del año pasado		Riesgo de este año		Expectativas de riesgo en 3 años	
1. Ciberseguridad	73%	1. Ciberseguridad	73%	1. Ciberseguridad	69%
2. Capital humano	51%	2. Continuidad del negocio	51%	2. Disrupción digital (incluida la IA)	59%
3. Continuidad del negocio	47%	3. Capital humano	49%	3. Continuidad del negocio	47%
4. Cambios reglamentarios	39%	4. Disrupción digital (incluida la IA)	39%	4. Capital humano	42%
5. Disrupción digital (incluida la IA)	34%	5. Cambios reglamentarios	38%	5. Cambio climático/medio ambiente	39%
6. Liquidez financiera	32%	6. Cambios en el mercado/la competencia	32%	6. Cambios reglamentarios	37%
7. Cambios en el mercado/la competencia	32%	7. Liquidez financiera	31%	7. Incertidumbre geopolítica	31%
8. Incertidumbre geopolítica	30%	8. Incertidumbre geopolítica	30%	8. Cambios en el mercado/la competencia	30%
9. Líneas de jerarquía corporativas/de gobierno	27%	9. Líneas de jerarquía corporativas/de gobierno	25%	9. Liquidez financiera	25%
10. Cadena de abastecimiento (incluidos los terceros)	26%	10. Cultura corporativa	24%	10. Cadena de abastecimiento (incluidos los terceros)	24%
11. Cultura corporativa	26%	11. Fraude	24%	11. Líneas de jerarquía corporativas/de gobierno	22%
12. Fraude	24%	12. Cadena de abastecimiento (incluidos los terceros)	23%	12. Fraude	21%
13. Comunicaciones/reputación	21%	13. Cambio climático/medio ambiente	23%	13. Cultura corporativa	20%
14. Cambio climático/medio ambiente	19%	14. Comunicaciones/reputación	20%	14. Comunicaciones/reputación	15%
15. Salud/seguridad	11%	15. Salud/seguridad	11%	15. Salud/seguridad	10%
16. Fusiones/adquisiciones	6%	16. Fusiones/adquisiciones	6%	16. Fusiones/adquisiciones	9%

Latin America Risk in Focus 2025, IIA

Riesgos asociados a la falta de auditorías en IA

- Decisiones Injustas o Discriminatorias
- Opacidad y Falta de Explicabilidad
- Riesgos Legales y Regulatorios
- Pérdida de Confianza de los Clientes
- Estancamiento en Innovación

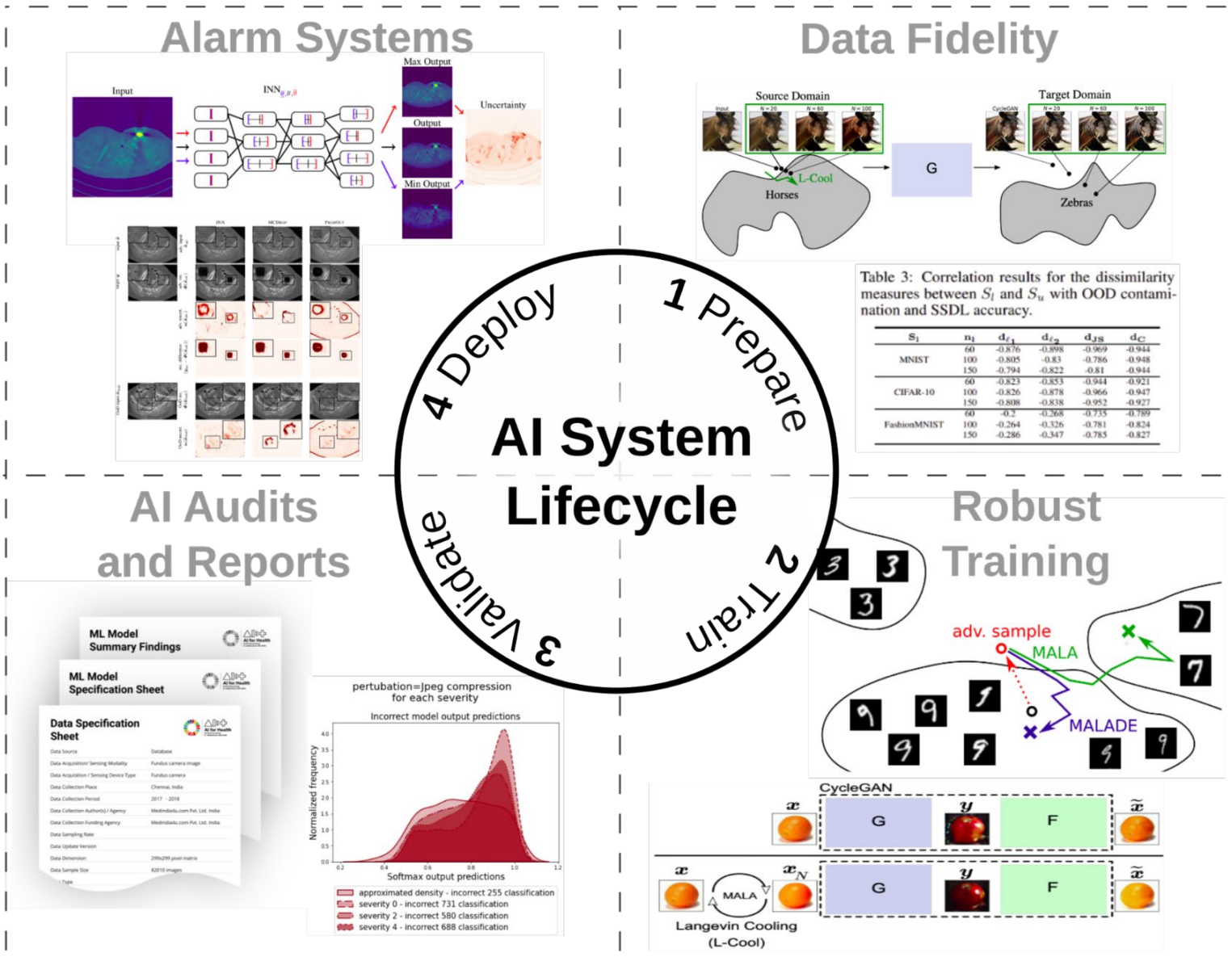
6 ámbitos de control interno

1. **Modelo de Gobierno** de sistemas de Inteligencia Artificial
2. Medición del **desempeño**
3. El factor **“Caja Negra”** (Black Box) en los sistemas de IA
4. El factor humano y el **sesgo algorítmico**
5. **Calidad de los datos**
6. Gobierno de **datos**

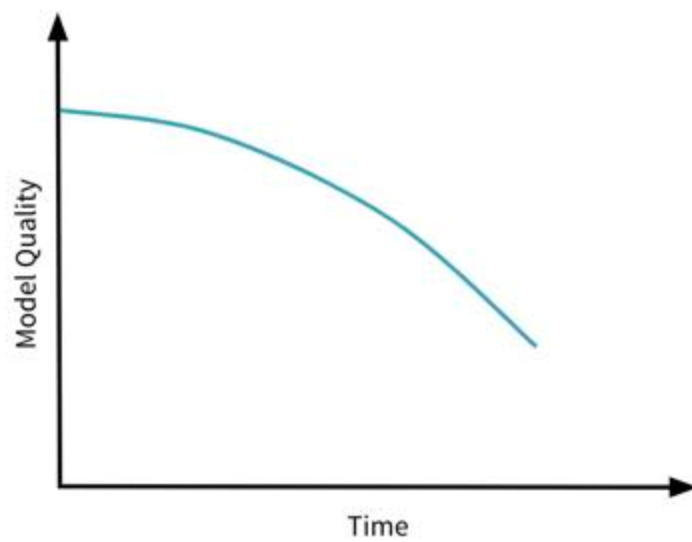
1. Gobierno de la IA



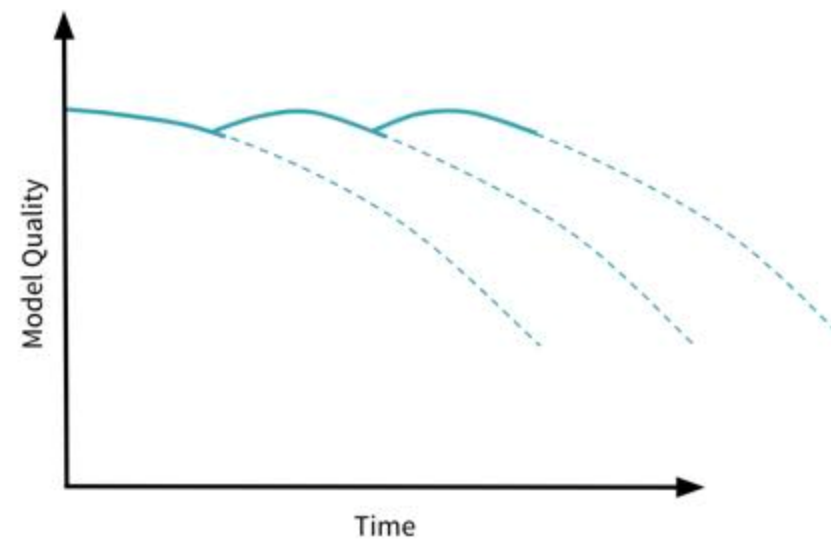
2. Medición del desempeño



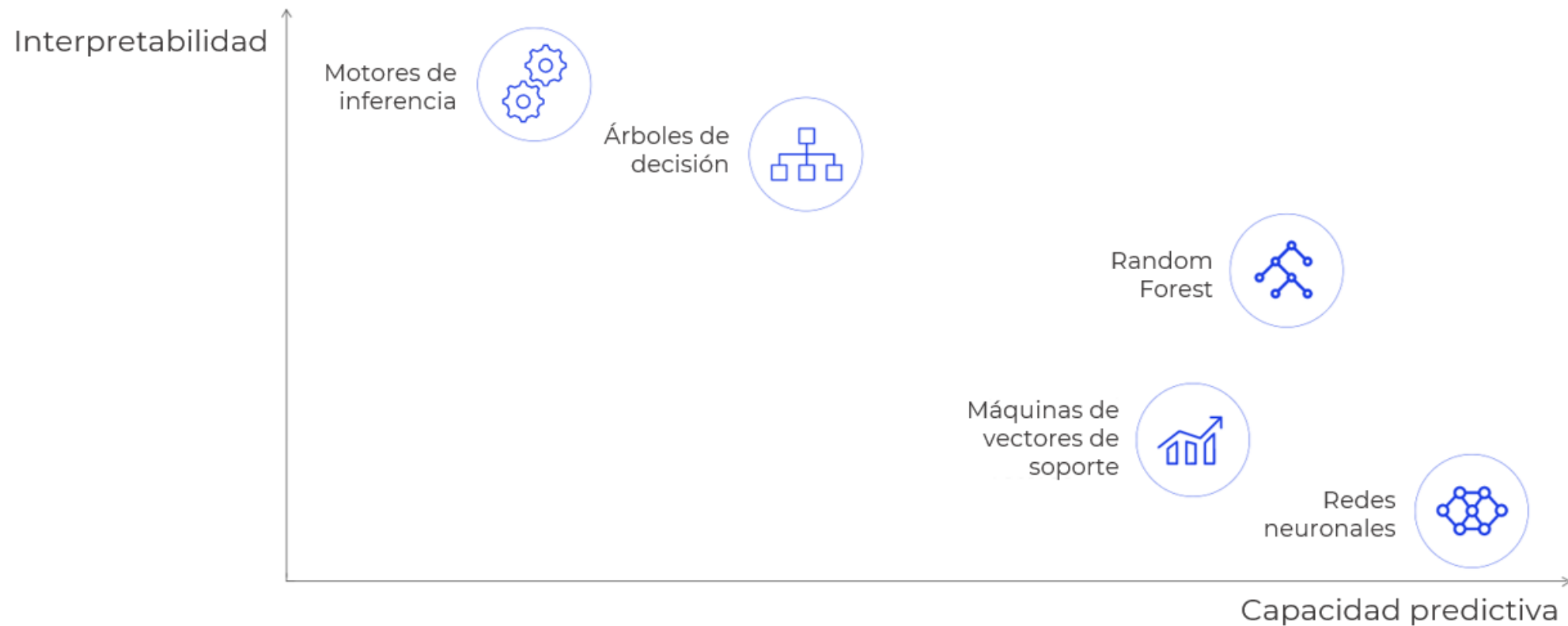
Static models



Refreshed models

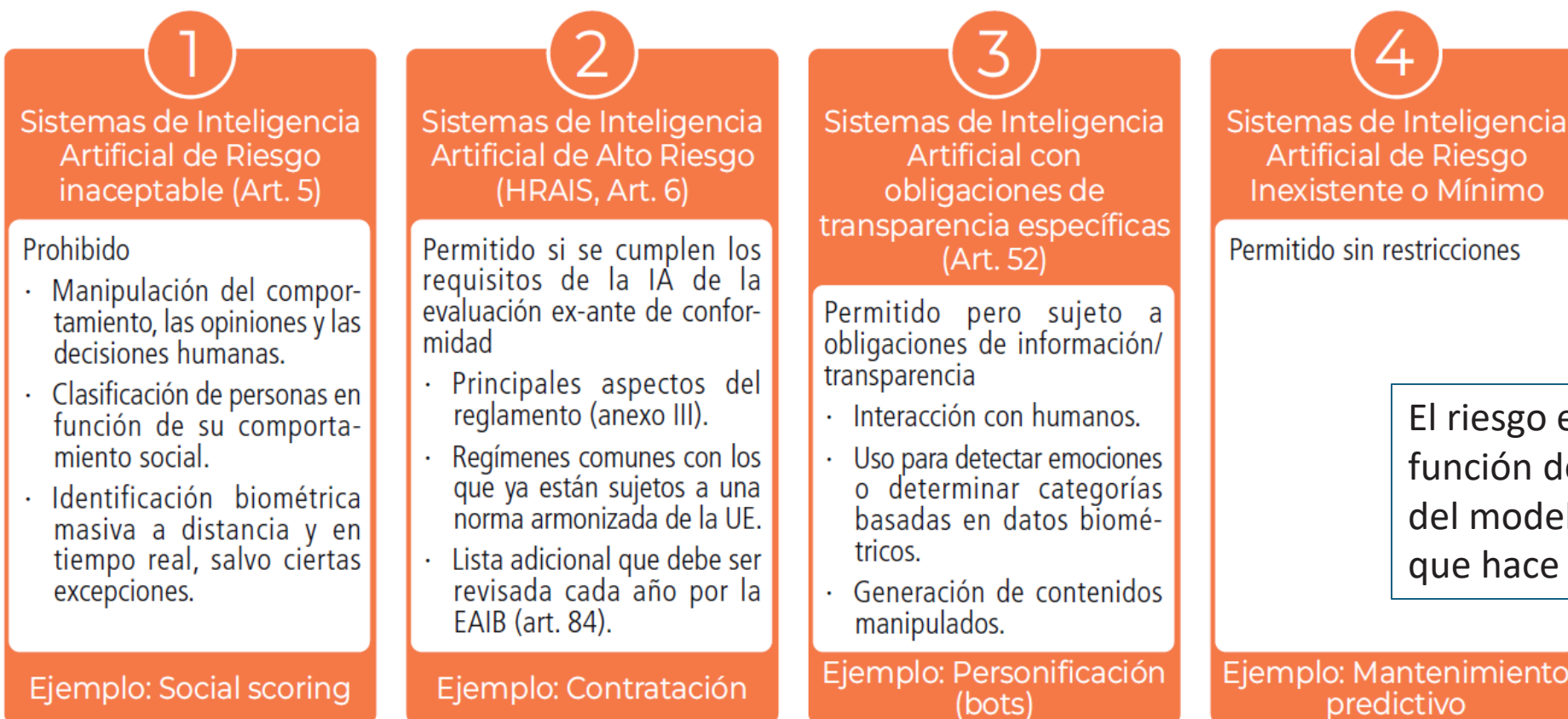


3. El factor “Caja Negra” en los sistemas de IA



4. El factor humano y el sesgo algorítmico

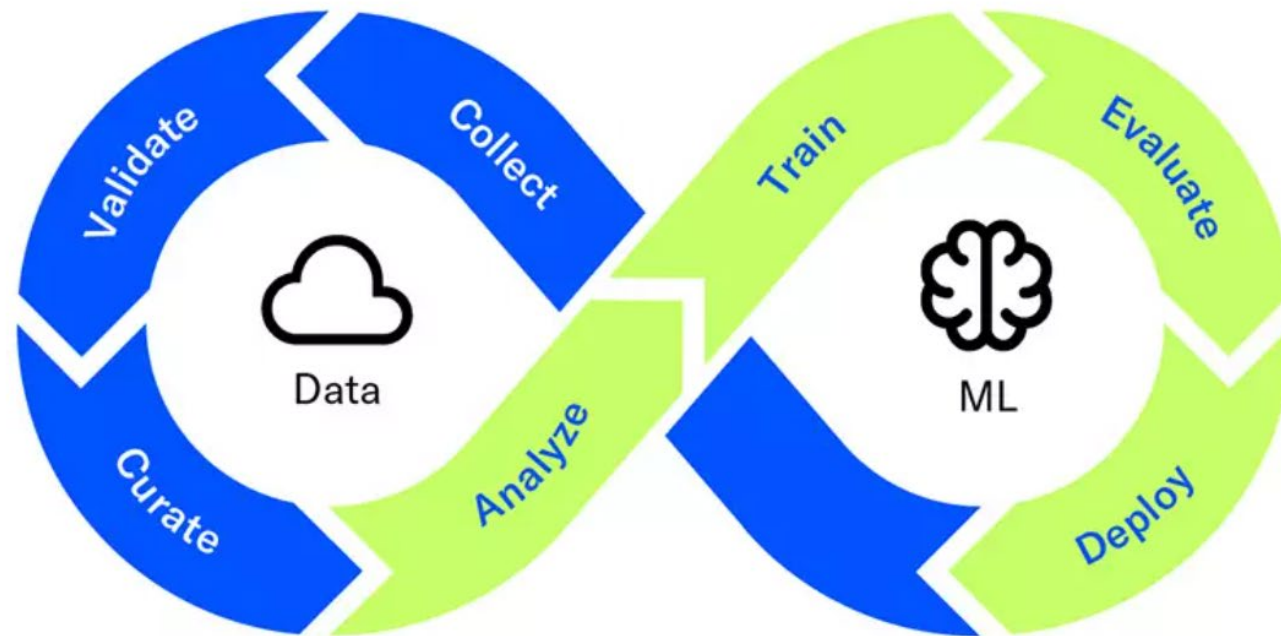
TIPOS DE SISTEMAS DE INTELIGENCIA ARTIFICIAL RECOGIDOS EN LA "AI ACT"



El riesgo es distinto en función del objeto final del modelo y de los datos que hace uso.

5. Calidad de los datos

Una auditoría de IA debe considerar tanto los algoritmos, como la calidad de los datos y las políticas de gobernanza.



6. Gobierno de Datos

Buenas Prácticas en Gobierno de Datos

Políticas claras

Definir políticas que rijan el uso, acceso y gestión de los datos, asegurando la coherencia en toda la organización.

Procesos robustos

Establecer procesos para la gestión del ciclo de vida de los datos, desde su creación hasta su eliminación, incluyendo la calidad, seguridad y cumplimiento.

Herramientas de gestión de datos

Aprovechar herramientas que faciliten la gestión y control de los datos, como plataformas de gestión de datos maestros (MDM), herramientas de calidad de datos y sistemas de gestión de riesgos.



Componentes Básicos

- ✓ Políticas
- ✓ Procedimientos
- ✓ Estándares
- ✓ Roles y Responsabilidades
- ✓ Herramientas

Identificar y clasificar el dato, medir su calidad y garantizar su trazabilidad.



Bases de la Auditoría de Gobierno de Datos

Principales riesgos asociados al Gobierno de Datos



INEXISTENCIA DE UN GOBIERNO FORMAL DE DATOS



Procesos desorganizados y duplicados.
Falta de rendición de cuentas.
Incumplimiento normativo.

FALTA DE CALIDAD DE DATOS

Decisiones erróneas basadas en información incorrecta.

Pérdida de oportunidades de negocio.



INTEGRACIÓN DEFICIENTE DE DATOS

Dificultad para integrar datos provenientes de múltiples fuentes o sistemas.
Retrasos en la entrega de información clave.

FALTA DE CULTURA DE DATOS

Toma de decisiones fragmentadas.
Falta de capacitación en el manejo adecuado de los datos.



INCUMPLIMIENTO NORMATIVO

Multas sustanciales por parte de organismos reguladores.
Suspensión de operaciones.
Litigios prolongado

MALA GESTIÓN DE DATOS MAESTROS

Datos maestros inconsistentes o desactualizados utilizados en múltiples sistemas.
Problemas de integración entre sistemas.
Incremento del esfuerzo manual para reconciliación de datos.

RETENCIÓN EXCESIVA O INSUFICIENTE DE DATOS



Incremento de costos de almacenamiento.
Incumplimiento normativo por retención excesiva.
Pérdida de información crucial para análisis o investigaciones futuras.

VIOLACIONES DE SEGURIDAD DE DATOS



Sanciones legales y regulatorias.
Daño reputacional significativo.
Pérdida de confianza de clientes y socios

Metodología de Auditoría



El análisis a desarrollar por parte del auditor interno dependerá en gran medida del grado de madurez de la organización.

En empresas poco maduras, la auditoría se centrará en seleccionar, definir y ejecutar controles de calidad para analizar los resultados.

En empresas maduras, el trabajo consistirá en supervisar si la forma en la que se miden los datos es adecuada.



Planificación y alcance

Recopilar y revisar documentación.
Revisar la existencia y efectividad de políticas de gobierno de datos.
Verificar que existan responsables designados para la gestión de datos.



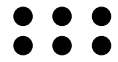
Ejecución

Definir objetivos y criterios de auditoría.
Identificar áreas críticas y priorizar actividades



Evaluación y Reporte

Identificar hallazgos y brechas
Discutir y presentar resultados



Pruebas de Auditoría - Gobierno



Existencia de una Política de Gobierno de Datos



Roles y Responsabilidades



Cultura de Datos y Capacitación

PRUEBA

Revisar si existe un documento formal que defina las políticas, roles y responsabilidades en el gobierno de datos.

- Validar si se ha conformado un comité o grupo directivo para el gobierno de datos.
- Verificar que los roles estén definidos y asignados (ej. Chief Data Officer (CDO), Data Owner, Data architect, Report owner).

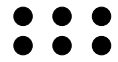
- Evaluar si el personal ha recibido formación sobre manejo y gobernanza de datos.
- Revisar encuestas o métricas que reflejen la adopción de una cultura basada en datos.

EVIDENCIA

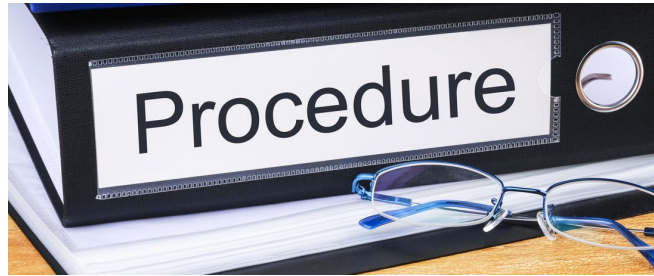
- Política de Gobierno de Datos aprobada.
- Minutas de reuniones donde se haya discutido su implementación.

- Organigramas funcionales.
- Manual de organización funcional donde se detallen estos roles y responsabilidades.

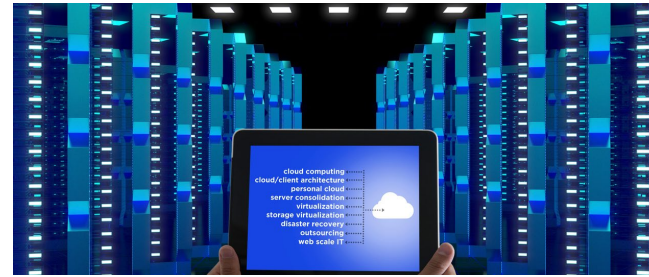
- Registros de capacitaciones.
- Encuestas de satisfacción.
- Políticas de comunicación sobre gobernanza de datos



Pruebas de Auditoría – Ciclo de Vida



Captura y Procesamiento



Almacenamiento



Archivado y Eliminación

PRUEBA

- Revisar la existencia de controles para prevenir la captura de datos incompletos, incorrectos o duplicados, y con los formatos establecidos en las políticas internas

- Revisar las configuraciones en los sistemas de almacenamiento, como el cifrado de datos en reposo y el acceso restringido.
- Validar la integridad de los datos almacenados mediante comparación con fuentes de entrada y pruebas de consistencia.

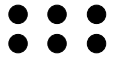
- Revisar las políticas de archivado para asegurar que se cumplen los plazos definidos para mover datos de producción en archivos.
- Verificar que los datos se eliminan conforme a las normativas legales y políticas internas

EVIDENCIA

- Políticas de captura de datos.
- Ejecución de pruebas de validación de datos en tiempo real.
- Configuraciones de validaciones automáticas en sistemas.

- Políticas de cifrado y backups.
- Logs de auditoría de sistemas de almacenamiento
- Configuración de permisos de acceso

- Políticas de archivado y eliminación de datos.
- Pruebas de recuperación de datos archivados.
- Registros de aprobación de eliminación.
- Logs detallados del ciclo de vida del dato.



Pruebas de Auditoría - Gestión



Calidad de Datos

Seguridad y Trazabilidad

Disponibilidad de Datos Críticos

PRUEBA

- Ejecutar pruebas de validación de calidad de datos (integridad, precisión, consistencia y completitud).
- Revisar reportes automatizados de calidad de datos

- Revisar que existan controles de acceso a datos (ej. listas de permisos, autenticación) y simular accesos no autorizados.
- Evaluar si se puede rastrear el origen, transformación y destino de los datos críticos en el ciclo de vida.

- Realizar pruebas de acceso a los datos críticos en escenarios de contingencia.
- Validar la implementación de sistemas de respaldo y recuperación.

EVIDENCIA

- Reportes de calidad de datos.
- Logs de herramientas de gestión de calidad.
- Políticas de calidad establecidas.

- Políticas de acceso.- Auditorías de permisos y usuarios.
- Logs de accesos y eventos de seguridad.
- Documentación del lineaje de datos.- Herramientas de trazabilidad utilizadas.

- Reportes de pruebas de recuperación.
- Inventarios de datos críticos.
- Configuración de respaldos automáticos

Riesgos Asociados a los Datos en la IA

RIESGOS	CONTROL DE AUDITORÍA
<p>Calidad de los Datos Insuficiente</p> <p>Datos incompletos, imprecisos o inconsistentes afectan la capacidad del modelo para aprender y generalizar.</p>	<ul style="list-style-type: none">• Revisar los procesos de limpieza, validación y enriquecimiento de datos.• Verificar que se implementen métricas de calidad, como precisión, completitud y consistencia.
<p>Sesgos en los Datos</p> <p>Datos históricos con prejuicios inherentes perpetúan inequidades en las decisiones del modelo.</p>	<ul style="list-style-type: none">- Realizar auditorías de los conjuntos de datos para identificar y documentar posibles sesgos.- Evaluar los resultados del modelo en diferentes grupos para detectar discriminación.
<p>Uso de Datos no Autorizados</p> <p>Uso de datos sin el consentimiento adecuado o en violación de regulaciones</p>	<ul style="list-style-type: none">- Verificar la existencia de acuerdos de consentimiento explícito.- Auditar los sistemas de gestión de datos personales para garantizar el cumplimiento normativo.
<p>Violaciones Éticas en la Gestión de Datos</p> <p>Recolección y uso de datos sin evaluar el impacto social o ético, incluyendo discriminación, sesgos y perjuicios culturales.</p>	<ul style="list-style-type: none">- Auditar si se realizan evaluaciones de impacto ético para los datos y modelos.- Revisar las políticas de la organización relacionadas con el uso ético de los datos.

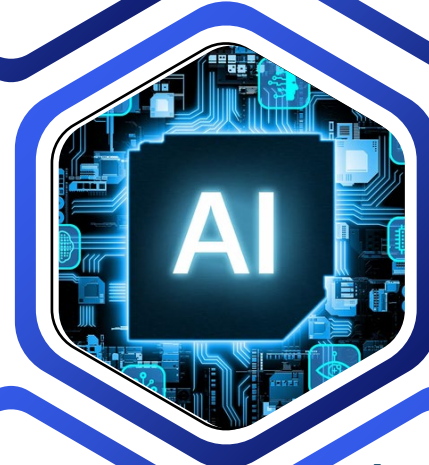
Desafíos para los Auditores

Evaluar la transparencia y la explicabilidad de las decisiones tomadas por modelos complejos.

Afrontar la falta de experiencia técnica y comprensión de IA dentro del equipo de auditoría.



Ajustar las metodologías de auditoría para abordar los riesgos específicos de la IA y los datos, como sesgos, seguridad y privacidad.



Identificar y mitigar sesgos en los datos de entrenamiento y en los resultados generados por la IA.



Utilizar herramientas avanzadas para analizar grandes volúmenes de datos y auditar modelos de IA.

Asegurar que los modelos de IA y las estrategias de datos estén alineados con las metas estratégicas de la organización.

***"El futuro de la auditoría interna está en el poder de los datos
y la ética de la inteligencia artificial."***



Instituto de
Auditores Internos
de Argentina