Universidad de Buenos Aires
Facultad de Ciencias Económicas

La Gobernanza de la Inteligencia Artificial

Material de Estudio

MASTERING AI GOVERNANCE
USING THE TRACE GOVERNANCE MODEL

TRACE Model (Governance Framework)

T **R** **A** **C** **E**

Transparency	Risk	Accountability	Controls	Evidence
Make AI systems visible, explainable, and traceable.	***Identify, classify, and prioritize AI risks early.***	***Assign ownership so governance isn't "everyone's job."***	***Put guardrails that prevent failure not just policies.***	***Make governance audit-ready and regulator-proof.***
Create a complete inventory of AI models, agents, and automations	Classify AI systems by risk level (low / medium / high)	Define who owns AI systems: business + IT + legal	Access control (RBAC), PII filtering, safe prompts, tool restrictions	Logging: prompts, outputs, actions, tool calls
Document where AI is used + what data it touches	Detect and prevent Shadow AI usage	Set approval workflows for new AI use cases	Human-in-the-loop checkpoints for high-risk workflows	Audit trail: who changed what, when, and why Generate
Make outputs explainable (why AI gave this answer/action)	Track risks like hallucinations, bias, privacy leaks, wrong actions	Establish escalation process for AI failures / incidents	Drift monitoring + bias checks + content safety filters	compliance dashboards for EU AI Act / ISO 42001 / GDPR

Phases of TRACE (12-Week Roadmap)

Week	Focus Area	Activities	Key Deliverables
1-2	Transparency	Map all AI systems (models, agents, copilots), data sources, integrations, owners.	AI Inventory, Data Access Map, AI Usage Baseline
3-4	Risk	Classify risks, identify Shadow AI pathways, define risk scoring model.	AI Risk Register, Shadow AI Report, Risk Tiering Matrix
5-6	Accountability	Assign governance roles, define approval workflows, set policy ownership.	RACI Chart, Approval Workflow, Governance Operating Model
7-8	Controls	Implement guardrails: RBAC, HITL steps, token limits, data masking, tool restrictions.	Control Library, Guardrail Configs, HITL Playbook
9-10	Evidence	Enable logging + monitoring + audit trails, establish compliance mapping.	Audit Logs, Evidence Repository, Compliance Dashboard
11-12	Reinforce + Scale	Run simulations, review incidents, optimize policies, scale model governance across org.	Governance Scorecard, Incident Playbooks, Scale Rollout Plan

https://www.linkedin.com/in/digitalprocessarchitect/

Vaibhav Aggarwal

Traducción y Comentarios

Dominando la Gobernanza de la Inteligencia Artificial usando el modelo TRACE

(TRACE Model – Governance Framework / Modelo TRACE – Marco de Gobernanza)

(AI – Artificial Intelligence / Inteligencia Artificial)

Modelo TRACE (Gobernanza de IA)

T – Transparencia (Transparency)

Objetivo: Hacer que los sistemas de IA sean **visibles, explicables y trazables**.

- Crear un **inventario completo** de:
  - modelos,
  - agentes,
  - automatizaciones.
- Documentar **qué datos utiliza la IA y dónde los utiliza**.
- Asegurar que los **resultados sean explicables**

  (por qué la IA dio determinada respuesta o tomó cierta acción).

Enfoque en Tecnologías y Sistemas de Información

- Catálogo de sistemas de IA integrado al **mapa de sistemas corporativos**.
- Relación directa con **Data Governance (Gobernanza de Datos)**.

R – Riesgo (Risk)

Objetivo: Identificar, clasificar y priorizar los riesgos de IA de forma temprana.

- Clasificar los sistemas de IA por nivel de riesgo:
  - bajo,
  - medio,
  - alto.
- Detectar y prevenir **Shadow AI**

  (*uso de IA no autorizado dentro de la organización*).
- Monitorear riesgos como:
  - alucinaciones,
  - sesgos,
  - filtraciones de datos,
  - acciones incorrectas.

Enfoque en Tecnologías y Sistemas de Información

- Evaluación de riesgos integrada a **gestión de riesgos de TI**.
- Relación con **seguridad de la información** y **compliance**.

A – Responsabilidad (Accountability)

Objetivo: Asignar responsables claros para que la gobernanza **no sea "de todos" y de nadie**.

- Definir quién es dueño de los sistemas de IA:
  - negocio,
  - TI,
  - legal.
- Establecer **flujos de aprobación** para nuevos casos de uso de IA.
- Crear procesos de **escalamiento** ante fallas o incidentes de IA.

Enfoque en Tecnologías y Sistemas de Información

- Integración con modelos **RACI**

(*Responsible, Accountable, Consulted, Informed – Responsable, Aprobador, Consultado, Informado*).

- Claridad organizacional en la operación de sistemas de IA.

C – Controles (Controls)

Objetivo: Implementar **barreras preventivas**, no solo políticas escritas.

- Controles de acceso **RBAC**

  (*Role-Based Access Control – Control de Acceso Basado en Roles*).

- Filtrado de prompts, restricciones de herramientas y uso.
- **Human-in-the-Loop (HITL – Humano en el Circuito)** para flujos de alto riesgo.
- Monitoreo de:
  - deriva del modelo (*model drift*),
  - sesgos,
  - seguridad de contenidos.

Enfoque en Tecnologías y Sistemas de Información

- Controles técnicos integrados a **ERP, CRM y plataformas de IA**.
- Gobernanza aplicada directamente en los sistemas, no solo en documentos.

E – Evidencia (Evidence)

Objetivo: Dejar la gobernanza **lista para auditoría y reguladores**.

- Registro (*logging*) de:
  - prompts,
  - resultados,
  - acciones,
  - llamadas a herramientas.
- **Auditoría completa**:

    - quién cambió qué,
    - cuándo,
    - y por qué.
- Generación de tableros de cumplimiento para:
    - **EU AI Act** (Ley de IA de la Unión Europea),
    - **ISO 42001** (Sistema de Gestión de IA),
    - **GDPR** (*General Data Protection Regulation – Reglamento General de Protección de Datos*).

Enfoque en Tecnologías y Sistemas de Información

- Integración con sistemas de **auditoría, logs y monitoreo**.
- Evidencia automatizada y trazable.

Fases del modelo TRACE (Hoja de ruta de 12 semanas)

Semanas 1–2 | Transparencia

Actividades

- Mapear todos los sistemas de IA (modelos, agentes, copilotos).
- Identificar fuentes de datos, integraciones y responsables.

Entregables clave

- Inventario de IA.
- Mapa de acceso a datos.
- Línea base de uso de IA.

Semanas 3–4 | Riesgo

Actividades

- Clasificar riesgos.
- Identificar Shadow AI.

- Definir modelo de scoring de riesgo.

Entregables clave

- Registro de riesgos de IA.
- Informe de Shadow AI.
- Matriz de priorización de riesgos.

Semanas 5–6 | Responsabilidad

Actividades

- Asignar roles de gobernanza.
- Definir flujos de aprobación.
- Establecer responsables de políticas.

Entregables clave

- Matriz RACI.
- Flujos de aprobación.
- Modelo operativo de gobernanza.

Semanas 7–8 | Controles

Actividades

- Implementar controles:
  - RBAC,
  - HITL,
  - límites de uso,
  - enmascaramiento de datos.
- Definir restricciones técnicas.

Entregables clave

- Biblioteca de controles.
- Configuración de guardrails.

- Manual de operación HITL.

Semanas 9–10 | Evidencia

Actividades

- Activar logging, monitoreo y auditorías.
- Mapear requisitos regulatorios.

Entregables clave

- Logs de auditoría.
- Repositorio de evidencias.
- Dashboard de cumplimiento.

Semanas 11–12 | Reforzar y Escalar

Actividades

- Simulaciones y pruebas.
- Revisión de incidentes.
- Optimización de políticas.
- Escalado del modelo a toda la organización.

Entregables clave

- Scorecard de gobernanza.
- Playbooks de incidentes.
- Plan de despliegue a escala organizacional.

Lectura clave para estudiantes de Administración

- La gobernanza de la IA es **un problema organizacional y de sistemas**, no solo técnico.
- TRACE conecta **estrategia, procesos, sistemas de información, riesgos y regulación**.

- El administrador cumple un rol central en **coordinar negocio, TI y cumplimiento normativo** dentro del uso de IA.

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.