

Manual de Estudio: AWS Certified AI Practitioner

Dominio 5.2: Gobernanza y Conformidad de Sistemas de IA

Material Técnico Detallado

1. Conformidad y el Modelo de Responsabilidad Compartida

La conformidad en AWS asegura que las cargas de trabajo cumplan con estándares globales y regionales. Al igual que en seguridad, se divide en:

- **AWS:** Responsable de la conformidad **de** la nube (certificaciones de centros de datos, hardware y red).
- **Cliente:** Responsable de la conformidad **en** la nube (configuración de sus aplicaciones y datos).

1.1. AWS Artifact

Es el servicio central para acceder a los informes de conformidad de AWS realizados por auditores externos.

- **Uso:** Proporcionar estos informes (SOC 2, ISO 27001) a tus propios auditores para reducir el ámbito de la auditoría, ya que el cliente "hereda" los controles ya validados de AWS.

2. Marcos y Normativas Globales de IA

El examen evalúa el conocimiento de estándares emergentes publicados en 2023 y regulaciones clave.

2.1. Estándares ISO y NIST

- **ISO 42001 e ISO 23894:** Establecen marcos para evaluar y administrar el riesgo sistemático en el desarrollo y despliegue de IA.
- **NIST AI Risk Management Framework (RMF):** Marco voluntario con cuatro funciones: **Gobernar, Asignar, Medir y Administrar**.

2.2. Ley de IA de la Unión Europea (EU AI Act)

Primera normativa integral que clasifica la IA según su riesgo:

1. **Riesgo Inaceptable (Prohibido):** Puntuación social, reconocimiento facial indiscriminado, inferencia de emociones en trabajo/educación.
2. **Alto Riesgo:** Herramientas de examen de currículos, sistemas de salud. Requieren gestión de riesgos estricta y gobernanza de datos.
3. **Riesgo Bajo/Desregulado:** Aplicaciones que no entran en las categorías anteriores.

3. Gestión y Estimación del Riesgo

Según el NIST, el riesgo se calcula como:

$$\text{Riesgo} = \text{Probabilidad del evento} \times \text{Gravedad de la consecuencia}$$

- **Riesgo Inherente:** El riesgo natural antes de aplicar controles.
- **Riesgo Residual:** El riesgo que queda después de aplicar mitigaciones y controles de seguridad.

4. Herramientas de Auditoría y Control en AWS

Servicio	Función en Conformidad/Gobernanza
AWS Audit Manager	Recopila automáticamente evidencia de uso para generar informes de auditoría (ej. para SOC 2 o GenAI).
AWS Config	Registra el historial de configuración de los recursos y detecta cambios que violen las reglas de conformidad.
Amazon Inspector	Escanea aplicaciones y contenedores en busca de vulnerabilidades de software y exposición de red.
AWS Trusted Advisor	Evalúa el entorno basándose en 6 categorías (seguridad, coste, etc.) y recomienda acciones correctivas.

5. Gobernanza de Datos

La gobernanza es el equilibrio entre el **acceso** (innovación) y el **control** (seguridad).

5.1. Roles Clave

- **Propietario de Datos (Data Owner):** Ejecutivo que toma decisiones sobre políticas, acceso y conformidad.
- **Administrador de Datos (Data Steward):** Persona operativa con conocimiento detallado que gestiona el día a día de los datos.

5.2. Servicios de Calidad y Trazabilidad

- **AWS Glue DataBrew:** Herramienta visual para creación de **perfiles de datos** y seguimiento de **trazabilidad** (linaje) sin código.
- **AWS Glue Data Quality:** Usa ML para recomendar reglas y detectar anomalías en los datos automáticamente.
- **AWS Lake Formation:** Centraliza permisos granulares (a nivel de fila, columna y celda) para lagos de datos en S3.

6. Ciclo de Vida de los Datos en S3

Por motivos de conformidad, los datos de entrenamiento deben conservarse de forma rentable usando reglas de ciclo de vida:

1. **S3 Standard:** Acceso frecuente.
2. **S3 Intelligent-Tiering:** Patrones de acceso desconocidos.
3. **S3 Glacier Deep Archive:** Retención a largo plazo (años) por requisitos legales con el menor coste.

7. Estrategia de Gobernanza de IA: Los 5 Ámbitos

La responsabilidad del cliente aumenta según cómo consuma la IA:

- **Ámbitos 1 y 2:** Consumo de aplicaciones de terceros (baja responsabilidad).
- **Ámbitos 3 a 5:** Creación, entrenamiento y refinamiento de modelos propios (máxima responsabilidad: clasificación de datos, modelado de amenazas y resistencia).