PREPARACIÓN PARA LA CERTIFICACIÓN DE SOCIOS DE AWS

# AI Practitioner

## Sesión de revisión de contenido 4

## Dominio 4 y Dominio 5

# Suscripción *opcional* a AWS Skill Builder

La suscripción a Skill Builder proporciona acceso a exámenes oficiales de práctica de certificación de AWS, contenido de capacitación digital a tu propio ritmo, incluidos desafíos abiertos, laboratorios a tu propio ritmo y aprendizaje basado en juegos. **Ten en cuenta que no se requiere la suscripción a Skill Builder para este programa Acelerador.**

## Capacitación digital gratuita

*ENLACE AQUÍ*

**Las características especiales incluyen:**

- Más de 6 cursos digitales.
- Planes de aprendizaje.
- 10 Juegos de preguntas de práctica.
- *AWS Cloud Quest (Fundacional).*

## Suscripción individual

*ENLACE AQUÍ*

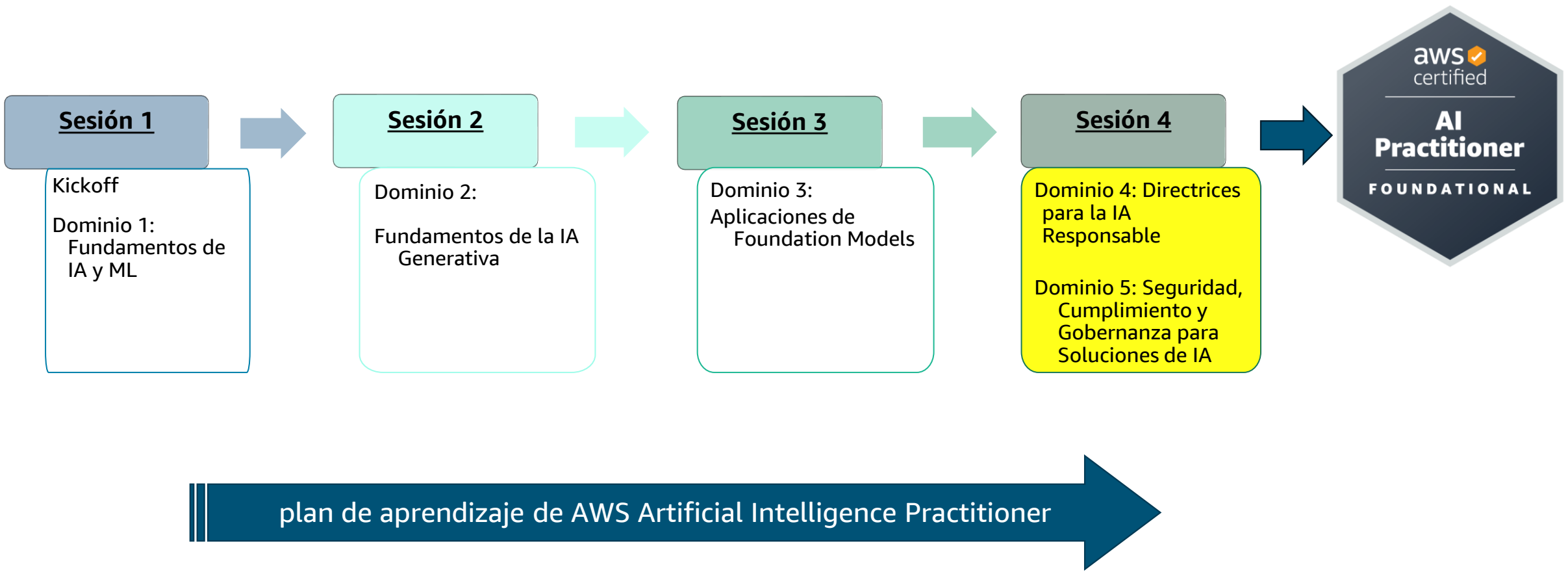
**Todo en la formación digital gratuita, además de:**

- AWS Cloud Quest (Intermedio - Avanzado).
- Exámenes de práctica oficiales de certificación.
- Cursos de Preparación para Exámenes Mejorados.
- Acceso ilimitado a más de 1000 laboratorios prácticos.
- AWS Jam Journeys (desafíos basados en laboratorio).
- Aula digital de AWS (solo anual).

Las suscripciones individuales tienen un precio de $29 USD al mes (*Flexibilidad para cancelar en cualquier momento*) o $449 USD por año.

Puedes inscribirte en el plan de preparación para el examen AI Practitioner. También recomendamos que las personas con perfil técnico usen AWS Cloud Quest: Generative AI Solutions para acceder a laboratorios y desarrollar habilidades prácticas.

# Resumen del programa



# Plan de estudios de formación digital semanal

Completa estos cursos digitales lo antes posible.

| Cursos del plan de aprendizaje de AWS Skill Builder |
| --- |
| Security, Compliance, and Governance for AI solutions |
| Essentials of Prompt Engineering |

| Plan de preparación para el examen (opcional) |
| --- |
| **Completo –** CloudQuest: Generative AI |
| Domain 4 Review; Domain 4 Practice* |
| Domain 5 Review; Domain 5 Practice* |
| AWS SimuLearn: Securing Data in Amazon S3 Using Amazon Macie and AWS KMS |
| *Official Pretest: AWS Certified AI Practitioner* |
| *AWS Escape Room: Exam Prep for AWS Certified AI Practitioner* |

* Requiere suscripción a AWS Skill Builder

# Resultados de aprendizaje actuales

Durante esta sesión, cubriremos:

- Declaración de tareas 4.1: Explicar el desarrollo de los sistemas de IA que son responsables
- Declaración de tareas 4.2: Reconocer la importancia de los modelos transparentes y explicables
- Declaración de tareas 5.1: Explicar los métodos para proteger los sistemas de IA
- Declaración de tareas 5.2: Reconocer las regulaciones de gobernanza y cumplimiento para los sistemas de IA

PREPARACIÓN PARA LA CERTIFICACIÓN DE SOCIOS DE AWS

# Dominio 4: Directrices para IA Responsable

## Declaración de tareas 4.1: Explicar el desarrollo de los sistemas de IA que son responsables

# ¿Qué es la IA responsable?

**IMPARCIALIDAD**

Considerar el impacto en diferentes grupos de interés

**EXPLICABILIDAD**

Comprender y evaluar salidas del sistema

**CONTROLABILIDAD**

Disponer de mecanismos para monitorear y dirigir el comportamiento del sistema de IA

**SEGURIDAD**

Prevención de resultados dañinos del sistema y mal uso

**PRIVACIDAD Y SEGURIDAD**

Obtención, uso y protección adecuados de datos y modelos

**GOBERNANZA**

Incorporación de las mejores prácticas en la cadena de suministro de IA, incluyendo proveedores e implementadores

**TRANSPARENCIA**

Permitir a las partes interesadas tomar decisiones informadas sobre su compromiso con un sistema de IA

**VERACIDAD Y ROBUSTEZ**

Lograr resultados correctos del sistema, incluso con entradas inesperadas o adversarias

# Sesgo (Bias) del conjunto de datos

## ¿Qué es?

- El sesgo del conjunto de datos se refiere al sesgo sistemático o desequilibrio en los datos utilizados para entrenar un modelo de Machine Learning

## ¿Cuáles son los tipos comunes de sesgo del conjunto de datos?

- **Sesgo de muestreo:** Los datos recopilados no representan la población verdadera.
- **Sesgo histórico:** Los datos reflejan sesgos e inequidades del pasado en la sociedad.

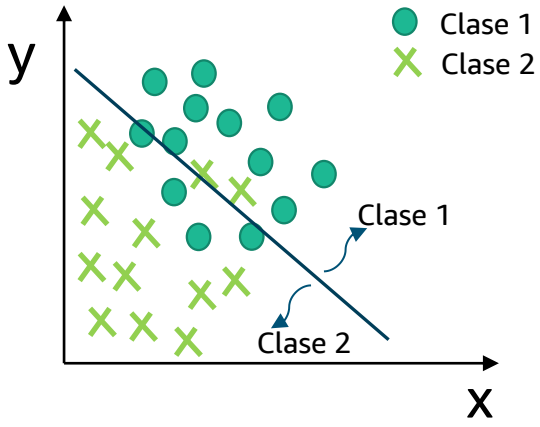
## ¿Cómo identificar el desequilibrio?

sí introduce

- Calcular la relación entre la clase más pequeña frente a los datos totales

# Problemas de generalización del modelo — Sesgo vs Varianza

## **Underfitting** (subajuste)

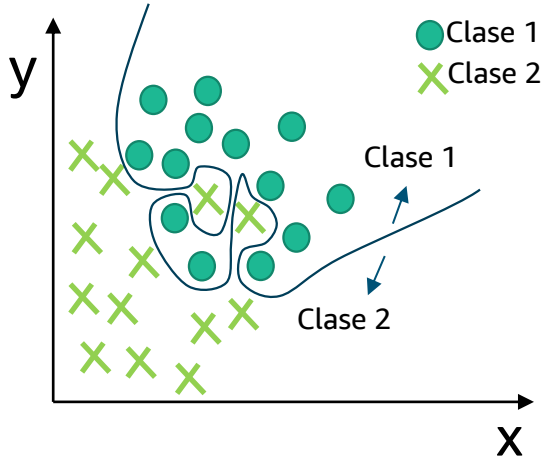



El modelo es demasiado sencillo para capturar la relación entrada/salida.

Tendrá un mal entrenamiento y rendimiento en las pruebas.

Cómo arreglarlo:
Aumentar los datos de entrenamiento o el número de iteraciones sobre los datos existentes.

## **Overfitting** (sobreajuste)

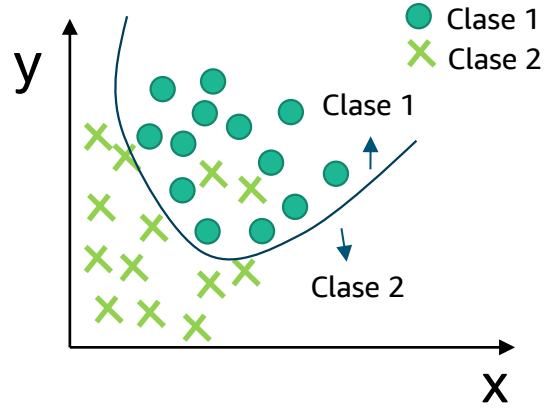



El modelo capta el ruido en lugar de la relación subyacente.

Veremos buenos puntajes en los datos de entrenamiento pero pobres resultados en los datos de las pruebas.

Cómo arreglarlo:
Reducir la flexibilidad del modelo: menos funciones, grupos más pequeños de datos por trabajo de entrenamiento, más regularización (ajuste de pesos de las características), detención temprana.

## **Appropriate Fitting**
(ajuste apropiado)




Bajo sesgo, Baja varianza

# Apoyar el uso responsable de ML durante todo el ciclo de vida del modelo

## A bordo

Configurar usuarios de ML con permisos personalizados

## Construir

Realizar análisis de sesgo durante el análisis exploratorio de datos

Documentar la información del modelo, como el uso previsto y las calificaciones de riesgo

## Entrenar

Realizar análisis de sesgos y explicabilidad después del entrenamiento

Capturar observaciones de capacitación y evaluación del modelo

## Desplegar

Explicar las inferencias individuales a partir de modelos en producción

## Monitorear

Validar el sesgo y la importancia relativa de las características a lo largo del tiempo

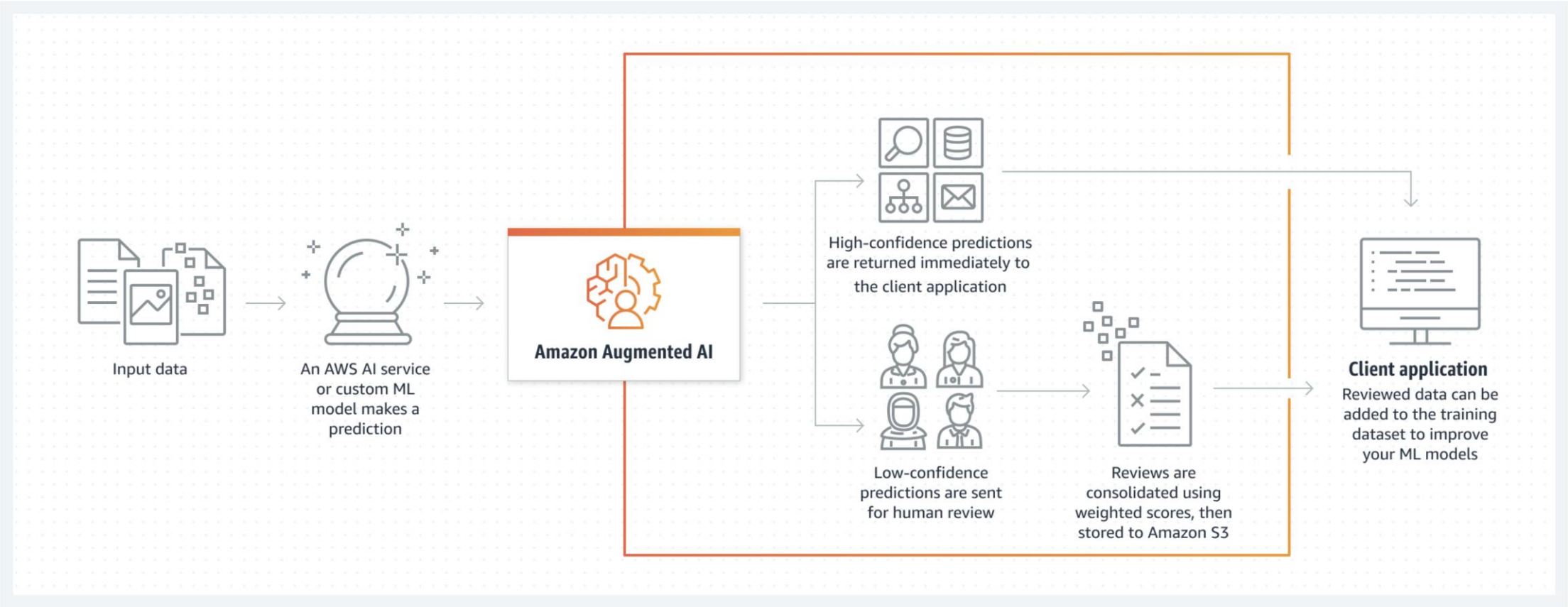
Auditar el desempeño y linaje de todos sus modelos, en un solo lugar

## Gobernanza

Usar herramientas de gobierno diseñadas específicamente para ayudar a implementar Marchine Learning de manera responsable

# Amazon Augmented AI (A2I)

## Implementar revisión humana de predicciones de ML



# Amazon SageMaker Clarify

Detecta sesgos en modelos ML y comprende las predicciones del modelo

### Identifica desequilibrios en los datos

Detecta sesgos durante la preparación de datos

### Revisa el modelo entrenado para ver si hay sesgo

Evalúa el grado en que varios tipos de sesgo están presentes en el modelo

### Explica el comportamiento general del modelo

Comprende la importancia relativa de cada característica para el comportamiento del modelo

### Explicar las predicciones individuales

Comprende la importancia relativa de cada característica para inferencias individuales

### Detectar cambios en el sesgo y en el comportamiento del modelo a lo largo del tiempo

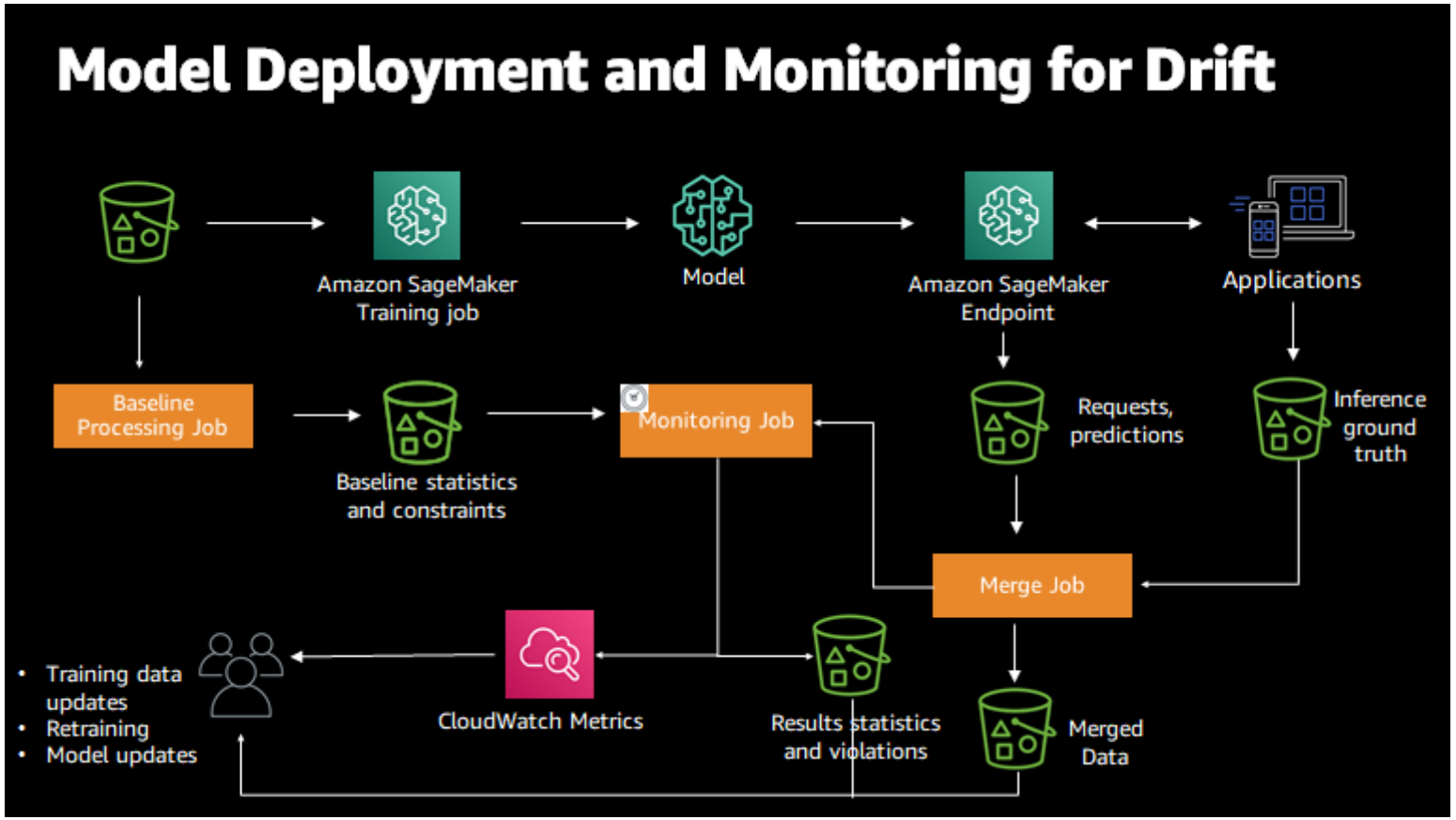
Proporciona alertas y detecta desviaciones a lo largo del tiempo debido a las condiciones cambiantes del mundo real

### Informes automatizados generados

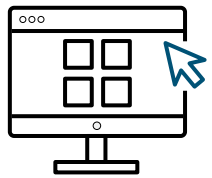
Produce informes sobre sesgos y explicaciones para apoyar presentaciones internas

# SageMaker Model Monitor

- Monitorea automáticamente los modelos ML en producción.
- Detecta problemas de calidad y desviaciones usando reglas
- Alerta a los usuarios cuando ocurren problemas

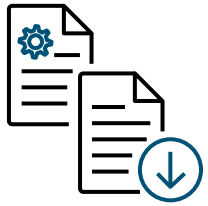


# Funciones de gobierno de ML



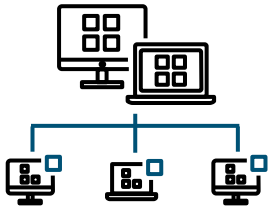
## Amazon SageMaker Role Manager

Define permisos mínimos en minutos



## Amazon SageMaker Model Cards

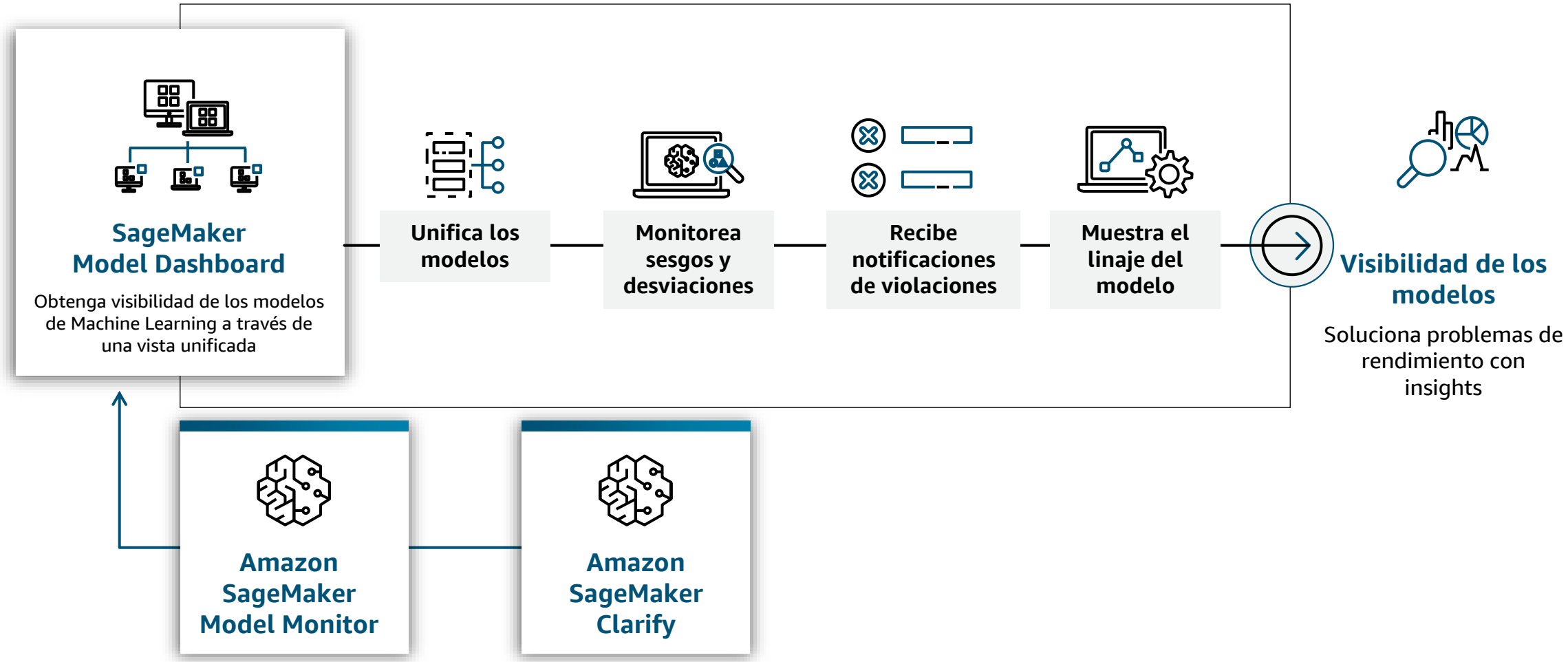
Documenta, recupera y comparte la información necesaria del modelo



## Amazon SageMaker Model Dashboard

Supervisa el rendimiento del modelo a través de una vista unificada

# Amazon SageMaker Model Dashboard



PREPARACIÓN PARA LA CERTIFICACIÓN DE SOCIOS DE AWS

# Dominio 4: Directrices para IA Responsable

## Declaración de tareas 4.2: Reconocer la importancia de los modelos transparentes y explicables

# Modelos transparentes y explicables

## Transparencia, Interpretabilidad y Explicabilidad

- Transparencia: Observando la lógica interna del modelo
- Interpretabilidad: Entendiendo la lógica interna del modelo
- Explicabilidad: Explicación del comportamiento del modelo en términos humanos

## Herramientas de Transparencia

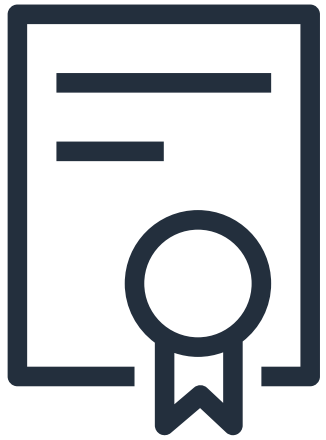
- Amazon SageMaker Model Cards
- Modelos de código abierto
- Documentación sobre datos, licencias, limitaciones

## Tradeoffs

- Transparencia vs. rendimiento/complejidad del modelo
- El balance depende de las necesidades del caso de uso

# Diseño centrado en el ser humano

**Construir un equipo diverso y multidisciplinario**



**Priorizar la educación**

**Equilibrar la IA y el juicio humano**

PREPARACIÓN PARA LA CERTIFICACIÓN DE SOCIOS DE AWS

# Dominio 5: Seguridad, Cumplimiento y Gobernanza para Soluciones de IA

## Declaración de tareas 5.1: Explicar los métodos para proteger los sistemas de IA

# La importancia de la gobernanza y el cumplimiento para los sistemas de IA

Ventajas de la gobernanza y el cumplimiento:

- Administrar, optimizar y escalar la iniciativa de IA organizacional es el núcleo de la perspectiva de gobernanza.
- La gobernanza y el cumplimiento son importantes para los sistemas de IA utilizados en los negocios para garantizar prácticas de IA responsables y confiables.
- La gobernanza ayuda a las organizaciones a establecer políticas, pautas y mecanismos de supervisión claros para garantizar que los sistemas de IA se alineen con los requisitos legales y reglamentarios, además de los principios éticos y los valores sociales.

# Consideraciones de seguridad y privacidad para sistemas de IA

Detección de amenazas

Gestión de vulnerabilidades

Protección de la infraestructura

Prompt injection

Cifrado de datos

# AWS Identity and Access Management

AWS Identity and Access Management

**AWS Identity and Access Management (IAM)** permite administrar el acceso a los servicios y recursos de AWS.

**Características de IAM**

- Usuario de IAM
- Grupo IAM
- Rol de IAM
- Política de IAM
- Autenticación multifactor

# AWS Key Management Service

AWS Key Management Service

- **AWS Key Management Service (AWS KMS)** ayuda a los clientes a realizar operaciones de cifrado mediante el uso de llaves criptográficas.
- Se puede elegir los niveles específicos de control de acceso necesarios para las llaves.

# Amazon Macie

Amazon Macie

- Automatiza la detección de datos confidenciales a escala
- Permite obtener una visibilidad rentable de los datos confidenciales almacenados en Amazon S3
- Evalúa el inventario de buckets de Amazon S3 para controles de seguridad y acceso
- Reduce el tiempo de clasificación con informes procesables de datos confidenciales que se encuentran en Amazon S3.

# Amazon Virtual Private Cloud

Amazon Virtual Private Cloud

- Red virtual aislada en AWS
- Configuración de red personalizable
- Integración perfecta con otros servicios de AWS

# AWS PrivateLink

AWS PrivateLink

- Conectividad privada segura a los servicios de AWS
- Evita internet pública, reduce la exposición de datos
- Simplifica la administración y el escalado de la red

PREPARACIÓN PARA LA CERTIFICACIÓN DE SOCIOS DE AWS

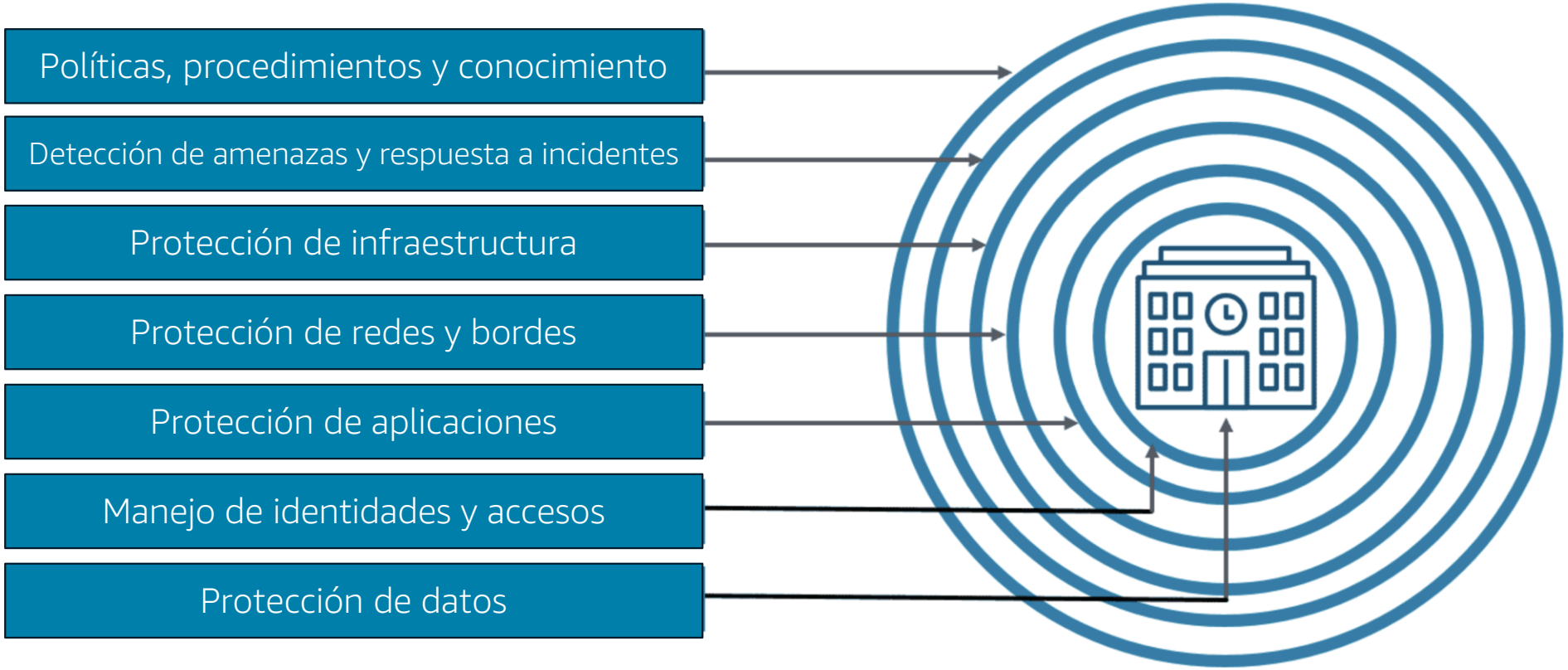
# Dominio 5: Seguridad, Cumplimiento y Gobernanza para Soluciones de IA

## Declaración de tareas 5.2: Reconocer las regulaciones de gobernanza y cumplimiento para los sistemas de IA

# Cumplimiento de los estándares de IA


- Complejidad y opacidad
- Dinamismo y adaptabilidad
- Capacidades emergentes
- Riesgos únicos
- Algoritmo de responsabilidad

# Defensa en profundidad



# ¿Qué estrategias de gobierno de datos están asociadas con la IA?

Las siguientes son algunas estrategias clave de gobierno de datos que las organizaciones pueden considerar.

- Calidad e integridad de los datos
- Protección de datos y privacidad
- Gestión del ciclo de vida de los datos
- IA Responsable
- Estructura y funciones de gobierno
- Intercambio de datos y colaboración.

PREPARACIÓN PARA LA CERTIFICACIÓN DE SOCIOS DE AWS

# Servicios y características de AWS para proteger los sistemas de IA

# AWS CloudWatch

AWS CloudWatch

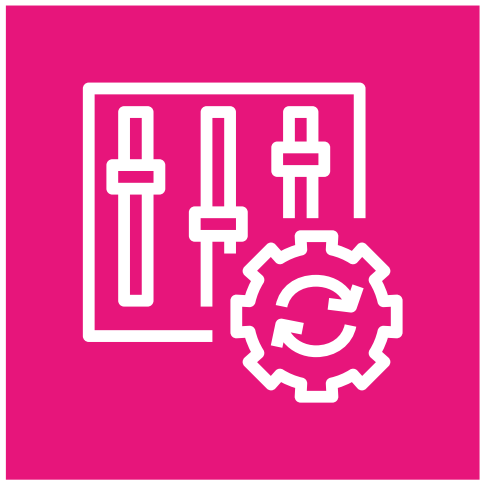
- Supervisa la infraestructura y recursos de AWS y locales en tiempo real
- Proporciona acceso a todas las métricas desde una sola ubicación
- Permite configurar alertas y acciones automáticas en respuesta a métricas

# AWS CloudTrail

AWS CloudTrail

- Realiza un seguimiento de las actividades de los usuarios y las solicitudes de API en toda la infraestructura de AWS
- Filtra los registros generados por las llamadas a la API para ayudar con el análisis operativo y la solución de problemas

# AWS Config



AWS Config

- Descubre y registra automáticamente el estado y configuración de los recursos.
- Realiza un seguimiento de los cambios; recopila un registro histórico de los cambios.
- Evalua los cambios de configuración con respecto a las políticas de cumplimiento.
- Automatiza las actividades de remediación.

# Amazon Inspector

Amazon Inspector

- Amazon Inspector escanea continuamente los recursos, incluidos los siguientes:
  - Instancias de Amazon EC2
  - Imágenes de contenedores en Amazon Elastic Container Registry
  - Funciones de AWS Lambda
- Amazon Inspector se integra con AWS Organizations, AWS Security Hub y Amazon EventBridge.

# AWS Audit Manager

AWS Audit Manager

**AWS Audit Manager** proporciona un proceso automatizado y continuo para lo siguiente:

- Recopila evidencia de controles de seguridad
- Evalúa si los controles funcionan de manera efectiva
- Proporciona informes de evaluación para agilizar la preparación de auditorías

# AWS Artifact

AWS Artifact

**AWS Artifact** proporciona acceso bajo demanda a informes de seguridad y cumplimiento y a ciertos acuerdos en línea.

- Permite acceder a informes de cumplimiento de auditores externos

# AWS Trusted Advisor

AWS Trusted Advisor

- Proporcionar orientación en tiempo real para mejorar el entorno de AWS
- Compara la infraestructura con las prácticas recomendadas de AWS en cinco categorías
- Evalúa e implementa recomendaciones en todas las etapas de implementación

# Matriz de alcance de seguridad de IA generativa

## Un modelo mental para clasificar casos de uso

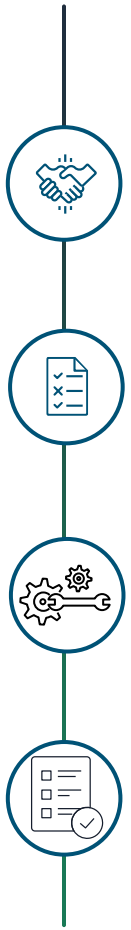
| Alcance 1: Aplicación para consumidor final | Alcance 2: Aplicación empresarial | Alcance 3: Modelos preentrenados | Alcance 4: Modelos afinados | Alcance 5: Modelos autoentrenados |
|---|---|---|---|---|
| Uso de servicios de IA generativa 'públicos'<br><br>Ej: ChatGPT, Midjourney | Uso de una aplicación o SaaS con funciones generativas de IA<br><br>Ej.: Amazon Q Developer | Construyendo tu app en un modelo versionado<br><br>Ej.: Amazon Bedrock base models | Afinamiento de un modelo con sus datos<br><br>Ej: Modelos personalizados de Amazon Bedrock, Amazon Sage JumpStart | Entrenar un modelo desde cero con sus datos<br><br>Ej.: Amazon SageMaker |

Gobernanza y Cumplimiento | Legal y Privacidad | Gestión de Riesgos | Controles | Resiliencia

PREPARACIÓN PARA LA CERTIFICACIÓN DE SOCIOS DE AWS

# Mejores prácticas para implementaciones de IA seguras y compatibles

# **IA Responsable:** Mejores prácticas



Las personas primero

Evaluar el riesgo (uso) caso por caso

Iterar a lo largo del ciclo de vida de la IA

Probar, volver a probar y luego volver a probar

# Infraestructura de la IA generativa:

## Un enfoque seguro

Aislamiento completo de los datos de IA del operador de infraestructura

Capacidad para que los clientes mantengan sus datos de IA aislados

Comunicaciones de infraestructura protegida

# Verificación de conocimientos

# IA responsable en modelos ML

**Usted es un científico de datos que trabaja para una empresa de servicios financieros que utiliza modelos de ML para evaluar las solicitudes de préstamos. La compañía se compromete a promover prácticas de IA responsables para garantizar la equidad y evitar sesgos en sus procesos de toma de decisiones. Su tarea es implementar una solución que pueda ayudar a detectar y mitigar posibles sesgos en el modelo de aprobación de préstamos.**

**¿Cuál es el enfoque más adecuado para atender este requisito?**

A. Utilizar Amazon SageMaker Clarify para monitorear el modelo en busca de posibles sesgos durante la capacitación y la implementación, y aplicar técnicas de mitigación de sesgos como preprocesamiento de datos o ajuste de parámetros del modelo.

B. Revisar manualmente los datos de entrenamiento y los resultados del modelo para identificar cualquier patrón de sesgo, y hacer ajustes a los datos o modelos según sea necesario.

C. Implementar un sistema basado en reglas que aplique criterios predefinidos a las solicitudes de préstamos, asegurando decisiones consistentes e imparciales.

D. Implementar el modelo en un entorno de prueba y monitorear de cerca los resultados para detectar cualquier signo de sesgo antes de lanzarlo a producción.

# IA responsable en modelos ML

**Usted es un científico de datos que trabaja para una empresa de servicios financieros que utiliza modelos de ML para evaluar las solicitudes de préstamos. La compañía se compromete a promover prácticas de IA responsables para garantizar la equidad y evitar sesgos en sus procesos de toma de decisiones. Su tarea es implementar una solución que pueda ayudar a detectar y mitigar posibles sesgos en el modelo de aprobación de préstamos.**

**¿Cuál es el enfoque más adecuado para atender este requisito?**

A. **Utilizar Amazon SageMaker Clarify para monitorear el modelo en busca de posibles sesgos durante la capacitación y la implementación, y aplicar técnicas de mitigación de sesgos como preprocesamiento de datos o ajuste de parámetros del modelo.**

B. Revisar manualmente los datos de entrenamiento y los resultados del modelo para identificar cualquier patrón de sesgo, y hacer ajustes a los datos o modelos según sea necesario.

C. Implementar un sistema basado en reglas que aplique criterios predefinidos a las solicitudes de préstamos, asegurando decisiones consistentes e imparciales.

D. Implementar el modelo en un entorno de prueba y monitorear de cerca los resultados para detectar cualquier signo de sesgo antes de lanzarlo a producción.

# Acceso a FMs en Amazon Bedrock

**Usted es un practicante de IA en una empresa que está ampliando el uso de los servicios de AWS, incluido Amazon Bedrock para Machine Learning. Su equipo está preocupado por asegurar el acceso a los modelos fundacionales previamente entrenados y garantizar que solo los usuarios autorizados puedan acceder a ellos.**

**¿Qué servicio de AWS sería el más adecuado para asegurar el acceso a Amazon Bedrock?**

A. AWS Identity and Access Management (IAM)

B. Servicio de administración de claves de AWS (KMS)

C. Inspector de Amazon

D. Amazon Macie

# Acceso a FMs en Amazon Bedrock

**Usted es un practicante de IA en una empresa que está ampliando el uso de los servicios de AWS, incluido Amazon Bedrock para Machine Learning. Su equipo está preocupado por asegurar el acceso a los modelos fundacionales previamente entrenados y garantizar que solo los usuarios autorizados puedan acceder a ellos.**

**¿Qué servicio de AWS sería el más adecuado para asegurar el acceso a Amazon Bedrock?**

A. **AWS Identity and Access Management (IAM)**

B. Servicio de administración de claves de AWS (KMS)

C. Inspector de Amazon

D. Amazon Macie

# Pregunta coincidente

**Una empresa necesita implementar la gestión y gobierno para su aplicación de IA generativa.**

**Seleccione el servicio de AWS correcto de la siguiente lista que almacenaría cada elemento de Amazon SameMaker. Cada servicio de AWS debe seleccionarse una o más veces**

A) AWS CloudTrail
B) Amazon CloudWatch

1) Logs de Amazon SageMaker Training jobs.
2) Métricas de invocaciones de Amazon SageMaker endpoint.
3) API calls para Amazon SageMaker.
4) Métricas para ejecuciones de Amazon SageMaker Pipeline.

# Pregunta coincidente

**Una empresa necesita implementar la gestión y gobierno para su aplicación de IA generativa.**

**Seleccione el servicio de AWS correcto de la siguiente lista que almacenaría cada elemento de Amazon SameMaker. Cada servicio de AWS debe seleccionarse una o más veces**

A) AWS CloudTrail
B) Amazon CloudWatch

| | | |
|---|---|---|
| 1) | Logs de Amazon SageMaker Training jobs. | **B) Amazon CloudWatch** |
| 2) | Métricas de invocaciones de Amazon SageMaker endpoint. | **B) Amazon CloudWatch** |
| 3) | API calls para Amazon SageMaker. | **A) AWS CloudTrail** |
| 4) | Métricas para ejecuciones de Amazon SageMaker Pipeline. | **B) Amazon CloudWatch** |

# Uso compartido de recursos

## Tutorial en vivo de documentación útil

# Recursos

https://aws.amazon.com/machine-learning/responsible-ai/

https://docs.aws.amazon.com/sagemaker/latest/dg/governance.html

https://docs.aws.amazon.com/sagemaker/latest/dg/model-monitor.html#model-monitor-how-it-works

https://aws.amazon.com/blogs/enterprise-strategy/responsible-ai-best-practices-promoting-responsible-and-trustworthy-ai-systems

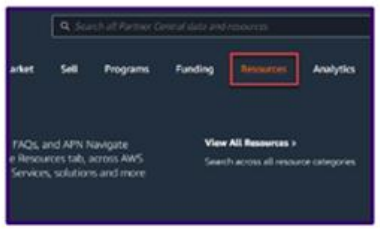
https://aws.amazon.com/blogs/security/securing-generative-ai-an-introduction-to-the-generative-ai-security-scoping-matrix/

# El Centro de Excelencia de IA Generativa

Más de 190 artefactos de IA Generativa

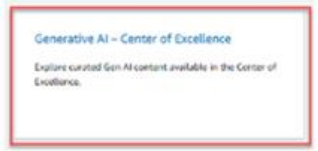
Más 80,000 Interacciones

Más de 1,300 socios de AWS



Partner Central > Resources

Guides




Generative AI – Center of Excellence

Página del CoE de Partner Central

# ¿Preguntas?

# Gracias por asistir a esta sesión