WORLD COMPLIANCE ASSOCIATION *Evento Recomendado*



ONLINE

Anatomía de un incidente: qué pasa cuando un problema toca la IA, la seguridad y los datos a la vez

DESCRIPCIÓN DEL EVENTO

Un incidente relacionado con una herramienta de inteligencia artificial puede activar simultáneamente obligaciones en materia de gobierno de la IA, seguridad de la información, protección de datos y gestión de riesgos. A través de un caso práctico, analizaremos cómo debe actuar una organización desde la prevención hasta la resolución del incidente, abordando la coordinación entre equipos, las obligaciones de notificación y los plazos aplicables, así como las medidas necesarias para evitar que una situación similar vuelva a producirse.

FECHA DEL EVENTO
2026-11-24

LUGAR

HORARIO
16:00-17:30 (hora España)

PRECIO
Gratuito

INFORMACIÓN ADICIONAL

Inscríbete al Evento

Colaboradores

Formalize

WORLD COMPLIANCE ASSOCIATION *Evento Recomendado*



ONLINE

Anatomía de un incidente: qué pasa cuando un problema toca la IA, la seguridad y los datos a la vez

OBJETIVOS

Mostrar, a través de un caso práctico, cómo un mismo incidente activa a la vez obligaciones de gobierno de la IA, seguridad de la información, protección de datos y gestión de riesgos. Ofrecer claves para coordinar a los distintos equipos, cumplir los plazos de cada marco y aprovechar lo aprendido para reforzar el sistema de compliance.

PROGRAMA

El webinar sigue un caso práctico de principio a fin: una empresa de servicios de 500 empleados incorpora una herramienta de IA de un proveedor externo para preseleccionar candidatos. Meses después, el proveedor sufre un ciberataque que expone currículums y datos personales de los candidatos. A lo largo de cuatro fases se analiza qué exige cada marco, qué suele ocurrir en las organizaciones y cómo hacerlo bien en la práctica.

1. **Antes del incidente:** gobierno de la IA, evaluación de riesgos y diligencia debida con el proveedor.
2. **Detección y respuesta:** gestión del incidente de seguridad y coordinación con el proveedor.
3. **Protección de datos:** evaluación de la brecha, notificación a la autoridad y comunicación a los afectados.
4. **Cierre y mejora:** análisis de causas, revisión de riesgos y controles, e informe a la dirección.

Al final de cada fase se abre un turno breve de preguntas de los participantes.

DIRIGIDO A

- Responsables de Compliance, riesgos y control interno.
- Delegados de Protección de Datos (DPO).
- Responsables de seguridad de la información (CISO).
- Abogados y asesores legales de empresa.
- Auditores internos.

PONENTES

Estefanía Morocoa
Head of Product Enablement en Formalize

Nicolás Ballesteros
Compliance Specialist en Formalize