DIGITAL EN DIRECTO

IA aplicada a la Ciberseguridad

Usa la IA con control: protege datos, automatiza con trazabilidad y evita riesgos operativos

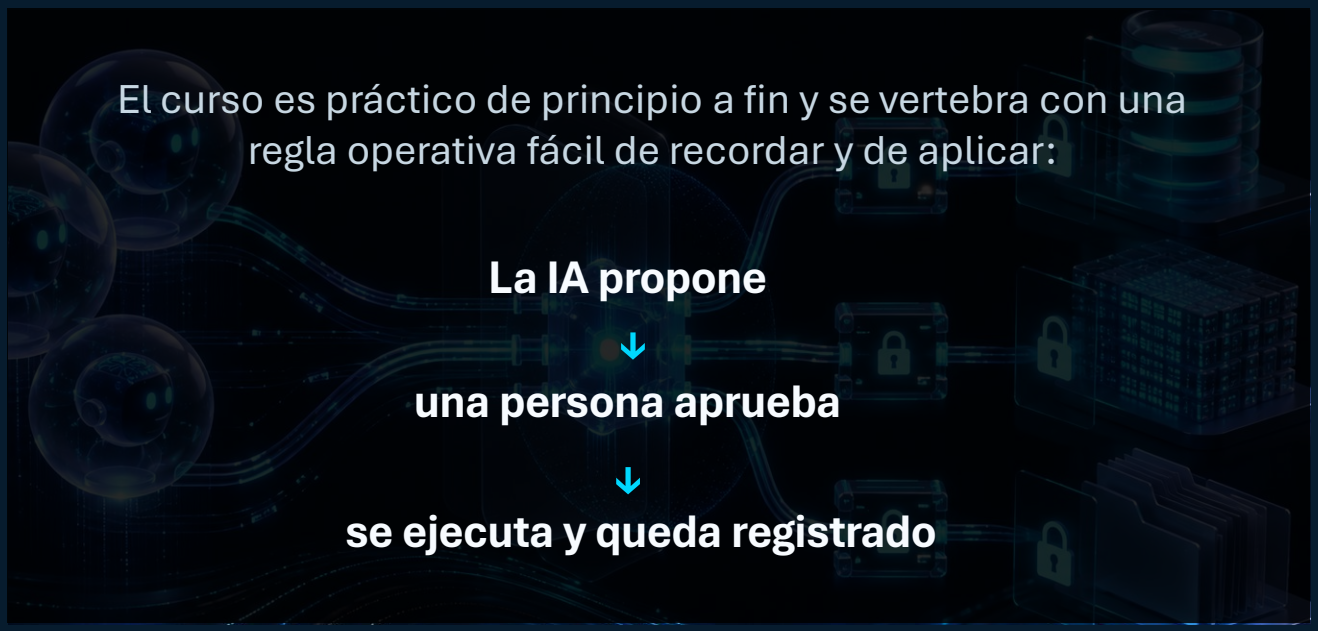
Una formación práctica para integrar la inteligencia artificial en el día a día laboral de forma segura, responsable y orientada a negocio.

Inicio 6 de octubre · 12 horas · formato online en directo

#IA #ciberseguridad #Copilot #M365 #gobernanza #automatizaciónsegura

Cuando la IA entra en tus procesos, la seguridad no puede improvisarse.

Las organizaciones ya trabajan en ecosistemas mixtos: Microsoft 365 y Copilot, Google, herramientas web y aplicaciones de terceros. El valor aparece cuando la IA se conecta a datos, permisos, procesos y APIs. Ahí también nace el riesgo.



01 De “usar IA” a “usar IA con control”

El objetivo no es frenar la innovación: es convertirla en un hábito seguro, con mínimos privilegios, aprobación humana, trazabilidad y privacidad por diseño.

02 Más productividad, menos exposición

El curso traduce amenazas, controles y marcos normativos en decisiones concretas para dirección, riesgo, compliance y equipos de ciberseguridad.

Por qué esta formación es relevante ahora

01 Amenazas potenciadas por IA

Deepfakes, voice cloning, prompt injection y fraude del CEO elevan el impacto de ataques conocidos.

02 El valor está en los conectores

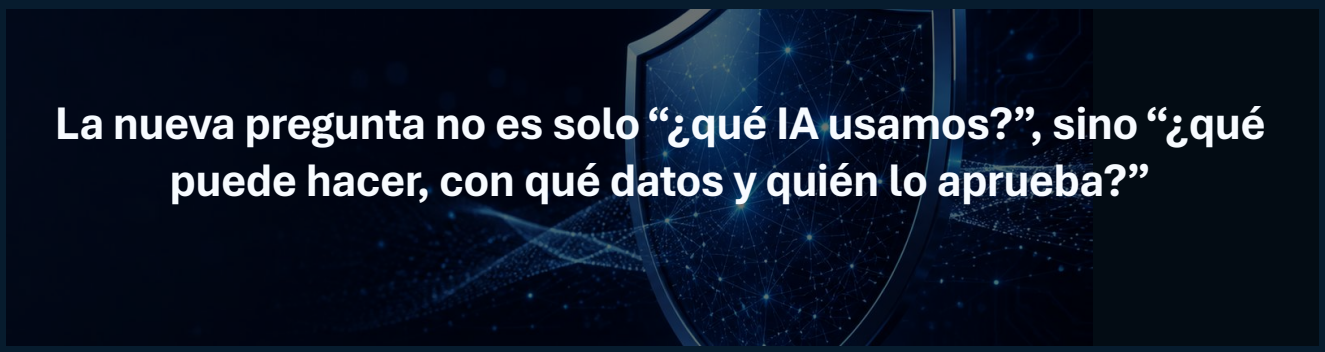
MCP, APIs y agentes permiten automatizar, pero también exponen datos, permisos y acciones irreversibles.

03 Permisos excesivos = incidentes graves

El mínimo privilegio, también para agentes de IA, es la primera línea de defensa operativa.

04 La gobernanza ya no es opcional

AI Act, ISO 42001 y NIST AI RMF obligan a decidir qué se aprueba, quién responde y cómo se comunica el riesgo.



Objetivos de la formación

- Comprender el panorama de amenazas potenciadas por IA y sus implicaciones para negocio.
- Identificar riesgos de modelos, prompt injection, deepfakes, voice cloning y fraude BEC.
- Aplicar la regla IA propone → persona aprueba → ejecución registrada.
- Configurar criterios de uso seguro en Microsoft 365, Copilot y ecosistemas mixtos.
- Definir controles de mínimo privilegio, backups, trazabilidad, aprobación humana y privacidad por diseño.
- Construir un plan de aplicación 30/60/90 adaptado a la organización.

Resultado esperado

Salir con criterio para usar herramientas de IA con control: qué permitir, qué bloquear, qué registrar y cómo convertir la seguridad en una práctica diaria sin perder velocidad.

A quién va dirigido

- Dirección, riesgo y compliance: obligaciones, inversión, prioridades y comunicación del riesgo.
- Responsables de ciberseguridad: configuración real de controles, laboratorios y recetario aplicable.
- Equipos de sistemas, IT, datos, IA y transformación digital que activan herramientas y automatizaciones.
- Mandos intermedios que necesitan criterio para usar IA sin exponer información sensible.

Especialmente útil para organizaciones que...

trabajan con Microsoft 365 / Copilot, Google, IA web y apps de terceros; quieren conectar la IA a datos de empresa; o necesitan una guía común para decidir permisos, automatizaciones y límites.

Modalidad

Digital en directo, a través del campus APD.

Duración

12 horas · seis sesiones síncronas de 2 horas cada una

Enfoque

Ruta común para dirección y perfiles técnicos, con profundidad ajustada a cada rol y ejercicios para trasladar lo aprendido a la realidad de cada empresa.

Contenido del curso

- Apertura: vuestro flujo de trabajo y dónde está el riesgo real.
- Panorama de amenazas potenciadas por IA. Casos reales (fraude del CEO con voice cloning, Europol).
- Seguridad de modelos e IA ofensiva (OWASP LLM). DEM Oen directo: prompt injection y deepfake.
- AI Act y gobernanza (ISO 42001, NIST AI RMF). Qué decide la dirección y cómo comunicar el riesgo.
- Seguridad según el dispositivo: móvil, aplicación y navegador. Qué activar y qué desactivar siempre.
- SOC asistido por IA
- Objetivos prácticos.
- Microsoft 365 + Copilot con control: MFA y Conditional Access, permisos, qué activar/desactivar. HANDS-ON.
- Mínimo privilegio y gestión de accesos (también identidad por agente de IA).
- Copias de seguridad 3-2-1 con copia inmutable y prueba de restauración. HANDS-ON.
- Agentes, MCP, conectores y APIs: automatización segura con aprobación humana. Lista de qué NO entra en la IA.
- Simulacro BEC / fraude del CEO: verificación fuera de banda.
- Plan de aplicación 30/60/90, consola de referencia y mini - encuesta.

Metodología

Sesiones síncronas en tiempo real, con un enfoque práctico y orientado a la aplicación inmediata.

01 Marco y decisión

Conceptos clave, impacto en negocio y criterios para priorizar.

02 Demos en directo

Deepfake, voice cloning y prompt injection para visualizar el riesgo.

03 Hands-on guiado

M365/Copilot, accesos, backups, GitHub y automatizaciones.

04 Plan final

Checklist, plan 30/60/90 y acciones concretas por rol.

Qué se lleva el participante

- Consola/recetario de referencia: M365/Copilot, accesos, backups, agentes y detección.
- Checklist de seguridad por dispositivo: qué activar y qué desactivar.
- Lista de qué NO entra en la IA y criterios de automatización segura.
- Plan de aplicación 30/60/90 personalizable por organización.
- Material de sesión y banco de preguntas y respuestas.

Experto del programa

Juan Ma Perals

Ciberseguridad & IA

Juan Ma Perals es asesor en ciberseguridad, gobernanza de IA y automatización segura. Ayuda a empresas, pymes y directivos a entender riesgos digitales complejos, adoptar herramientas innovadoras con criterio y convertir la ciberseguridad y la inteligencia artificial en decisiones prácticas de negocio.

Es experto colaborador en APD además de CEO y fundador de PersalOne, Presidente Fundador del Global CISO Council Spain Chapter, Experto Evaluador para la Comisión Europea, NATO DIANA Mentor y EUDIS Defence & Dual-Use Expert, participando en iniciativas vinculadas a innovación, seguridad, tecnología, defensa y entornos de doble uso. También forma parte de la Junta Directiva de la Asociación Territorio Compliance, donde trabaja en la conexión entre cumplimiento, gobernanza de IA y realidad empresarial.

Como docente, su enfoque es muy práctico: enseñar a hacer. Sus formaciones ayudan a equipos y directivos a comprender el riesgo, adquirir criterio, usar herramientas actuales y construir una base sólida para avanzar en IA, ciberseguridad y automatización sin comprometer datos, operativa ni reputación.

Durante los últimos años ha mentorizado startups y proyectos tecnológicos en programas vinculados a INCIBE Emprende, incluyendo colaboraciones en programas de incubación y aceleración junto a Sherpa Tribe con la colaboración de la UNIR. En este contexto ha acompañado proyectos en fases tempranas, ayudándoles a aterrizar su propuesta, reforzar su enfoque tecnológico y conectar innovación, seguridad y mercado.

Su trabajo combina visión técnica, capacidad pedagógica y enfoque empresarial para ayudar a las empresas a mejorar productividad, reducir riesgos, cumplir con nuevas exigencias regulatorias y tomar mejores decisiones antes de que un problema técnico se convierta en un problema de negocio.

“La IA debe acelerar el trabajo, no multiplicar el riesgo: propone, una persona aprueba y todo queda registrado.”

Formación Open e In-Company

Disponible en modalidad open para profesionales y también adaptable en formato in-company para equipos de dirección, compliance, ciberseguridad, IT, datos y transformación digital.

Información práctica formación open

Fecha: 6, 8, 13, 15, 20 y 22 de octubre
Horario: de 10:00 a 12:00 · 12 horas en 6 sesiones de 2 horas
Modalidad: online en directo a través del campus APD

Cuota de inscripción formación open

Socios Globales / Genius APD: 590 € + IVA
Socios Protectores APD: 472 € + IVA
No socios: 944 € + IVA

In-Company

Programa adaptable para compañías que quieran formar a sus equipos en uso seguro de IA, gobierno, automatización con control, M365/Copilot y resiliencia operativa.

¿Hablamos?

+34 91 523 79 00 · jtovar@apd.es · www.apd.es