



**PROMUOVE 9 Ottobre 2026**

**un seminario in modalità mista FAD Sincrona/Presenza** sala Verde del APA Confartigianato  
Imprese Milano Monza e Brianza (fino ad un massimo di 30 posti) via Gianbattista Stucchi, 64 Monza

**IA LOCALE nella PA: architetture, sicurezza e governance**  
**RESILIENZA, SICUREZZA, SOVRANITA' TECNOLOGICA E CONTINUITA' OPERATIVA**

**OBIETTIVI**

**Ingegneri per l'Italia Digitale.**  
**Competenza, responsabilità, territorio**



L'evento approfondisce opportunità e limiti dell'AI generativa nella Pubblica Amministrazione, confrontando modelli locali, infrastrutture on-premise e servizi cloud, anche qualificati, rispetto a costi, prestazioni, protezione dei dati e governance.

Il programma affronta i rischi cyber, con una sessione CERT AgID, la progettazione di architetture sicure e le responsabilità di amministrazioni, fornitori e utilizzatori. Particolare attenzione è dedicata all'accesso ai documenti interni tramite RAG, alla tracciabilità e al controllo degli output.

Una demo su documentazione non sensibile mostrerà il funzionamento di una knowledge base locale, evidenziando fonti, possibili allucinazioni e controlli di sicurezza. La tavola rotonda conclusiva discuterà casi d'uso, competenze necessarie e complementarità tra cloud e on-premise.

**MODALITA' di PARTECIPAZIONE**

**ISCRIZIONE:** [www.ordineingegneri.mb.it](http://www.ordineingegneri.mb.it)

previa registrazione

Evento valido per il rilascio di **3 crediti formativi** professionali (D.P.R. 137 del 07/08/2012) per gli iscritti all'albo degli ingegneri OIMB

**COSTO PARTECIPAZIONE:**

**Presenza: gratuito (max 30 posti)**

**FAD Sincrona: € 20,00**

**PROGRAMMA**

14.00 Saluti istituzionali – **Ing. Pierpaolo Cicchiello**

Presidente **Ordine Ingegneri Provincia MB**

14.10 **Ing. Carmelo Alessandro Bonaccorso**

Breve introduzione e presentazione dei Relatori

14.15 **Ing. Gianni Amato, CERT AgID** - Rischi cyber dei modelli AI locali

Esposizione accidentale di dati e prompt; prompt injection e data poisoning; supply chain dei modelli e dei pacchetti open source; gestione di pesi, checkpoint e dataset; logging, auditing e controllo accessi; rischi da plugin, agenti e strumenti collegati al modello.

15.45 **Ing. Enrico Frumento, Cybersecurity Research Lead @CEFRIEL**

L'AI promette controllo, velocità, difesa. Nella pratica, è proprio questa promessa a diventare il punto cieco: si adotta lo strumento prima di aver stabilito entro quali limiti può operare. Per i CIO, il momento richiede una lettura concreta, distante dal rumore che accompagna ogni ondata tecnologica. L'AI sta già modificando il profilo del rischio, le catene di responsabilità e i presupposti su cui regge la governance della sicurezza. Adesso, non in un futuro prossimo.

Il pericolo vero oggi come oggi non è tanto una AI che allucina, ma una AI che allucina con le credenziali.

16.30 **Luca Sambucci, AI Security** - Prompt injection e attacchi all'IA: casi reali.

Per attaccare un sistema di IA generativa non serve un exploit, basta una frase scritta nel posto giusto. Vedremo cos'è una prompt injection e in che modo manipola gli LLM per far restituire agli attaccanti gli output desiderati. Quando al modello si collegano memoria e strumenti, l'IA diventa agentica, e quella frase smette di essere semplice testo, diventando un'azione eseguita con le credenziali dell'organizzazione. La superficie di attacco si allarga a tutto ciò che il modello è autorizzato a toccare e la catena di responsabilità si allunga con lei.

Il mercato ha risposto con una nuova categoria di difese, gli strumenti di AI detection and response (AIDR). Vedremo che cosa intercettano davvero sotto il red teaming automatizzato, cosa lasciano passare e quanto sono davvero utili.

Porteremo in sala i casi reali: prompt injection diretta e indiretta, manipolazione dei modelli, abuso degli agenti e degli strumenti collegati. Poi metteremo un modello sotto attacco dal vivo, per vedere quanto regge.

17.20 – 18.00 Dibattito

Responsabile Scientifico, tecnico organizzativo

**Ing. Carmelo Alessandro BONACCORSO**

Commissione Artificial Intelligence

Ordine degli Ingegneri della Provincia  
di Monza e della Brianza

ORGANIZZAZIONE: ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI MONZA E DELLA BRIANZA

Via A.G. Passerini 2 - 20900 Monza (MB) Italy - tel. +39.039.2301911 - fax +39.039.2307347

[segreteria@ordineingegneri.mb.it](mailto:segreteria@ordineingegneri.mb.it) - [www.ordineingegneri.mb.it](http://www.ordineingegneri.mb.it)