

# Sicurezza del dato, responsabilità professionale e il ruolo dell'AI nella professione che cambia

*Programma e traccia organizzativa del seminario*

|                       |                                                  |
|-----------------------|--------------------------------------------------|
| <b>Data</b>           | Venerdì 23 ottobre 2026                          |
| <b>Sede</b>           | Ordine degli Ingegneri della Provincia di Biella |
| <b>Welcome coffee</b> | 14:30                                            |
| <b>Inizio lavori</b>  | 15:00                                            |
| <b>Moderatore</b>     | Gianluca Giovanardi – CEO INOMA                  |

## 1. Obiettivo e filo conduttore

L'Intelligenza Artificiale costituisce il filo conduttore dell'intero pomeriggio. Il seminario mette in relazione AI, gestione del dato, Privacy/GDPR, Cybersecurity, perdita dei dati e continuità operativa, con un taglio concreto rivolto alla professione dell'ingegnere.

**Percorso narrativo:** AI → Dato → Privacy → Cybersecurity → Perdita dati → Continuità operativa.

## 2. Programma

| ORARIO        | INTERVENTO                                                                                | RELATORE                                      |
|---------------|-------------------------------------------------------------------------------------------|-----------------------------------------------|
| 14:30 – 15:00 | Accoglienza, registrazione partecipanti e welcome coffee                                  |                                               |
| 15:00 – 15:10 | Apertura e saluti istituzionali                                                           | Ing. Alberto Prospero                         |
| 15:10 – 15:20 | Introduzione – AI, dati e sicurezza: una trasformazione che riguarda già la professione   | Gianluca Giovanardi – CEO INOMA e Moderatore  |
| 15:20 – 15:45 | L'AI e l'ingegnere: opportunità, rischi e trasformazione della professione                | Botchi / Sealo – Mark Comerro                 |
| 15:45 – 16:10 | AI, Privacy e GDPR: dati, obblighi e responsabilità professionale                         | Avv. Gianluca Buffa                           |
| 16:10 – 16:35 | Cybersecurity nell'era dell'AI: nuove minacce e protezione del dato                       | Marco Vallini – INOMA                         |
| 16:35 – 17:05 | Perdita dei dati e continuità operativa: prevenzione, backup, ripristino e infrastrutture | Marco Vallini – INOMA                         |
| 17:05 – 17:35 | Tavola rotonda – AI, dati, sicurezza e responsabilità professionale                       | Tutti i relatori – modera Gianluca Giovanardi |
| 17:35 – 17:55 | Q&A e confronto con il pubblico                                                           | Tutti i relatori                              |
| 17:55 – 18:00 | Conclusioni e chiusura dei lavori                                                         | Gianluca Giovanardi / Ordine                  |
|               |                                                                                           |                                               |

### 3. Traccia dei singoli interventi

#### Gianluca Giovanardi – Introduzione (10 min)

- L'AI è già entrata nell'attività quotidiana di aziende e professionisti.
- Passaggio dall'AI generativa agli Agent AI, capaci di interagire con documenti, applicazioni e processi.
- Il dato come patrimonio centrale dell'AI: quali informazioni affidiamo ai sistemi, dove vengono elaborate e chi può accedervi.
- Presentazione del percorso del seminario: AI, Privacy, Cybersecurity e continuità operativa.
- Messaggio chiave: l'adozione dell'AI deve procedere insieme alla corretta gestione e protezione del dato.

#### Botchi / Sealo – AI e professione (25 min)

- Evoluzione da chatbot e AI generativa agli Agent AI.
- Differenza tra interrogare un'AI e affidarle attività e processi.
- Interazione con documenti, email, gestionali, database e procedure.
- Casi d'uso per studi professionali: documentazione tecnica, ricerca, automazione, assistenza interna e interazione con i clienti.
- Esempio concreto di Botchi con taglio tecnico-divulgativo, non commerciale.
- Introduzione al tema dei dati necessari all'AI e passaggio all'intervento Privacy.

#### Avv. Gianluca Buffa – Privacy, GDPR e AI (25 min)

- Tipologie di dati e informazioni affidate agli strumenti AI.
- Utilizzo di contratti, progetti, relazioni tecniche, email, dati personali e informazioni riservate.
- GDPR, AI Act, ruoli e responsabilità nel trattamento.
- Rapporto con fornitori e piattaforme AI e aspetti legati ai servizi cloud.
- Policy interne per l'utilizzo dell'AI.
- Responsabilità del professionista rispetto agli output dell'AI.
- Caso pratico: utilizzo di un servizio AI pubblico per elaborare un documento riservato di un cliente.

#### Marco Vallini – Cybersecurity nell'era dell'AI (25 min)

- AI come strumento di difesa e come acceleratore delle minacce.
- Phishing e social engineering evoluti, deepfake e impersonificazione.
- Furto delle credenziali e protezione delle identità digitali.
- MFA, controllo degli accessi, endpoint e protezione dei dispositivi.
- Sicurezza dei dati utilizzati dagli Agent AI e rischi delle integrazioni/API.
- Logging, monitoraggio e principio del minimo privilegio.
- Messaggio chiave: maggiore autonomia dell'AI richiede maggiore controllo sulle autorizzazioni.

#### Perdita dati e continuità operativa (30 min)

- Cause di indisponibilità o perdita del dato: guasti, errore umano, ransomware, cancellazioni e indisponibilità dei servizi.
- Differenza tra backup e continuità operativa.
- RTO e RPO spiegati in modo semplice.
- Backup protetti/immutabili, disaster recovery e test periodici di ripristino.
- Ridondanza delle infrastrutture; cloud, on-premise e sistemi ibridi.
- Dove risiedono i dati utilizzati dall'AI e confronto tra AI locale e AI cloud dal punto di vista infrastrutturale.

- Domanda conclusiva: se domani tutti i sistemi fossero indisponibili, quanto tempo servirebbe realmente per tornare operativi?

## 4. Tavola rotonda finale

Scenario comune proposto dal moderatore: uno studio di ingegneria introduce un Agent AI collegato alla propria documentazione, alle email, ai progetti e ad alcuni sistemi aziendali.

- Botchi / Sealo: quali attività possiamo realmente affidare oggi a un Agent AI?
- Avv. Gianluca Buffa: quali limiti dobbiamo porci nell'utilizzo dei dati e quali responsabilità emergono?
- Marco Vallini: come evitare che l'Agent AI diventi un nuovo punto di accesso alle informazioni aziendali?
- Infrastrutture: dove devono risiedere dati e servizi e cosa succede se diventano indisponibili?
- Domande incrociate: cloud o AI locale? Policy interne? Controllo degli accessi? Responsabilità in caso di errore? Continuità operativa?