



CTRL+ ALT+ FUTURE

RIAVVIARE PER INNOVARE?

- **TECNOLOGIE EMERGENTI.**
- **NUOVI SCENARI DI RISCHIO.**
- **MODELLI DI GOVERNO IN EVOLUZIONE.**

DATA

12-13 ottobre 2026

SEDE

Palazzo Lombardia

Auditorium Testori

CITTA

Milano

Piazza Città di Lombardia 1

Tecnologia. Rischio. Governo.

L'intelligenza artificiale, il quantum computing e le capacità cyber stanno ridefinendo il rapporto tra innovazione, competizione e sicurezza.

La loro natura dual use ne amplifica il valore economico e strategico e, al tempo stesso, il potenziale destabilizzante. Dipendenze, interconnessioni e concentrazioni tecnologiche incidono ormai sulla continuità delle organizzazioni, sulla resilienza delle filiere e sulla stabilità dei sistemi economici.

Il 40° Convegno Nazionale AIEA affronta questa evoluzione da due prospettive complementari: i nuovi scenari del rischio tecnologico e i modelli chiamati a governarlo.

12 OTTOBRE

La nuova geografia del rischio tecnologico

Geopolitica, tecnologie emergenti e nuovi fattori di rischio sistemico

La prima giornata mette a fuoco le trasformazioni che stanno ridefinendo il contesto tecnologico e di rischio, osservandone le implicazioni economiche, strategiche e geopolitiche attraverso il confronto tra istituzioni, ricerca, industria e sistema finanziario.

13 OTTOBRE

Governare tecnologie e rischi in evoluzione

Governance, ICT Risk Management, resilienza e assurance

La seconda giornata sposta la prospettiva sui modelli di governo: responsabilità, processi decisionali, gestione del rischio, resilienza e assurance di fronte a tecnologie, dipendenze e minacce in continua evoluzione.

A CHI SI RIVOLGE

Board e C-Suite

Risk, Audit e Compliance

CISO, CIO e Technology Leadership

Istituzioni, Autorità, Advisory e Professionisti

ISCRIZIONI

Soci AIEA

Partecipazione gratuita previa iscrizione. Posti in presenza limitati.

Non Soci AIEA

Per informazioni sulle modalità di partecipazione: aiea@aiea.it

CREDITI PROFESSIONALI

Per i Soci AIEA, la partecipazione consente il riconoscimento dei crediti CPE ISACA validi per il mantenimento delle certificazioni professionali.

SEGUICI SU LINKEDIN



**AIEA - Associazione Italiana
Information Systems Auditors**

01 La nuova geografia del rischio tecnologico

Geopolitica, tecnologie emergenti e nuovi fattori di rischio sistemico

08:45-09:30 **Registrazione Ospiti e Welcome Coffee**

09:30-09:50 **Apertura dei lavori e saluti istituzionali**

09:50-10:20 **CTRL + ALT + FUTURE: ripartire per innovare e mantenere il controllo**

L'IA ha smesso di limitarsi a rispondere: ora agisce, decide e trasforma interi settori su scala nazionale, e si riparte proprio da qui, da ciò che questo cambiamento richiede davvero alla leadership. Esploreremo il divario crescente tra ciò che l'IA può fare e ciò che le organizzazioni sono pronte a governare, e perché velocità e controllo debbano essere costruiti insieme, non trattati come opposti. Attingendo all'esperienza diretta di ISACA - dal suo AI Innovation Lab al lavoro con le comunità locali in Europa - mostra cosa significhi colmare quel divario nella pratica, con un invito diretto all'azione: ISACA Global, i chapter e i membri, insieme, per costruire, localizzare e far crescere la fiducia nell'era dell'IA.

Massimo Migliuolo, Chair, ISACA Global Board of Directors

10:20-11:05 **La tecnologia nella nuova geografia del potere**

Capacità di calcolo, infrastrutture digitali, dati, tecnologie emergenti e catene di fornitura sono diventati fattori della competizione economica e geopolitica. Una lettura delle dinamiche globali che stanno trasformando dipendenze tecnologiche e rapporti di forza tra Paesi, imprese e mercati.

Federico Fubini, Inviato ed editorialista, Vicedirettore del Corriere della Sera

11:05-11:35 **L'AI non è una commodity: rischi e governo di una tecnologia inevitabile**

L'AI è ormai inevitabile per le imprese, ma i rischi più rilevanti dipendono soprattutto da come viene adottata: come un bene da acquistare, invece che come un sistema da progettare e governare. L'intervento distingue gli elementi transitori da quelli destinati a consolidarsi, mette a fuoco gli impatti su processi, competenze e controlli e propone alcuni criteri per usarla. Particolare attenzione è dedicata ai costi e ai rischi della dipendenza da modelli e piattaforme, e alla necessità di preservare la capacità di giudicarli e, quando serve, di cambiarli.

Alfonso Fuggetta, Professore ordinario di Informatica, Politecnico di Milano

11:35-12:00 **Coffee Break**

12:00-13:15 **Intelligenza artificiale, decisione e responsabilità**

L'evoluzione dell'AI sta ampliando gli spazi in cui i sistemi possono analizzare, pianificare e agire con livelli crescenti di autonomia. Cambia così il rapporto tra decisione, responsabilità e controllo, con implicazioni che attraversano tecnologia, diritto e dimensione umana. Un confronto a più voci su ciò che accade quando una parte crescente delle decisioni e delle azioni viene affidata ai sistemi intelligenti.

don Luca Peyron, Istituto Italiano per l'Intelligenza Artificiale – AI4I

Raffaele Giarda, Partner, ADVANT Nctm

Oreste Pollicino, Professore ordinario di Diritto costituzionale, Università Bocconi, Founder Pollicino Advisory

modera **Anna Capoluongo**, Avvocato e Data Protection Officer

13:15-14:30 **Light Lunch presso Foyer Testori**

14:30-15:00

Rischio tecnologico e resilienza nel settore finanziario

L'evoluzione delle minacce, le interdipendenze dell'ecosistema finanziario e l'emergere di nuove tecnologie stanno modificando il profilo di rischio del settore. La prospettiva della Vigilanza sui principali fattori di attenzione e sulle implicazioni per la resilienza del sistema finanziario.

Valentina Cappa, Vice Capo Divisione Supporto Statistico e Informatico, Banca d'Italia

15:00-15:30

Prepararsi al quantum computing: implicazioni, rischi e scelte

Il quantum computing è ancora in una fase di sviluppo, ma alcune delle sue implicazioni richiedono già oggi scelte consapevoli da parte delle organizzazioni. Sicurezza e protezione delle informazioni da un lato, nuove capacità di calcolo, sperimentazione e competenze dall'altro evolvono secondo tempi diversi, in un contesto nel quale la distanza dalla prossima generazione di sistemi quantum si misura ormai in anni, non in decenni. L'intervento propone una lettura del quantum dal punto di vista del rischio e delle decisioni, per distinguere ciò che richiede preparazione immediata, ciò che va esplorato progressivamente e ciò che può attendere.

Mario Onorato, Practice Leader, Risk & Compliance, IBM Promontory

15:30-16:00

Quantum computing e maturità del sistema finanziario

L'Osservatorio CIPA sul Quantum Computing presenta le attività in corso e le priorità emerse nel confronto nazionale, europeo e internazionale, insieme alla nuova rilevazione sul livello di maturità del settore bancario e finanziario rispetto alle tecnologie quantistiche e alla crittografia post-quantistica. Strategia, governance, investimenti, competenze e iniziative di implementazione diventano dimensioni misurabili, anche attraverso indicatori destinati a supportare nel tempo il monitoraggio dell'evoluzione del settore e il benchmarking.

Sonia Guida, Segreteria Tecnica CIPA, Banca d'Italia

Katia Boria, Segreteria Tecnica CIPA, Banca d'Italia

16:00-16:30

Coffee Break

16:30-17:45

Dalla ricerca alla preparazione: il quantum computing nelle strategie delle organizzazioni

Il quantum computing sta passando dalla frontiera della ricerca a una questione concreta di strategia tecnologica e sicurezza. Tempi di maturazione, casi d'uso, impatto sulla crittografia e transizione post-quantum pongono già oggi una domanda alle organizzazioni: cosa è davvero rilevante e come prepararsi senza inseguire l'hype? Un confronto tra ricerca e operatori che, da prospettive diverse, stanno sperimentando queste tecnologie e lavorando sulle implicazioni del loro sviluppo.

Massimo Bernaschi, Dirigente Tecnologo, Consiglio Nazionale delle Ricerche - CNR

Antonio Greco, Università di Siena e Istituto Nazionale di Fisica Nucleare - Sezione di Pisa

Davide Corbelleto, Distinguished Quantum Specialist, Intesa Sanpaolo

Mario Trinchera, Technical Coordinator, CERTFin

modera **Stefano Scapecchi**, Senior ICT Auditor e docente ISACA

17:45-18:00

Chiusura della prima giornata

18:00-20:00

Cocktail di Networking presso Foyer Testori

02 Governare tecnologie e rischi in evoluzione

Governance, ICT Risk Management, resilienza e assurance

08:45-09:15 **Registrazione Ospiti e Welcome Coffee**

09:15-09:30 **Apertura lavori della seconda giornata**

09:30-10:00 **Governare l'innovazione: rischio e resilienza nelle decisioni strategiche**

Le interdipendenze tecnologiche, l'evoluzione delle minacce e la velocità della trasformazione rendono insufficienti verifiche episodiche e modelli di controllo separati dai processi decisionali. La prospettiva Forrester su come integrare Risk e Security nelle scelte di business, facendo della governance tecnologica uno strumento per orientare decisioni, investimenti e priorità e rafforzare la resilienza senza frenare innovazione e crescita.

Edoardo Zavarella, Principal Consultant, Forrester

10:00-10:40 **Verso la resilienza strutturale: la roadmap ACN per le misure di sicurezza rafforzate**

L'Agenzia per la Cybersicurezza Nazionale (ACN) ha delineato la transizione verso la terza fase attuativa del decreto NIS2, avviando l'introduzione delle misure di sicurezza rafforzate di lungo termine. Questa transizione segna il decisivo passaggio dai requisiti minimi di base a una postura di resilienza strutturale e continuativa nel tempo, supportata da un rigoroso piano di controlli e ispezioni. L'intervento illustrerà le principali novità definite dall'Autorità e gli obiettivi della consultazione pubblica, basata sui principi di proporzionalità e gradualità, per integrare e sostituire progressivamente le misure adottate nella prima fase.

Prefetto Milena Antonella Rizzi, Capo Servizio Regolazione, Agenzia per la Cybersicurezza Nazionale (ACN)

dialoga con la relatrice **Luca Savoia**, Partner, Forvis Mazars

10:40-11:15 **Test, esercitazioni e simulazioni: misurare la preparazione nell'era delle minacce accelerate e degli scenari emergenti**

In un contesto di minacce più rapide, complesse e interconnesse, piani e controlli non sono sufficienti a rappresentare la capacità effettiva di risposta di un'organizzazione. Test, esercitazioni e simulazioni consentono di verificare sul campo processi decisionali, coordinamento, dipendenze, capacità di risposta e ripristino dei servizi. Le evidenze che ne derivano permettono non solo di individuare vulnerabilità e aree di miglioramento, ma anche di orientare priorità, investimenti e scelte di governo. Una prospettiva sul ruolo del testing nella resilienza operativa digitale, anche attraverso approcci threat-led e framework come TIBER - con particolare attenzione agli scenari emergenti legati alle tecnologie di frontiera, inclusi i rischi cyber da modelli di AI avanzati e le implicazioni della transizione verso soluzioni crittografiche quantum-safe.

Mauro De Santis, Policy Officer, Banca d'Italia

11:15-11:45 **Coffee Break**

11:45-12:30

Vulnerabilità, terze parti e difesa della superficie di attacco

La gestione delle vulnerabilità, il controllo della catena di fornitura e l'impiego di strumenti avanzati per la difesa delle infrastrutture. Le evidenze e gli orientamenti emersi dai tavoli di lavoro di settore di ABI Lab, EBF e CERTFin.

Roberto Tordi, Ricerca ABI Lab e CERTFin

Marco Rotoloni, co-Responsabile Ricerca ABI Lab

12:30-13:15

Governare e assicurare il rischio tecnologico: AIIA e AIEA a confronto

Tecnologie emergenti, nuove minacce e regolamentazione stanno ampliando il perimetro del rischio tecnologico. AIIA e AIEA si confrontano su come evolvono governance e assurance e sul contributo di Internal Audit e IT Governance alla resilienza dell'organizzazione.

Massimiliano Bosio, Presidente, AIIA - Associazione Italiana Internal Auditors

Luca Pertile, Presidente, AIEA - ISACA Milan Chapter

modera **Simona Di Felice**, Vice Presidente, AIEA - ISACA Milan Chapter

13:15-14:15

Light Lunch presso Foyer Testori

14:15-15:00

Audit delle tecnologie emergenti: approcci, metodi e competenze

Intelligenza artificiale, sistemi sempre più autonomi, quantum computing e nuove architetture tecnologiche introducono oggetti di audit per i quali metriche, evidenze e criteri di valutazione non sono sempre consolidati. Come definire il perimetro di verifica? Quali competenze e strumenti servono? E come assicurare tecnologie che evolvono rapidamente senza rinunciare al rigore dell'audit? Un confronto sulle pratiche che stanno emergendo e sulle questioni ancora aperte.

Claudio Giulietti, Head of Internal Audit, esperto Risk & Governance

Cristiano Paris, ISACA Accredited Trainer

Matteo Tavola, Responsabile Supporto normativo per la protezione dei dati personali, ARIA S.p.A. - Azienda Regionale per l'Innovazione e gli Acquisti

Stefano Scapecchi, ISACA Accredited Trainer, ISACA Advanced in AI Audit™ (AAIA™)

modera **Fabio Schiera**, Founder, Data&co

15:00-15:50

AIEA for NIS2: governance, risk and accountability

Il recepimento della Direttiva NIS2 impone un profondo cambio di paradigma non solo tecnologico, ma organizzativo, ponendo nuove e complesse sfide in termini di governance, gestione del rischio e responsabilità (accountability) dei vertici aziendali. Il Gruppo di Lavoro presenta ufficialmente i propri tavoli di cantiere, condividendo la roadmap delle attività e le prime riflessioni emerse dal confronto tra i professionisti del settore, con l'obiettivo di fornire un framework concreto per affrontare la transizione normativa.

Luca Savoia, Partner, Forvis Mazars e Coordinatore Gruppo di Lavoro AIEAforNIS2

Giulia Palmarini, IT Audit Manager, Recordati

Luca Verdolini, Senior, Forvis Mazars

Con la partecipazione dei referenti del Gruppo di Lavoro AIEAforNIS2

15:50-16:20

Il ruolo del CSIRT nella NIS2: dalla segnalazione alla gestione della crisi

La Direttiva pone un forte accento sulla tempestività e sull'efficacia nella gestione degli incidenti. In questo contesto, il ruolo del Computer Security Incident Response Team (CSIRT) diventa fondamentale per assicurare la continuità operativa. Un confronto pratico sulle dinamiche di segnalazione, risposta e mitigazione delle crisi cyber, con la testimonianza diretta di chi gestisce l'operatività sul campo.

Filadelfio Emanuele, CISO, Elmec Informatica

16:20-16:40

Coffee Break

16:40-17:15

**Formazione professionale per Audit, Risk e Security:
AI e nuovi modelli di apprendimento**

L'intelligenza artificiale e la rapidità dell'evoluzione tecnologica stanno accorciando i cicli di aggiornamento delle conoscenze e modificando strumenti, metodi e modalità di lavoro. Per i professionisti di Audit, Risk e Security diventa quindi ancora più importante integrare competenze tecniche, capacità di giudizio e apprendimento continuo. L'intervento riflette su come devono evolvere i percorsi di formazione e sviluppo professionale per accompagnare ruoli chiamati a operare in contesti sempre più dinamici.

Marco Crestan, Segretario del Consiglio Direttivo, AIEA - ISACA Milan Chapter**Brunella Di Silvestro**, Trainer e Coach professionista, associata ICF

17:15-17:30

Saluti e chiusura dei lavori

Come raggiungerci

INGRESSO DA PIAZZA CITTÀ DI LOMBARDIA

Auditorium Giovanni Testori, Palazzo Lombardia

Piazza Città di Lombardia, 1 · 20124 Milano

L'Auditorium Testori si trova all'interno di Palazzo Lombardia, in una posizione facilmente raggiungibile con i principali collegamenti urbani e ferroviari. L'accesso all'Auditorium è da Piazza Città di Lombardia.

METROPOLITANA

- M2** Gioia
- M3** Centrale FS · Sondrio
- M5** Isola

TRENO E PASSANTE

Milano Centrale
Milano Porta Garibaldi
Passante: fermata Repubblica

AUTOBUS

Linee 43, 60, 81