



ASSOCIAZIONE
ITALIANA
INFORMATION
SYSTEMS
AUDITORS



ISACA®
Milan Chapter

nota anche come

PRESENTA



NUMERI SICURI

**GDPR E DPO,
INTELLIGENZA ARTIFICIALE,
RISK QUANTIFICATION**

Milano, 18 novembre 2020 14.00-18.00

online in streaming

in attesa di poter tornare nell'Auditorium UniCredit Services – Milano

IL PROGRAMMA

14:00	Saluti e introduzione
14:10	<u><i>Maria Roberta Perugini</i></u> GDPR – Tutte le domande a cui un DPO deve sapere rispondere
15:00	<u><i>Sergio Napolitano</i></u> Intelligenza Artificiale: applicazione nella cybersecurity e rischi connessi
15:40	Coffee Break
16:00	<u><i>Giancarlo Butti, Alberto Piamonte</i></u> Metodologie per il Risk Quantification. Un approccio al metodo FAIR
16:00	<u><i>Alberto Piamonte</i></u> Evoluzione del Risk Management e Risk Quantification
17:00	<u><i>Giancarlo Butti</i></u>
17:30	Dibattito con i Relatori
18:00	Conclusioni e networking

LE RELAZIONI

Maria Roberta Perugini

GDPR – Tutte le domande a cui un DPO deve sapere rispondere

La normativa sulla protezione dei dati personali è particolarmente complessa e stratificata e i dubbi e le incertezze sulla corretta applicazione delle norme possono condurre ad effetti deleteri per il rischio di non individuare correttamente il perimetro di tutela e quale sia la normativa applicabile nelle varie situazioni. Molti sono ancora i dubbi interpretativi o le errate convinzioni, derivanti molto spesso dall'assenza di una reale conoscenza della normativa e delle sue implicazioni, pratiche e giuridiche, da parte di chi è tenuto ad attuarla. Per contribuire a fare chiarezza, il libro assume un approccio concreto accompagnando la struttura domanda/risposta con un'articolazione approfondita della risposta – ove opportuno – anche a livello teorico: ciò al fine di coniugare la soddisfazione del bisogno di concretezza degli operatori con la necessaria formazione e creazione di consapevolezza.

Sergio Napolitano

Intelligenza Artificiale: applicazione nella cybersecurity e rischi connessi

L'intelligenza artificiale è sia uno strumento di difesa in ambito cybersecurity per potenziare le capacità difensive delle aziende, ma anche uno strumento di attacco per creare minacce sempre più sofisticate e automatizzate. Verranno illustrate le strategie di mascheramento degli attacchi attraverso tecniche di Adversarial Attack e i rischi connessi ai Deepfake e al Social Engineering 2.0

Giancarlo Butti, Alberto Piamonte

Metodologie per il Risk Quantification. Un approccio al metodo FAIR

L'analisi dei rischi è un'attività fondamentale quale strumento per identificare le aree dove è prioritario intervenire con delle opportune contromisure.

Diventa quindi fondamentale da un lato la capacità di recuperare le informazioni necessarie per effettuare una stima attendibile dei possibili impatti sulle varie tipologie di asset che interessano l'azienda, le conseguenze dirette ed indirette sull'organizzazione, le conseguenze sui diritti e libertà delle persone fisiche...

Analogamente si deve procedere per la corretta individuazione degli scenari di rischio, la loro probabilità di accadimento e la probabilità che il verificarsi di tali eventi abbia effettivo impatto sugli asset e sull'azienda.

Una corretta valutazione non può tuttavia basarsi su semplice valutazione di natura qualitativa, ma è necessario un approccio che consenta una più precisa valutazione e rappresentazione dei singoli rischi e della loro aggregazione.

Ecco quindi il ricorso a metodologie che permettono una valutazione di natura quantitativa, quali FAIR (fra gli altri richiamate da ISACA nella ultima versione della Risk IT Practitioner Guide).

I RELATORI

Maria Roberta Perugini

Avvocato, si occupa sin dal 1995 di protezione dei dati personali e svolge attività di consulenza alle imprese in questa materia – compresi gli aspetti tecnici e organizzativi –, fornendo un supporto completo dei connessi profili contrattuali e in generale civilistici. Organizza e partecipa come relatrice e docente a convegni, master e corsi di specializzazione in materia di protezione dei dati personali di numerosi enti, associazioni, Università e istituzioni nonché workshop di formazione ed aggiornamento presso imprese e associazioni di categoria. Contribuisce alla Clusit Community for Security. Pubblica monografie e testi di aggiornamento e riflessione su problematiche attuali di data protection su riviste divulgative e scientifiche, online e cartacee. Co-fondatrice di IUSinTECH, un team di professionisti con specializzazioni nel campo del diritto applicato all'innovazione, alle nuove tecnologie, al risk management.

Sergio Napolitano (Auditando)

Ingegnere Elettronico. Ha maturato una significativa esperienza in diversi settori (Oil & Gas, Banking e Consumer Goods) e in differenti funzioni aziendali (Organizzazione, IT e Audit). Durante la sua carriera si è occupato di analisi dei processi, change management, IT Audit & Compliance, SOC reporting (ISAE3402 e SAS70) e Corporate Governance. Certificato CISA dal 2006, in AIEA ha fatto parte del gruppo che si è occupato della traduzione del manuale CISA. Attualmente svolge attività di consulenza in ambito IT Audit, GDPR, Cybersecurity, Analisi del Rischio fornitori e rispetto di Normative Nazionali ed Internazionali.

Giancarlo Butti

Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni. Oltre 120 corsi e seminari presso ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNIVERSITA DEGLI STUDI DI MILANO. Già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer e master presso diversi atenei. Ha all'attivo oltre 800 articoli e collaborazioni con oltre 30 testate. Ha pubblicato 25 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 15 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT. Socio e già proboviro di AIEA è socio del CLUSIT e del BCI. Partecipa a numerosi gruppi di lavoro ed è fra i coordinatori di www.blog.euoprivacy.info. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, CDPSE, ISM, DPO, CBCI, AMCBI.

Alberto Piamonte (KeyMap)

Alberto Piamonte, laureato nell'Università di Padova in Ingegneria Elettronica, fa attualmente parte del KeyMap Team, un gruppo di Consulenti ed Aziende che si occupa dello sviluppo di strumenti automatizzati e metodologie per attività di audit, l'analisi e gestione dei rischi, la certificazione conformità e la realizzazione di efficaci ed efficienti sistemi di controllo e di governo. Oltre che svolgere in prima persona attività di consulenza si occupa attivamente dei problemi relativi al governo dei sistemi IT tenendo frequenti corsi e seminari su metodologie quali COBIT, ITIL, ISO27001 e GDPR ed alla sensibilizzazione e diffusione delle relative tematiche. Una lunga carriera nel mondo ICT con significative esperienze internazionali. Istruttore, Implementor e Assessor COBIT5, è attualmente Consigliere ISACA Capitolo di Roma.

LUOGO E DATA

Venerdì, 18 ottobre 2020

Online sulla piattaforma di Videoconferenza/Streaming di AIEA

ISCRIZIONI

Soci AIEA

Portale delle Sessioni di Studio

<https://portale.aiea.jed.st/>

Se al primo accesso, recuperare la propria ISACA ID (numerica) dal sito ISACA o dalle comunicazioni di iscrizione/rinnovo e farsi inviare la password all'indirizzo preregistrato tramite la funzione

[Password dimenticata](#)

Un Socio AIEA invita un Non Socio

Ogni Socio AIEA può invitare un Non Socio, che potrà seguire lo streaming sulla pagina dedicata del Sito AIEA. Contattare Luca Pertile <luca.pertile@aiea.it> per la chiave di accesso.

Non Soci

Contattare la segreteria AIEA per associarsi o versare il contributo organizzativo per il singolo evento

[Segreteria AIEA](#)



Associazione Italiana Information Systems Auditors

L'Associazione Italiana Information Systems Auditors è stata costituita a Milano nel 1979 con lo scopo di promuovere l'approfondimento dei problemi connessi con il controllo del processo di elaborazione automatica dei dati e di favorire lo sviluppo di metodologie e tecniche uniformi per la loro soluzione.

In particolare, gli obiettivi dell'Associazione sono:

- promuovere un processo di sensibilizzazione di tutti i livelli organizzativi aziendali alla necessità di stabilire adeguati criteri di controllo, di affidabilità dell'organizzazione, Information Systems e di sicurezza dei sistemi;
- ampliare la conoscenza ed esperienza dei suoi oltre 800 membri nel campo dell'IT Governance, IT Security, Information Systems Auditing e Risk Control, favorendo lo scambio di metodologie per lo studio e la soluzione dei problemi inerenti;
- promuovere a livello nazionale la partecipazione alle certificazioni CISA, CISM, CGEIT, CRISC, CobiT e CSX

AIEA è associata da 40 anni ad ISACA, primo Capitolo in Europa, diventando nota internazionalmente come



ISACA® per i suoi oltre 145,000 soci in oltre 180 paesi e per la comunità dei professionisti IT è fonte affidabile di possibilità di networking, certificazioni professionali, conoscenza e standard negli ambiti IT Governance, Cybersecurity, IT Risk e Assurance

www.aiea.it