# Ciclo di seminari « Cyber Security Manager per la protezione dei dati ( 4CFP)

La Commissione Sicurezza Informatica propone un ciclo di seminari sulla Sicurezza Informatica per formare i professionisti sui principali temi legati alla protezione dei dati.
La moderna figura del Cyber Security manager nel rispetto della dottrina della sicurezza deve essere in grado di presidiare rischi e minacce a tutto campo in relazione agli scenari sempre in evoluzione nel campo tecnologico e normativo.
Da pochi mesi è stato pubblicato sulla Gazzetta Ufficiale dell'Unione europea il nuovo "Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati", la riforma organica della direttiva 95/46/Ce in materia di data protection.
Diventa quindi fondamentale per gli Ingegneri aggiornare le proprie competenze professionali per conoscere quali sono le principali novità introdotte, gli aspetti pratici da tenere in considerazione per lo svolgimento della professione.
Scopo del corso è quello di fornire i concetti base sulla sicurezza delle informazioni e le principali competenze su aspetti tecnologici, organizzativi e normativi relativi alla sicurezza alla protezione dei dati da archiviare o da scambiare in rete.
Il ciclo di Seminari comprende una serie di moduli a corredo della figura del Cyber Security Manager:

- **Seminario 1°-** "Protocolli, protezione perimetrale e controllo accessi di sistemi ICT" - 7 Ottobre 2017;
- **Seminario 2°-** "Il nuovo quadro normativo Europeo per la protezione dei dati " - 10 Ottobre 2017;
- **Seminario 3° -** "Data Loss prevention e Social Engineering" **-** 14 Ottobre 2017;
- **Seminario 4° -** "Deep & Dark Web" introduzione - 17 Ottobre 2017;
- **Seminario 5° -** "Soluzioni per progettare e implementare il cloud" – 21 Ottobre 2017;
- **Seminario 6°** - "Metodologie di risk analysis e di risk assessment: casi pratici d'utilizzo" – 24 Ottobre 2017;
- **Seminario 7° -** "Cybersecurity framework e i principali adempimenti normativi: le competenze del Security Manager" – 28 Ottobre 2017;
- **Seminario 8° -** "Linee guida di base per attuare un SGSI conforme alla normativa ISO 27001:2013 "– 31 Ottobre 2017;
- **Seminario 9° -** "Progettazione di sistemi biometrici per la sicurezza fisica e logica" 4 Novembre 2017;
- **Seminario 10° -** "Deep & Dark Web" - 7 Novembre 2017;

I seminari si terranno nell'aula 1 della nuova sede dell'Ordine.

Per informazione scrivere a formazione@ording.roma.it

Prenotazione obbligatoria sul sito dell'Ordine www.ording.roma.it al costo di € 20 per ciascun seminario.
La partecipazione a ciascun seminario per l'intera durata rilascia 4 CFP ai fini dell'aggiornamento professionale.
**La frequenza sarà attestata unicamente dalle firme e dagli orari di registrazione in ingresso ed in uscita.**

**L'iscrizione è obbligatoria sul sito dell'Ordine alla pagina:**
https://www.ording.roma.it/formazione/index.aspx

## Calendario del seminario:

Lezione 07 - 28.10.2017 (Sabato) ore 09:30 - 13:30

## Costi

La quota di partecipazione è di **€ 20** da versare tramite bonifico bancario o in contanti o bancomat presso la sede dell'Ordine.
L' ORDINE DEGLI INGEGNERI DI ROMA non è soggetto IVA.

## Sedi e orari del seminario

Sala Corsi presso Ordine degli Ingegneri della Provincia di Roma, Piazza della Repubblica, 59 - 00185 - Roma.
Orari: come da calendario.

## Requisiti d'ammissione:

Il corso è aperto a tutti.

## Attestati

Gli Ingegneri iscritti ai rispettivi Albi potranno scaricare l'attestato di partecipazione accedendo all'area personale del sito www.ming.it, non appena registrati i CFP conseguiti.

## Altre informazioni

Frequenza: Obbligatoria

## Condizioni generali:

Prima di procedere con l'iscrizione al corso leggere attentamente le norme allegate. Leggere documento.

## Note

Il numero di posti a disposizione è pari a 70 unità. L'iscrizione sarà completa solo dopo il pagamento, la cui ricevuta è da inviare via email a iscrizionecorsi@ording.roma.it.
La data dell'email stabilirà la precedenza di accesso al seminario. In caso di non ammissione per raggiunto numero massimo di partecipanti, si potrà richiedere il rimborso della quota versata alla Tesoreria dell'Ordine entro la fine del seminario (4 novembre 2017) o al massimo entro l'anno di riferimento, formulando apposita istanza da inviare a tesoreria@ording.roma.it.
Gli iscritti, che intendano ritirare la propria iscrizione per motivi non connessi all'organizzazione potranno chiedere il rimporto **dell'85%** dell'importo versato.
In caso di necessità l'Ordine si riserva la facoltà di modificare le date e/o la sede del seminario informando tempestivamente gli iscritti. Per tale motivo, si richiede di indicare correttamente la propria e-mail.

## Programma

**Programma 07 - 28.1.2017 (sabato) ore 09:15 - 13:30**

- **09.15 – 09:30 Registrazione e Saluti Iniziali**

Ing. **Carla CAPPIELLO, Presidente dell'Ordine degli Ingegneri di Roma**
Ing. **Francesco Marinuzzi, Consigliere dell'Ordine degli Ingegneri di Roma**

- **09.30 – 13.30 – Cybersecurity framework e i principali adempimenti normativi: le competenze del Security Manager"**

Ing. **Paola Rocco (Presidente Commissione "Sicurezza Informatica")**

Il seminario ha come obiettivo di fornire una panoramica generale delle misure di sicurezza da adottare per aumentare la resilienza delle organizzazioni verso attacchi informatici.
Il seminario avrà un focus sia sugli aspetti normativi che sulle linee guide pratiche o "best practices" da seguire, in particolare saranno trattati i seguenti argomenti:

- Introduzione e presentazione del Framework di sicurezza;
- Linee guida per l'implementazione;
- Definizione delle principali tipologie di dato trattate in azienda;
- Analisi dei principali provvedimenti normativi e delle misure di sicurezza da adottare per essere conformi

# Profilo docente:

**Ing. Paola Rocco**

Laureata in Ing. Informatica presso l'ateneo Federico II di Napoli, attualmente ricopre il ruolo di Senior Consultant. Svolge attività di consulenza nell'ambito della sicurezza delle informazioni, della privacy presso primari clienti nei principali segmenti di mercato: Bancario, Utility, Telecomunicazioni e nelle Pubbliche Amministrazioni. Ha gestito progetti relativi sia alla sicurezza logica che alla sicurezza fisica, in particolare ha lavorato nell'ambito del controllo accessi e sistemi di raccolta log, sicurezza perimetrale e DDoS mitigation, networking, policy e procedure di sicurezza, progettazione di sistemi antifrode e antispam per il traffico sms, sistemi integrati di videosorveglianza, Internal Auditing (validazione azioni correttive).

Lead Auditor ISO 27001, ISO 22301, ha conseguito l'abilitazione come R.S.P.P. e la certificazione ArcSight ESM. Attualmente è Presidente della Commissione Sicurezza Informatica presso l'Ordine degli Ingegneri della provincia di Roma, dove ha tenuto interventi tecnici nell'ambito dei Seminari organizzati sugli attacchi informatici, sulla Business Continuity, la videosorveglianza, la Cyber Security e il D.Lgs. 231/2001.

Componente del Comitato Scientifico del Master di II livello in "Responsabile della protezione dei dati personali: *Data protection officer e privacy expert*" presso Roma Tre, come delegata dell'Ordine degli Ingegneri della Provincia di Roma.