

MASTER ON LINE REATI INFORMATICI E CYBERSECURITY

Dall' 7 febbraio al 6 marzo 2024

10,5 ore (9 incontri in aula virtuale)

DOCENTI

PAOLO DAL CHECCO: Consulente informatico forense

MICHELE IASELLI: Vicedirigente del Ministero della Difesa, avvocato e docente di informatica giuridica

FRANCESCO MELONI: Avvocato penalista del Foro di Torino

OBIETTIVI

Il presente corso con i webinar ed i video dedicati ai reati informatici permette di fare il punto della situazione con riferimento alle diverse tipologie di reati informatici.

Nella **prima parte** del corso vengono analizzati i **reati informatici tradizionali** disciplinati dal codice penale, i **nuovi reati informatici** sorti con l'avvento della Rete ed i reati informatici che contraddistinguono il mondo della **protezione dei dati personali (GDPR)**

La **seconda parte** fornisce nozioni operative in tema di prevenzione della criminalità informatica. Vengono affrontati i profili della disciplina della responsabilità dell'Ente, con un focus sulle ipotesi di reato presupposto contemplate nel **D.Lgs. n. 231/2001**, e sulla relativa Parte Speciale del Modello Organizzativo. Un approfondimento è dedicato ai rapporti intercorrenti tra la tutela penale del **know-how aziendale** e i reati informatici nonché alle principali questioni di natura processuale (**tecniche di conduzione dell'investigazione difensiva** in materia informatico-forense)

La **terza parte** conclusiva affronta tutto ciò che riguarda le **procedure accertamento tecnico** e di **controllo aziendale** terminando con un **workshop pratico**

STRUTTURA DEL CORSO

- **3 mini-pillole stand alone da 20 minuti ciascuna**
- **8 webinar accreditati da un'ora ciascuno**
- **1 aula virtuale di esercitazione**

DESTINATARI

- Avvocati
- Laureati in discipline giuridico-economiche



- Manager, impiegati e funzionari di aziende private ed Enti pubblici

CREDITI FORMATIVI

Richiesta di accreditamento inoltrata al Consiglio Nazionale Forense

PERCHE' IL NOSTRO MASTER?

- **Formula live streaming** studiata per garantire una didattica modulabile in base alle proprie esigenze
- **Formazione interattiva** con momenti di confronto e spazi q&a dedicati. Durante i webinar potrai sempre inviare le tue domande al docente utilizzando la chat della piattaforma
- **Incontri videoregistrati.** Potrai ripassare gli argomenti delle lezioni in un secondo momento. Le videolezioni sono accessibili per tutta la durata dell'iniziativa e per i 90 gg successivi all'ultimo webinar La registrazione dell'evento è da considerare come semplice materiale didattico e NON rilascia crediti ai fini della formazione professionale continua
- **Materiale didattico** esaustivo. Al termine di ogni webinar saranno disponibili nel tuo profilo personale le slide dell'incontro, le risposte a tutte le domande di interesse poste durante l'evento e la registrazione della lezione

PROGRAMMA

Minipillole:

La prima minipillola:	La seconda minipillola:	La terza minipillola
è dedicata alla nascita del diritto penale dell'informatica e alla L. n. 48/2008; all'oggetto materiale e alla condotta dei reati informatici, ai soggetti del reato informatico e alle tipologie di reati informatici	è dedicata all'evoluzione de Web 2.0 e i nuovi reati informatici	è dedicata agli illeciti penali in materia di protezione dei dati personali

AULE VIRTUALI

I MODULO - NASCITA DEL DIRITTO PENALE DELL'INFORMATICA E IL CYBER CRIME CON LA LEGGE DI RATIFICA DELLA CONVENZIONE DI BUDAPEST

7 febbraio 2024, dalle 14.00 alle 15.00

- Il diritto penale dell'informatica
- La legge n. 48/2008
- Le diverse tipologie di reati informatici disciplinati dal c.p.
- Riferimenti giurisprudenziali
- Casistica giurisprudenziale

II MODULO - EVOLUZIONE DE WEB 2.0: LA NASCITA DI QUELLI CHE POTREMO DEFINIRE I NUOVI REATI INFORMATICI

8 febbraio 2024, dalle 14.00 alle 15.00

- Cos'è il web 2.0
- Diffamazione on line
- *Cyberstalking*
- *Cybebullismo*
- Pedopornografia on line
- I nuovi reati informatici
- Casistica giurisprudenziale

III MODULO - ILLECITI PENALI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

14 febbraio 2024, dalle 14.00 alle 15.30

- I principi del GDPR
- Il d.lgs. n. 101/2018
- Il trattamento illecito dei dati
- Falsità nelle dichiarazioni e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante
- Inosservanza di provvedimenti del Garante
- I nuovi illeciti penali
- Casistica giurisprudenziale



QUESTIONS & ANSWERS



QUALITÀ CERTIFICATA

A garanzia della qualità dei processi formativi, IPSGA Scuola di formazione è certificata ISO 9001:2015 ed è Centro accreditato AiFOS nell'ambito della sicurezza.

IV MODULO - I REATI INFORMATICI NELL'AMBITO DELLA RESPONSABILITÀ DEGLI ENTI, AI SENSI DEL D.LGS. N. 231/2001

15 febbraio 2024, dalle 14.00 alle 15.00

- Il Modello Organizzativo quale strumento di gestione della *cybersecurity*: il *risk assessment* in ambito *cyber*.
- La parte speciale del Modello Organizzativo dedicata ai reati informatici. Il ruolo delle norme tecniche e degli standard internazionali in tema di *cybersecurity*. Procedure, protocolli e strumenti di prevenzione in ambito *cyber*;
- Le ipotesi di reato presupposto ai sensi dell'art. 24 bis, D.Lgs. n. 231/2001;
- I nuovi reati presupposto in materia di tutela del perimetro di sicurezza nazionale cibernetica.
- La Legge 18 novembre 2019, n. 133 e il primo decreto attuativo (DPCM 30 luglio 2020 n. 131).

V MODULO - ANALISI CASISTICO-PROCESSUALE DEI PRINCIPALI REATI INFORMATICI

20 febbraio 2024, dalle 14.00 alle 15.00

- Il delitto di accesso abusivo a sistema informatico (art. 615 ter c.p.): rapporti con la tutela penale del *know-how*;
- Il delitto di danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)
- Il delitto di danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.);
- I reati commessi con l'uso di strumenti telematici. Peculiarità e problematiche di natura processuale:
 - la diffamazione a mezzo web;
 - la tutela penale del diritto d'autore;
 - la responsabilità penale del *Provider*.

VI MODULO - INVESTIGAZIONI DIFENSIVE

22 febbraio 2024, dalle 14.00 alle 15.30

- Investigazioni difensive e *digital forensics*: profili tecnici, informatici e giuridici.
- Gli accertamenti informatico-forensi: profili e problematiche di natura processuale.
- La gestione dell'incidente informatico in Azienda: *internal investigations*, attività di verifica dell'Organismo di Vigilanza e reporting verso gli Organi gestori e di controllo.

**QUESTIONS & ANSWERS****VII MODULO - ACCERTAMENTI TECNICI E ACQUISIZIONE DEI DATI****28 febbraio 2024, dalle 14.00 alle 15.00**

- I tre capisaldi dell'informatica forense
- Metodologie di acquisizione forense
- Strumenti per l'acquisizione dei dati in ottemperanza alle normative
- Le fonti di prova più comuni: smartphone, PC, web, email
- Consigli e *best practice* d'informatica forense

VIII MODULO - PROCEDURE INTERNE DI CONTROLLO AZIENDALE**29 febbraio 2024, dalle 14.00 alle 15.00**

- Regolare le procedure di controllo aziendale
- Gestire le procedure di controllo aziendale
- Strumenti idonei per il controllo aziendale
- Importanza delle *Policy*, Informativa e Documenti di Assegnazione risorse
- Prevenire, Identificare e Analizzare i reati informatici commessi in azienda e/o a danno dell'azienda

IX MODULO - WORKSHOP DIGITALE**6 marzo 2024, dalle 14.00 alle 15.30****QUESTIONS & ANSWERS****QUALITÀ CERTIFICATA**

A garanzia della qualità dei processi formativi, IPSCA Scuole di formazione è certificata ISO 9001:2015 ed è Centro accreditato AIFOS nell'ambito della sicurezza.