TINEXTA CYBER

DORA, NIS 2, DDL CYBER e AI ACT:

Seminario strategico sull'approccio integrato alle sfide del nuovo framework normativo

Con il patrocinio di:

ASSOCIAZIONE NAZIONALE GIOVANI INNOVATORI

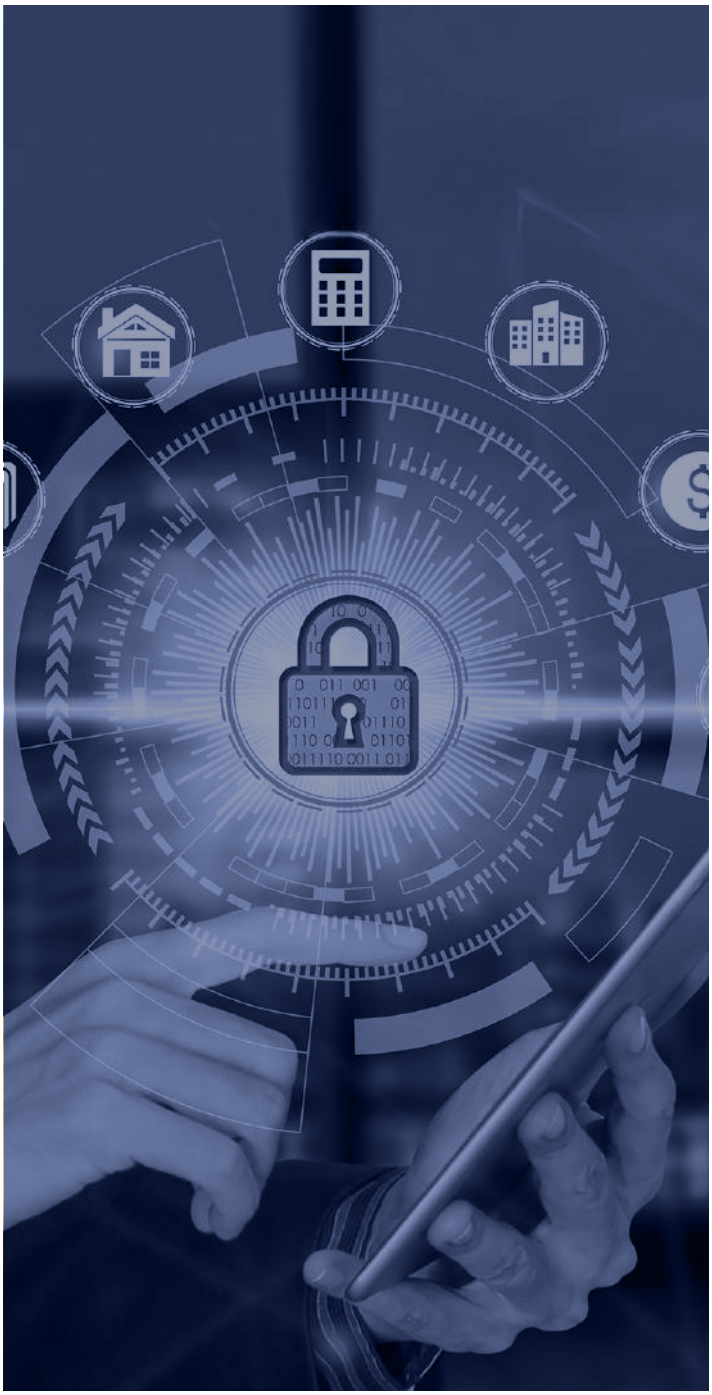
ASSINTEL ASSOCIAZIONE NAZIONALE IMPRESE ICT

Settembre'24

Se hai bisogno di maggiori informazioni, scrivi a

formazione@tinextacyber.com

martina.emanueli@tinextacyber.com



Descrizione

In un contesto in cui le minacce informatiche sono in costante aumento e sempre più sofisticate, conformarsi a normative come la Direttiva NIS 2 e il Regolamento DORA non è solo una questione di compliance, ma una necessità strategica per proteggere i dati aziendali, prevenire interruzioni operative e mantenere la fiducia dei clienti. Il corso esplorerà come queste regolamentazioni impattano le diverse funzioni aziendali e fornirà strumenti pratici per implementare misure di sicurezza efficaci, garantendo la continuità operativa e la sostenibilità a lungo termine dell'azienda.

Segui il corso da dove vuoi tu! Il corso è interamente somministrato in modalità DAD.

formazione@tinextacyber.com
martina.emanueli@tinextacyber.com

Obiettivo

L'obiettivo del corso è fornire una comprensione completa del nuovo framework normativo in cybersecurity, delineare ruoli e responsabilità aziendali, e sviluppare competenze per identificare e gestire rischi e incidenti informatici. I partecipanti impareranno a implementare politiche di sicurezza, monitorare attività aziendali, e ottimizzare investimenti in risorse tecnologiche, garantendo la coerenza tra strategia e operatività per la continuità aziendale.

Destinatari

Il corso è destinato ai manager aziendali, inclusi direttori generali, CEO, CIO, CISO e altri membri del senior management responsabili delle decisioni strategiche. È adatto ai responsabili della sicurezza informatica, come responsabili IT e del rischio, nonché al personale operativo che gestisce quotidianamente la sicurezza informatica, inclusi staff IT e amministratori di sistema. Anche consulenti esterni, analisti del rischio e professionisti del settore troveranno utile questo corso.

formazione@tinextacyber.com
martina.emanueli@tinextacyber.com

TINEXTA CYBER

Programma didattico

01 Il nuovo framework normativo in ambito cybersecurity

02 Il nuovo framework normativo in ambito cybersecurity

03 Principali rischi connessi al trattamento

04 Regole sul corretto utilizzo delle risorse aziendali

05 Politiche di Secure Smartworking

06 Monitoraggio delle attività e controlli consentiti

07 Assessment sulla cybersecurity posture

08 Centralità della procedura di Incident Response Management

09 Processo di Third Party Risk Management

10 Vantaggi e criticità legate all'utilizzo dell'AI in azienda

11 Aspetti metodologici e sostenibilità del sistema di Risk Governance

12 Risvolti legali, reputazionali, economici ed operativi legati al Cyber Crime

13 Corretto indirizzo degli investimenti in risorse tecnologiche, organizzazione e security management

14 Coerenza tra strategia e pianificazione operativa a garanzia della continuità

formazione@tinextacyber.com
martina.emanueli@tinextacyber.com

Prerequisiti

Non sono richiesti prerequisiti mandatori, tuttavia, è auspicabile che i partecipanti abbiano almeno una conoscenza di base dei concetti di cybersecurity e familiarità con le normative attualmente vigenti (come GDPR, ecc).

Metodologia

Il corso avrà una durata di 2 ore e verrà erogato in modalità sincrona attraverso la costituzione di una classe virtuale.
Al termine del corso verrà rilasciato un Attestato di Frequenza.

Calendario

19 Settembre ore 10:00 – 12:00

formazione@tinextacyber.com
martina.emanueli@tinextacyber.com