CYBERSECURITY, eIDAS, NIS2

La Direttiva NIS2 : i nuovi obblighi di cyber sicurezza per le aziende

Corso online



30/11/2026 - 8h

Descrizione del corso

La Direttiva NIS2 - Cosa è, quale impatto avrà sulle aziende e come essere pronti a rispettarla

Nata per migliorare il livello comune di cybersecurity in tutta l'Unione Europea, la Direttiva NIS2 attraverso un approccio basato sulla gestione del rischio, propone significative novità, che riguardano l'estensione dell'ambito di applicazione, l'introduzione di più rigorose misure di vigilanza, disposizioni precise sulla segnalazione degli incidenti e impone alle singole organizzazioni di affrontare i rischi di cybersecurity nelle catene di approvvigionamento e nei rapporti con i fornitori.

Il corso ha l'obiettivo di:

- Fornire una comprensione completa della Direttiva NIS2 e dei suoi impatti sulla cybersecurity
- Equipaggiare i partecipanti con competenze pratiche per valutare e affrontare i rischi di cybersecurity nelle organizzazioni pubbliche e private, nonché nella catene di approvvigionamento e nei rapporti con i fornitori
- Comprendere la portata della direttiva, valutare il suo impatto sulle operazioni delle organizzazioni e implementare strategie efficaci per garantire la conformità

Destinatari:

Il corso è rivolto al top management e al board aziendale; si rivolge inoltre a un'ampia gamma di professionisti e

stakeholder, inclusi ma non limitati a responsabili della cybersecurity, gestori delle catene di approvvigionamento e professionisti legali e normativi.

Prerequisiti

Non sono richiesti prerequisiti mandatori, tuttavia, è auspicabile che i partecipanti abbiano almeno una conoscenza di base dei concetti di cybersecurity e della normativa precedente (NIS1), per poter cogliere appieno le implicazioni dei cambiamenti introdotti dalla Direttiva NIS2.

Certificati/Attestati rilasciati

Al termine del corso verrà rilasciato un Attestato di Frequenza.

Programma

30 novembre 2026 dalle ore 8.45 alle 17.30

• Ambito di applicazione
• Entità essenziali e importanti
• Giurisdizione e territorialità
• Autorità competenti e punti di contatto unici
• Quadri nazionali di gestione delle crisi informatiche
• Divulgazione coordinata delle vulnerabilità e banca dati europea delle vulnerabilità
• Governance e misure di gestione del rischio di cybersicurezza
• Valutazioni coordinate del rischio di sicurezza delle catene di approvvigionamento critiche a livello dell’Unione
• Obblighi di rendicontazione
• Utilizzo di schemi europei di certificazione della cybersicurezza
• Standardizzazione
• Aspetti generali relativi alla vigilanza e all’applicazione
• Misure di vigilanza e di esecuzione in relazione ai soggetti essenziali
• Misure di vigilanza e di esecuzione in relazione ai soggetti importanti
• Violazioni che comportano una violazione dei dati personali
• Sanzioni