In qualità di Provider

In collaborazione con il partner scientifico

Organizza il corso di formazione

"La Direttiva NIS 2: obblighi e responsabilità degli amministratori aziendali e delle figure apicali" - IV EDIZIONE

Programma

10 marzo 2026

Con il supporto di

1. OBIETTIVI E DESTINATARI DEL CORSO DI FORMAZIONE

Il corso ha l'obiettivo di fornire le conoscenze di base in materia di cybersicurezza, necessarie agli organi di vertice per approvare con competenza i piani di implementazione delle misure di sicurezza e supervisionarne correttamente l'attuazione, in considerazione delle responsabilità legali che gravano su di loro in forza di legge.

Infatti, il percorso formativo si rivolge agli organi di amministrazione e direttivi delle aziende associate, i quali, in virtù di esplicite disposizioni di legge, sono soggetti a specifici obblighi che richiedono il possesso di conoscenze in ambito di sicurezza cibernetica.

2. STRUTTURA E CARATTERISTICHE DEL CORSO DI FORMAZIONE

Il piano formativo è strutturato in 1 giornata, dalle h. 10.00 alle h. 13.00 e dalle h. 14.00 alle h. 17.00, per una durata totale di 6 ore.

Il corso potrà essere seguito **via web o in presenza presso la sede di ASSTRA** – Associazione Trasporti, in Piazza Cola di Rienzo, 80/A – 00192 – Roma (RM).

La frequenza all'intera lezione è obbligatoria, in quanto requisito essenziale ai fini dell'ottenimento dell'**attestato di partecipazione** che sarà rilasciato da ASSTRA, utile ai fini della dimostrazione dell'acquisizione delle competenze in materia di cybersicurezza, richieste dalla normativa NIS 2 come requisito.

La presenza verrà verificata dal Tutor ASSTRA Service nel corso della giornata.

Ai fini del necessario accertamento dell'efficacia formativa dei partecipanti, è previsto **un test specifico finale per la valutazione dell'apprendimento dei temi trattati durante il corso**. Il test è costituito da 5 domande a risposta multipla, di cui una sola quella corretta, con l'obbligo di ottenere almeno il 60% di risposte esatte **per il rilascio dell'attestato di partecipazione.**

Inoltre, alla fine del corso **i partecipanti interessati dovranno esprimersi su appositi modelli preimpostati sulla qualità percepita su alcuni aspetti del corso** (organizzazione, docenti, ecc.).

3. DOCENTI

Il corso è organizzato da ASSTRA Service con il supporto scientifico dello studio legale WST Law & Tax Firm, che mette a disposizione, ai fini della docenza, specialisti del settore.

In particolare, il team messo a disposizione dallo studio sarà composto **dall'Avv. Raffaele Romano**, Senior Counsel e DPO certificato UNI 11697:2017 e **dall'Avv. Adebowale Adediwura**, Associate, CIPP/E, Lead Auditor ISO 27001 e 42011, entrambi del dipartimento Data Protection & New Tech di WST Law & Tax Firm.

4. MATERIALE DIDATTICO

Il materiale didattico, distribuito a tutti i partecipanti, è costituito da materiale formativo appositamente predisposto dai docenti.

5. ATTIVAZIONE E AULA

Per partecipare al Corso di formazione è necessaria la registrazione ed il versamento della relativa quota, secondo le indicazioni sotto riportate al paragrafo 6.
L'attivazione del corso è subordinata all'iscrizione di almeno 16 partecipanti.

6. ISCRIZIONI - COSTI E ISTRUZIONI PER IL VERSAMENTO DELLA QUOTA

Al fine di consentire una migliore organizzazione dell'evento formativo, si richiede alle aziende associate interessate di comunicare la propria adesione tempestivamente, **compilando, entro il giorno 24 febbraio 2026, il modulo *online* per la registrazione disponibile al seguente *link*:**

https://iscrizioni.asstra.it/Iscrizione_LaDirettivaNIS2_3_1

La quota di partecipazione al corso è pari:

- ad **euro 600,00 per ciascun iscritto;**
- ad **euro 550,00 per il 2°iscritto.**

Di seguito si riporta il programma formativo dell'intero corso.

10 marzo 2026, h. 10.00-17.00

1. Quadro normativo europeo e nazionale in materia di cybersicurezza: obblighi e scadenze per il *top management*
2. Responsabilità degli amministratori e degli organi di *governance* in materia di cybersicurezza
3. Modelli di *governance* della cybersicurezza: ruoli, deleghe e responsabilità aziendali
4. *Supply Chain* e sicurezza di filiera: gestione integrata dei fornitori e dei rischi *cyber*
5. Formazione obbligatoria e cultura aziendale della cybersicurezza
6. Sicurezza dei sistemi informatici e controlli aziendali: tutela dell'azienda e rispetto dei diritti dei lavoratori
7. *Policy* e processi aziendali per la gestione della cybersicurezza e degli incidenti informatici
8. Integrazione dei modelli di compliance *cybersecurity* e *data protection*: verso una gestione integrata dei rischi digitali