



CORSO DI FORMAZIONE ONLINE

**NIS2 E CYBERSICUREZZA
PER AMMINISTRATORI E DIRIGENTI
DI IMPRESE E PUBBLICHE AMMINISTRAZIONI,
SCENARIO EUROPEO, RESPONSABILITÀ DEGLI
ORGANI APICALI
E GESTIONE DEL RISCHIO INFORMATICO:
APPROFONDIMENTI OPERATIVI DALLE
INDICAZIONI ACN PER IMPRESE
E PUBBLICHE AMMINISTRAZIONI**

GIOVEDÌ 29 OTTOBRE 2026
dalle ore 9.30 alle ore 12.30

Codice MEPA: MMFDB09G

FORMAZIONE OBBLIGATORIA NIS2

Per gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e importanti, comprese le pubbliche amministrazioni rientranti nel perimetro NIS2, la formazione in materia di sicurezza informatica è espressamente prevista dall'art. 23, comma 2, del D.Lgs. 138/2024. Al termine del corso sarà rilasciato un attestato nominativo di partecipazione, che potrà essere conservato dall'organizzazione tra le evidenze documentali della formazione svolta ai fini dell'adempimento degli obblighi NIS2.



PRESENTAZIONE

Un attacco informatico può interrompere produzione, ordini, consegne o servizi pubblici essenziali. La protezione di sistemi e dati riguarda quindi direttamente chi amministra e dirige imprese e pubbliche amministrazioni: richiede scelte consapevoli, responsabilità definite, risorse e controlli.

Il corso affronta la cybersicurezza come parte della gestione dell'organizzazione, collegando il quadro NIS2 e le responsabilità degli organi apicali alle decisioni organizzative e ai presidi operativi, con attenzione alle specificità delle imprese e delle pubbliche amministrazioni.

La prima parte, affidata all'Avv. Prof. Andrea R. Sirotti Gaudenzi, inquadra la cybersicurezza nello scenario europeo e internazionale, tra trasformazione digitale, criminalità informatica, autonomia tecnologica e resilienza del sistema economico. La seconda parte, a cura dell'Avv. Gualtiero Roveda, approfondisce le responsabilità connesse agli incidenti e i presidi organizzativi: attuazione delle misure, evidenze, obiettivi, rischi, ruoli, matrice RACI, formazione e fornitori.

Il percorso assume particolare rilievo per i soggetti rientranti nel perimetro NIS2, poiché il D.Lgs. 138/2024 pone a carico degli organi di amministrazione e direttivi uno specifico **obbligo di formazione in materia di sicurezza informatica**. L'attestato rilasciato al termine del corso potrà essere acquisito dall'organizzazione quale **evidenza della formazione svolta**.

Direttore scientifico del corso: Avv. Gualtiero Roveda

OBIETTIVI DEL CORSO

Il percorso fornisce una mappa di lavoro comprensibile anche a chi non possiede competenze informatiche specialistiche. Al termine, i partecipanti potranno:

- comprendere l'evoluzione della cybersicurezza nel quadro europeo e internazionale;
- riconoscere i diversi profili di responsabilità che possono emergere da un incidente cyber;
- distinguere le misure formalmente adottate dalla loro attuazione e dalle evidenze che la dimostrano;
- definire obiettivi di sicurezza coerenti con le attività e le priorità dell'organizzazione;
- individuare processi, servizi, sistemi, dati e fornitori critici;
- comprendere gli elementi essenziali della valutazione del rischio e le scelte di trattamento;
- attribuire compiti e responsabilità, tenendo conto anche della governance delle pubbliche amministrazioni e della matrice RACI;
- organizzare formazione, segnalazioni e coordinamento in caso di incidente;
- individuare i principali presidi da richiedere ai fornitori e nei contratti;
- impostare un percorso di miglioramento con attività, responsabili ed evidenze verificabili.



ARTICOLAZIONE

Prima parte - dalle 9.30 alle 10.30

Avv. Prof. Andrea R. Sirotti Gaudenzi

Cybersicurezza e trasformazione digitale nello scenario europeo e internazionale.

Seconda parte - dalle 10.30 alle 12.30

Avv. Gualtiero Roveda

Incidenti cyber, responsabilità degli apicali e presidi organizzativi in imprese e PA.

PROGRAMMA DEL CORSO

PRIMA PARTE - DALLE 9.30 ALLE 11.00

Docente: Avv. Prof. Andrea R. Sirotti Gaudenzi

Cybersicurezza e trasformazione digitale nello scenario europeo e internazionale

1. La cybersicurezza come interesse europeo e nazionale

L'evoluzione della sicurezza digitale da questione specialistica a priorità per istituzioni, imprese e cittadini. La dimensione transnazionale delle minacce e il rapporto tra protezione delle infrastrutture, stabilità economica e sicurezza collettiva.

2. Il disegno europeo della resilienza digitale

Le finalità della NIS2 nel percorso europeo di rafforzamento della sicurezza e della cooperazione. Il rapporto tra armonizzazione delle regole, mercato unico digitale e capacità dei sistemi economici di resistere alle perturbazioni.

3. Criminalità informatica e dimensione internazionale

L'evoluzione del cybercrime e dei modelli criminali nell'economia digitale. Le difficoltà legate alla territorialità delle condotte, all'individuazione degli autori e alla cooperazione tra Stati nel contrasto agli attacchi.



4. Dipendenze tecnologiche e autonomia digitale

La concentrazione dei servizi digitali, il ruolo delle grandi piattaforme e le dipendenze tecnologiche delle imprese europee. Sovranità digitale, interconnessione dei mercati e vulnerabilità sistemiche.

5. Innovazione e fiducia nel sistema economico

Cybersicurezza come condizione per uno sviluppo digitale sostenibile e affidabile. Il rapporto tra innovazione, tutela dei diritti e fiducia nei servizi; resilienza e competitività delle imprese nel medio e lungo periodo. L'uso dell'intelligenza artificiale e i rischi legati alla cybersicurezza.

PROGRAMMA DEL CORSO

SECONDA PARTE - DALLE 11.00 ALLE 12.30

Docente: Avv. Gualtiero Roveda

Incidenti cyber, responsabilità degli apicali e presidi organizzativi in imprese e PA

1. Incidenti significativi e responsabilità degli organi apicali

Governo del rischio, adeguatezza degli assetti, vigilanza ACN, protezione dei dati e danni all'organizzazione, agli utenti e alla filiera. Per le imprese, sanzioni NIS e possibili responsabilità gestorie, penali omissive e dell'ente ai sensi del D.lgs. 231/2001. Per le PA, ripartizione delle competenze tra organi di indirizzo, vertice amministrativo, dirigenti, RTD e responsabili ICT.

2. Misure di base obbligatorie ed evidenze dell'attuazione

Decorso il termine di 18 mesi, le misure di sicurezza di base e gli undici documenti indicati dalle Linee Guida ACN devono essere attuati e mantenuti aggiornati. Decisioni, budget, verifiche, test, azioni correttive ed evidenze da conservare e sottoporre all'organo di amministrazione o direttivo.

3. Obiettivi e cultura della sicurezza

Minacce ricorrenti e impatto su attività e servizi. Obiettivi misurabili, priorità e riesame periodico. Fattore umano, consapevolezza e limiti della sola protezione tecnica.

4. Individuare gli obblighi applicabili

NIS2, Perimetro di sicurezza nazionale cibernetica, GDPR e requisiti settoriali o contrattuali; per le PA, anche CAD, misure AgID e approvvigionamenti digitali. Verifica del perimetro, monitoraggio normativo e tracciamento delle decisioni.



5. Asset critici e rischio informatico

Processi, sistemi, dati e dipendenze esterne. Minacce, vulnerabilità, probabilità, impatto e rischio residuo. Mitigare, trasferire, accettare o evitare il rischio. Esempi: blocco del gestionale ordini e indisponibilità di un servizio digitale pubblico.

6. Organizzare il presidio della cybersicurezza

Mandato, poteri, risorse, budget e reporting. Nelle PA, raccordo tra vertice, dirigenti, RTD, responsabili ICT, referenti NIS e fornitori. Ruoli e contatti per rilevazione, contenimento, notifica e ripristino.

7. Matrice RACI e responsabilità

Chi esegue, chi risponde dell'attività, chi viene consultato e chi informato. Distinzione tra compiti operativi, decisioni e flussi informativi, anche nelle amministrazioni con competenze distribuite tra più uffici.

8. Formazione e consapevolezza

Percorsi differenziati per vertici, personale e figure tecniche. Regole comprensibili, segnalazione delle anomalie, test, simulazioni di phishing e conservazione delle evidenze formative.

9. Fornitori e contratti

Valutazione e monitoraggio dei fornitori critici. Requisiti su accessi, backup, aggiornamenti e continuità del servizio. Obblighi di comunicazione e collaborazione; per le PA, requisiti cyber negli atti di gara, nei capitolati e nei contratti.

DESTINATARI

Componenti degli organi di amministrazione e direttivi, amministratori delegati, imprenditori, direttori generali, dirigenti e responsabili di funzione. Nelle pubbliche amministrazioni il corso è rivolto, in particolare, ai Segretari generali, ai Direttori generali, ai dirigenti apicali e ai dirigenti inseriti nella governance NIS, in relazione alle funzioni concretamente esercitate. Si rivolge inoltre a responsabili IT e della sicurezza informatica, RTD, referenti NIS, responsabili compliance, legali, risk manager, internal auditor, DPO e referenti privacy, responsabili acquisti e consulenti.

I contenuti operativi sono utili anche alle organizzazioni chiamate a presidiare il rischio informatico nei rapporti con utenti, clienti, fornitori e filiere, oltre che a verificare gli obblighi direttamente applicabili.

DOCENTI DEL CORSO

Accademia Europea Formazione srl
Via Circonvallazione Nuova, 69/A 47924 Rimini (RN)
N. Rea RN 423969 P.IVA 04533430403
Tel. 0541-448562 - 333-2430327

E-mail: info@accademiaeuropea.net - Pec: accademiaeuropea@pec.it www.accademiaeuropea.net



Avv. Prof. Andrea R. Sirotti Gaudenzi

Avvocato abilitato all'esercizio della professione dinanzi alle Magistrature superiori, è docente universitario e arbitro internazionale. Svolge attività di docenza in Italia e all'estero. Ha patrocinato davanti alla Corte europea dei diritti dell'Uomo e alla Corte di giustizia dell'Unione europea.

Responsabile scientifico e formatore accreditato dal Ministero della Giustizia ai sensi del D.M. n. 180/2010 presso vari enti, è presente nell'Albo dei Docenti della Scuola Superiore della Magistratura. Dirige il Master in diritto, arte e nuove tecnologie organizzato da Wolters Kluwer ed è docente nel Master in informatica giuridica presso l'Università Sapienza di Roma. È titolare degli insegnamenti di *International Criminal Law* e di *Cybercrime* nel corso PhD in *Law & Criminology* di Malta.

È membro del Comitato scientifico del Dipartimento interuniversitario di criminologia clinica, vittimologia e psicopatologia forense del Consorzio universitario Humanitas di Roma. È stato Presidente della Corte d'Appello della Federazione Ginnastica d'Italia. Collabora con le testate del gruppo «Il Sole 24 Ore».

Ha diretto vari Trattati giuridici, tra cui il *Trattato in materia di proprietà intellettuale e concorrenza* edito da Utet e il *Trattato operativo dei contratti d'impresa* edito da Maggioli.

Ha coordinato il Trattato *La disciplina dell'intelligenza artificiale e degli algoritmi avanzati*, Zanichelli, 2026. Assieme al Prof. Vincenzo Franceschelli ha scritto *La legge italiana sull'intelligenza artificiale*, Maggioli, 2025.

Il suo manuale *Il nuovo diritto d'autore* è giunto alla tredicesima edizione nel 2026.

Coordina varie collane editate da diverse case editrici e ha curato numerose pubblicazioni in tema di diritto commerciale, diritto industriale, proprietà intellettuale, diritto delle tecnologie informatiche, diritto internazionale, diritto della concorrenza, diritto sportivo.

Siede nel comitato scientifico delle riviste *Il diritto d'autore*, *Rivista di diritto industriale e Altalex*. Collabora stabilmente con le testate del gruppo «Il Sole 24 Ore».

È responsabile scientifico dell'Istituto nazionale per la formazione continua di Roma.

Avv. Gualtiero Roveda

Avvocato abilitato all'esercizio della professione dinanzi alle Magistrature superiori – Giornalista pubblicista esercita la professione forense nel settore del diritto d'impresa, del diritto del lavoro, della compliance aziendale, della sicurezza sul lavoro, della privacy, della cybersecurity e della responsabilità amministrativa degli enti ex D.Lgs. 231/2001.

Da oltre vent'anni cura le relazioni industriali per un'Associazione nazionale di categoria ed è responsabile tecnico della Commissione che stipula il Contratto Collettivo Nazionale di Lavoro del relativo comparto. È inoltre componente della Commissione paritetica nazionale istituita dal medesimo contratto collettivo.

È responsabile, ai sensi della Legge 11 gennaio 1979, n. 12, dell'organizzazione di uffici dedicati alla gestione degli adempimenti in materia di lavoro.

È stato componente del Comitato Scientifico della Scuola Forense di Forlì-Cesena.



Svolge attività di consulenza e formazione in materia di sicurezza sul lavoro, legislazione alimentare, D.Lgs. 231/2001, privacy, protezione dei dati personali, sicurezza informatica, NIS2 e intelligenza artificiale.

Certificazioni

È in possesso delle seguenti certificazioni IDCERT, livello Specialised:

IDCERT Privacy Specialist; IDCERT DPO / RPD; IDCERT Digital Competence; IDCERT IT Security

Pubblicazioni

È autore e coautore di pubblicazioni in materia giuridica e d'impresa, tra cui:

- *La fattura commerciale e la gestione dei crediti*, Experta S.p.A., 2003;
- *Gestione e recupero del credito. Aspetti operativi, civili, processuali e fiscali*, Experta, 2008;
- *La sicurezza sul lavoro. Responsabilità civile, penale e amministrativa*, Altalex Editore, 2016;
- *La chiave delle cose nascoste*, Primiceri Editore, 2016;
- *Insidie processuali e strategie difensive*, partecipazione con AA.VV., Maggioli Editore, 2018;
- *Trattato operativo dei contratti d'impresa*, partecipazione con AA.VV., Maggioli Editore, 2022;
- *La chiave delle cose nascoste*, II edizione, YCP, 2022;
- *La disciplina della sicurezza informatica*, Simposio Editore, 2025;
- *La disciplina dell'intelligenza artificiale e degli algoritmi avanzati*, partecipazione con AA.VV., Zanichelli, 2026.

Ha scritto articoli in materia di diritto d'impresa per Guida al Diritto – Il Sole 24 Ore e Altalex. Collabora inoltre con la testata giornalistica Fruitimprese, registrata presso il Tribunale di Roma al n. 99/87 del 2 marzo 1987, e con Consulenza Agricola, registrata presso il Tribunale di Forlì al n. 9/18 del 19 novembre 2018.

QUOTA SINGOLA DI PARTECIPAZIONE

Iscrizione al corso online

Euro 369,00 + IVA (se dovuta)

Il pagamento della quota deve avvenire all'atto di iscrizione per soggetti privati (Società, associazioni, cooperative, fondazioni, enti privati, libero professionista), mediante bonifico bancario utilizzando le seguenti coordinate:

Conto corrente bancario IBAN: IT74R0899524207000000092212 intestato ad Accademia Europea Formazione S.r.l. c/o Riviera Banca Credito Cooperativo di Rimini e Gradara, filiale di Rimini Città (RN).

Il pagamento della quota di iscrizione per gli enti pubblici avverrà di norma a 30 giorni data fattura (modalità applicabile per Enti Pubblici e Aziende a partecipazione pubblica).

Se la fattura è intestata ad Ente Pubblico, la quota è esente IVA, ai sensi dell'art. 10, D.P.R. n. 633/72 (e successive modificazioni). Nelle fatture emesse in esenzione IVA verrà addebitato il



costo del bollo virtuale pari a € 2,00.

Le adesioni si intenderanno perfezionate con la completa compilazione della domanda di iscrizione al webinar seguirà la trasmissione del link di collegamento all'evento e l'emissione della fattura elettronica.

È necessario procedere alla compilazione della domanda di iscrizione per ogni partecipante (in caso di più iscritti appartenenti ad uno stesso ente o azienda occorre indicare un indirizzo e-mail diverso per ogni partecipante).

Il contratto si intenderà concluso e quindi efficace e vincolante tra le parti nel momento in cui il cliente avrà inoltrato telematicamente il modulo di iscrizione seguendo l'apposita procedura online.

Agli iscritti assenti sarà garantita la trasmissione del link per accedere al video della formazione erogata e della relativa documentazione.

Il corso sarà corredato da idoneo materiale illustrativo e didattico in formato digitale e il rilascio dell'attestato di partecipazione.

Sarà attivo un servizio di segreteria organizzativa dalle ore 9,00 alle 13,00 al numero di telefono 0541/448562.

MODALITÀ DI PARTECIPAZIONE
PER ISCRIVERSI:
CLICCA QUI

Procedendo all'iscrizione, verrà perfezionata l'adesione al webinar (uno o più moduli) con impegno a procedere al pagamento per l'erogazione della formazione richiesta.

Prima dell'inizio del corso sarà inviata all'indirizzo e-mail indicato il link di collegamento al webinar e si procederà all'emissione della fattura elettronica.