ACCADEMIA EUROPEA

CORSO DI FORMAZIONE ONLINE

DIRETTIVA NIS2 2026 E ADEMPIMENTI OBBLIGATORI: I DOCUMENTI CHE GLI ORGANI DI AMMINISTRAZIONE E DIRETTIVI DOVRANNO APPROVARE ENTRO OTTOBRE 2026

Governance, template operativi e criteri di redazione secondo le Linee guida ACN

VENERDÌ 18 SETTEMBRE 2026

Dalle ore 9.00 alle ore 13.00

Codice MEPA: ZIH189MBR

PRESENTAZIONE

Il corso è dedicato agli adempimenti obbligatori previsti dalla Direttiva NIS2 e, in particolare, ai documenti che gli organi di amministrazione e direttivi dei soggetti NIS dovranno predisporre, esaminare e approvare entro la scadenza di ottobre 2026, secondo quanto previsto dalle Linee guida ACN.

L'incontro ha un taglio operativo e intende fornire ai partecipanti un quadro chiaro dei documenti richiesti, dei criteri di redazione da adottare e delle modalità con cui tali documenti devono essere collegati alla governance dell'organizzazione, alla valutazione del rischio, alle misure di sicurezza di base e al piano di adeguamento.

La Direttiva NIS2 non viene affrontata come un mero adempimento tecnico o documentale, ma come una disciplina di governo dell'organizzazione. La cybersicurezza incide infatti sugli assetti organizzativi, sulla gestione del rischio d'impresa, sulla continuità operativa, sui rapporti con i fornitori, sulla formazione del personale e sulle responsabilità degli organi apicali.

Particolare attenzione sarà dedicata al significato dell'approvazione dei documenti da parte degli organi di amministrazione e direttivi.

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: accademiaeuropa@pec.it www.accademiaeuropea.net

Tale approvazione non rappresenta un passaggio puramente formale, ma costituisce il momento in cui l'organizzazione assume decisioni su responsabilità, priorità, risorse, budget, controlli, monitoraggio e modalità di supervisione del percorso di adeguamento.
La prima parte del corso sarà dedicata alla governance NIS2, al ruolo degli organi apicali e al collegamento tra cybersicurezza, adeguati assetti organizzativi e continuità aziendale.
La seconda parte sarà dedicata all'analisi dei principali documenti richiamati dall'Appendice C delle Linee guida ACN, con proposte operative di template, criteri di impostazione, modalità di adattamento alla specifica organizzazione e indicazioni pratiche per l'approvazione, la verbalizzazione e la conservazione delle evidenze.
Ai partecipanti saranno messi a disposizione materiali operativi, template documentali e tracce utili per la predisposizione dei documenti da sottoporre agli organi competenti.

Obiettivi del corso:

Il corso si propone di fornire ai partecipanti strumenti pratici per:

- comprendere gli adempimenti obbligatori previsti dalla Direttiva NIS2 in vista della scadenza di ottobre 2026;
- individuare i documenti da predisporre e sottoporre all'approvazione degli organi di amministrazione e direttivi;
- comprendere il ruolo degli organi apicali nella governance della cybersicurezza;
- distinguere tra compliance formale e reale presa in carico del rischio cyber;
- impostare un sistema documentale coerente con le Linee guida ACN;
- adattare i template documentali alle caratteristiche dell'organizzazione;
- collegare valutazione del rischio, misure di sicurezza di base, piano di trattamento e piano di adeguamento;
- predisporre documenti utilizzabili in sede di approvazione da parte degli organi apicali;
- organizzare delibere, verbalizzazioni, flussi informativi e conservazione delle evidenze;
- documentare il percorso di adeguamento dell'organizzazione entro ottobre 2026.

Direttore scientifico del corso : **Avv. Gualtiero Roveda**

ACCADEMIA EUROPEA

PROGRAMMA DEL CORSO

Modulo webinar: Venerdì *18 settembre 2026*
Dalle 9.00 alle 10.30 - Docente Avv. Prof. Andrea R. Sirotti Gaudenzi

Direttiva NIS2, governance e responsabilità degli organi apicali
La NIS2 come disciplina di governo dell'organizzazione

La Direttiva NIS2 sarà esaminata non soltanto come disciplina tecnica in materia di sicurezza informatica, ma come normativa destinata a incidere sulla governance dell'organizzazione, sugli assetti interni, sui processi decisionali e sulla gestione del rischio.
La cybersicurezza diventa un elemento centrale dell'organizzazione aziendale o dell'ente, con effetti sulla continuità operativa, sulla gestione dei servizi essenziali o importanti, sulle responsabilità interne e sui rapporti con fornitori, partner e soggetti esterni.

☐ **Il ruolo degli organi di amministrazione e direttivi**

Saranno approfondite le responsabilità degli organi di amministrazione e direttivi, con particolare riferimento alla necessità di comprendere, approvare e supervisionare le misure di gestione del rischio cyber.

Saranno trattati, in particolare:

- responsabilità degli organi apicali;
- approvazione delle misure di sicurezza;
- supervisione del percorso di adeguamento;
- comprensione del rischio informatico;
- formazione degli organi di amministrazione e direttivi;
- attribuzione di ruoli e responsabilità;
- assegnazione di risorse e budget;
- controllo sull'effettiva attuazione delle misure.

☐ **L'approvazione dei documenti come atto di governance**

L'approvazione dei documenti richiesti dalle Linee guida ACN sarà analizzata come un vero atto di governance.
I documenti non costituiscono semplici allegati formali, ma strumenti attraverso i quali l'organo amministrativo definisce indirizzi, priorità, responsabilità, risorse, controlli e modalità di monitoraggio.

L'approvazione documentale rappresenta quindi un passaggio essenziale per dimostrare che l'organizzazione ha preso in carico il rischio cyber e ha avviato un percorso strutturato di adeguamento.

☐ **Cybersecurity, adeguati assetti e continuità aziendale**

Sarà approfondito il collegamento tra Direttiva NIS2, adeguati assetti organizzativi, gestione del rischio d'impresa e continuità aziendale.

Particolare attenzione sarà dedicata a:

- processi critici;
- sistemi informativi e di rete;
- continuità operativa;
- dipendenze da fornitori esterni;
- servizi IT e cloud;
- gestione delle crisi;
- responsabilità degli organi apicali;
- documentazione del percorso decisionale.

☐ **Dalla compliance documentale alla prova dell'organizzazione**

La parte finale dell'intervento sarà dedicata al valore probatorio della documentazione. Saranno esaminati gli strumenti attraverso i quali l'organizzazione può dimostrare l'effettiva presa in carico del rischio cyber:

- delibere;
- verbali;
- flussi informativi;
- report periodici;
- piani di adeguamento;
- monitoraggio delle attività;
- evidenze documentali;
- riesame periodico da parte degli organi competenti.

***Seconda parte*: Dalle 10.30 alle 13.00 - Docente Avv. Gualtiero Roveda**

I documenti dell'Appendice C: template operativi, criteri di redazione, approvazione ed evidenze
Come leggere l'Appendice C delle Linee guida ACN
La seconda parte del corso sarà dedicata all'individuazione e all'analisi dei documenti che devono essere predisposti e sottoposti all'approvazione degli organi di amministrazione e direttivi.
Saranno illustrati i criteri per costruire un perimetro documentale coerente con la struttura dell'organizzazione, con i requisiti applicabili e con le misure di sicurezza di base.

Saranno trattati:

- individuazione dei documenti richiesti;
- collegamento con i requisiti di riferimento;
- proporzionalità rispetto a dimensioni, attività, servizi e rischi;
- coordinamento tra documenti di governance e piani operativi;
- raccordo con il piano di adeguamento;
- evidenze da raccogliere e conservare.

☐ **Documenti oggetto dei template**

1. Organizzazione per la sicurezza informatica
Saranno forniti criteri per redigere il documento che descrive il modello organizzativo adottato per la cybersicurezza.

Il documento dovrà indicare:

- ruoli e responsabilità;
- funzioni coinvolte;
- referenti interni;
- flussi decisionali;
- flussi informativi verso gli organi apicali;
- rapporti con fornitori esterni;
- modalità di aggiornamento del modello organizzativo;
- raccordo con gli organi di amministrazione e direttivi.

2. Politiche di sicurezza informatica
Saranno illustrate le modalità per impostare le politiche generali di sicurezza informatica dell'organizzazione.

Il documento dovrà disciplinare:

- principi generali di sicurezza;
- obiettivi della politica;
- ambito di applicazione;
- regole interne;
- responsabilità;
- collegamento con procedure già esistenti;
- modalità di aggiornamento;
- criteri di comunicazione interna.

3. Valutazione del rischio posto alla sicurezza dei sistemi informativi e di rete
Sarà analizzato il documento di valutazione del rischio cyber quale base del percorso di adeguamento.

Saranno trattati:

- attività e servizi rilevanti;
- processi critici;
- sistemi informativi e di rete;
- minacce;
- vulnerabilità;
- impatti;
- misure di sicurezza esistenti;
- rischio residuo;
- criteri di priorità;
- collegamento con le misure di sicurezza di base.

4. Piano di trattamento del rischio
Saranno illustrate le modalità per trasformare la valutazione del rischio in un piano di azioni concrete.

Il piano dovrà contenere:

- misure da adottare;
- priorità di intervento;

- responsabili interni;
- scadenze;
- risorse necessarie;
- budget;
- fornitori coinvolti;
- modalità di verifica dell'attuazione;
- aggiornamenti da sottoporre agli organi apicali.

5. Piano di gestione delle vulnerabilità

Sarà analizzato il documento destinato a disciplinare l'identificazione, la valutazione e il trattamento delle vulnerabilità.

Saranno esaminati:

- scansioni periodiche;
- segnalazioni interne ed esterne;
- patch management;
- classificazione delle vulnerabilità;
- tempi di intervento;
- responsabilità operative;
- tracciamento delle attività;
- riesame periodico;
- raccordo con fornitori IT e servizi esterni.

6. Piano di adeguamento

Sarà illustrato come costruire il piano operativo verso la scadenza di ottobre 2026.

Il documento dovrà indicare:

- attività da completare;
- gap da colmare;
- cronoprogramma;
- priorità;
- responsabilità interne;
- fornitori coinvolti;
- dipendenze operative;
- evidenze da raccogliere;
- stato di avanzamento;
- aggiornamenti da presentare al CdA o all'organo equivalente.

7. Piano di continuità operativa
Saranno forniti criteri per impostare il documento finalizzato ad assicurare la continuità delle attività e dei servizi rilevanti.

Il piano dovrà considerare:

- scenari di indisponibilità;
- processi prioritari;
- servizi essenziali o importanti;
- risorse necessarie;
- ruoli e responsabilità;
- tempi di ripristino;
- comunicazioni interne ed esterne;
- verifiche e test periodici;
- collegamento con la valutazione del rischio.

8. Piano di ripristino in caso di disastro
Sarà approfondita la distinzione tra continuità operativa e disaster recovery.

Il piano dovrà disciplinare:

- sistemi critici;
- infrastrutture;
- backup;
- priorità di ripristino;
- responsabilità tecniche;
- tempi di recupero;
- test periodici;
- raccordo con fornitori IT, cloud provider e outsourcer;
- conservazione delle evidenze dei test effettuati.

9. Piano di gestione delle crisi
Saranno illustrate le modalità per predisporre un piano destinato alla gestione degli eventi critici che superano la normale operatività.

Il documento dovrà prevedere:

- composizione del gruppo di crisi;
- ruoli e poteri decisionali;

- procedure di attivazione;
- comunicazioni interne;
- comunicazioni esterne;
- rapporti con clienti e fornitori;

- rapporti con autorità e organi societari;
- gestione delle evidenze;
- riesame post-crisi.

10. Piano di formazione

Sarà analizzato il piano formativo necessario per supportare l'attuazione della Direttiva NIS2.

Il documento dovrà indicare:

- destinatari della formazione;
- contenuti formativi;
- periodicità;
- formazione degli organi apicali;
- sensibilizzazione del personale;
- formazione dei referenti tecnici e organizzativi;
- tracciamento delle presenze;
- conservazione delle evidenze;
- aggiornamento dei percorsi formativi.

11. Piano per la gestione degli incidenti di sicurezza informatica

Saranno forniti criteri per impostare ruoli, procedure e flussi relativi alla gestione degli incidenti cyber.

Il piano dovrà disciplinare:

- rilevazione degli incidenti;
- classificazione dell'evento;
- escalation interna;
- analisi dell'incidente;
- contenimento;
- raccolta delle evidenze;
- comunicazioni interne;
- coinvolgimento dei fornitori;

- collegamento con gli obblighi di notifica;
- riesame dell'incidente;
- azioni correttive.

☐ Approvazione, verbalizzazione e conservazione delle evidenze

Nella parte finale dell'intervento saranno esaminate le modalità operative per sottoporre i documenti agli organi di amministrazione e direttivi.

Saranno trattati:

- predisposizione delle delibere;
- verbalizzazione delle decisioni;
- indicazione dei documenti approvati;
- richiamo alla valutazione del rischio;
- approvazione di piani, misure, risorse e priorità;
- attribuzione delle responsabilità;
- richiesta di aggiornamenti periodici;
- gestione delle versioni documentali;
- conservazione delle evidenze;
- tracciabilità delle approvazioni;
- programmazione del riesame periodico;
- predisposizione di un fascicolo documentale NIS2.

☐ Materiali operativi per i partecipanti

Ai partecipanti saranno messi a disposizione materiali di supporto, tra cui:

- proposte operative di template documentali;
- tracce per la redazione dei principali documenti richiesti dalle Linee guida ACN;
- criteri per adattare i template alla propria organizzazione;
- schema di piano di adeguamento verso ottobre 2026;
- tracce di delibera;
- tracce di verbalizzazione;
- indicazioni per la conservazione delle evidenze documentali;
- schema di fascicolo documentale NIS2;
- indicazioni operative per il riesame periodico dei documenti approvati.

DESTINATARI

Il corso è rivolto ai soggetti coinvolti nella governance, nella gestione e nell'attuazione degli adempimenti previsti dalla Direttiva NIS2, in particolare, il corso si rivolge a:componenti degli organi di amministrazione, componenti degli organi direttivi, amministratori delegati, direttori generali, vertici aziendali, responsabili IT, responsabili della sicurezza informatica, CISO, security manager, cyber risk manager, responsabili compliance, responsabili legali, uffici affari societari, risk manager, internal auditor, responsabili continuità operativa e business continuity, DPO e referenti privacy coinvolti nei processi cyber, responsabili acquisti, procurement e gestione fornitori IT, consulenti legali, tecnici e organizzativi, enti pubblici, società private, gruppi societari, organizzazioni rientranti o potenzialmente rientranti nel perimetro NIS2.

DOCENTI DEL CORSO

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.

Coordina varie collane edite 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.
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 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 (Societa, associazioni, cooperative, fondazioni, enti privati, libero professionista), mediante bonifico bancario utilizzando le seguenti coordinale:

> 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.
La Direttiva Zangrillo (Ministero della Pubblica Amministrazione del 14 Gennaio 2025, prot. n. 123/2025) prevede l'obbligo di 40 ore annue di formazione per ogni dipendente pubblico, ed in ottemperanza a tale direttiva il corso prevede un Test finale, che sarà riportato nell'attestato di partecipazione.
Il corso sarà corredato da idoneo materiale illustrativo e didattico in formato digitale.
Sarà attivo un servizio di segreteria organizzativa dalle ore 9,00 alle 13,00 al numero di telefono Fisso 0541/448562 - Cel: 333-2430327.

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.