



CORSO DI FORMAZIONE ONLINE

DIRETTIVA NIS2, CYBERSICUREZZA, GDPR, PROTEZIONE DEI DATI E OBBLIGO DI FORMAZIONE PER I DIPENDENTI DELLE IMPRESE E DELLA P.A. TRA RISCHI E RESPONSABILITÀ

*Riconoscere le minacce, evitare le truffe
e proteggere le informazioni nel lavoro quotidiano*

VENERDÌ 11 DICEMBRE 2026
dalle ore 9:00 alle ore 12:00

Codice MEPA: ASMM2910

FORMARE IL PERSONALE È UN OBBLIGO PER LE ORGANIZZAZIONI

NIS2. Per i soggetti essenziali e importanti, la formazione in sicurezza informatica rientra nelle misure obbligatorie. Gli organi di amministrazione e direttivi devono promuoverne l'offerta periodica ai dipendenti (artt. 23, comma 2, lett. b), e 24, comma 2, lett. g), D.Lgs. 138/2024).

Privacy. Le organizzazioni devono istruire il personale che tratta dati personali e assicurare una formazione adeguata alle mansioni e ai rischi, nell'ambito delle misure organizzative richieste dal GDPR (artt. 29, 32 e 39, par. 1, lett. b)).

È previsto il rilascio di un attestato nominativo di partecipazione. L'organizzazione potrà conservare programma e presenze tra le evidenze della formazione svolta. Il percorso va integrato con le istruzioni e le procedure interne applicabili alle singole mansioni.

PRESENTAZIONE

Un messaggio ingannevole, una falsa telefonata o una password comunicata alla persona sbagliata possono provocare un blocco delle attività e la diffusione di dati personali. I dipendenti devono saper riconoscere queste situazioni e sapere come comportarsi, anche quando hanno già commesso un errore.

Il corso collega il quadro europeo della cybersicurezza alle precauzioni da adottare nel lavoro quotidiano. La prima parte, affidata all'Avv. Prof. Andrea R. Sirotti Gaudenzi, affronta la trasformazione digitale, la criminalità informatica e le dipendenze tecnologiche nello scenario europeo e internazionale.

La seconda parte, a cura dell'Avv. Gualtiero Roveda, segue un percorso pratico: truffe informatiche e telefoniche, furto d'identità, esposizione dei dati, controllo dei collegamenti e protezione degli accessi. Esempi, brevi video e prove guidate aiutano a riconoscere le richieste sospette e a segnalare tempestivamente gli errori.

Direttore scientifico: Avv. Gualtiero Roveda

OBIETTIVI DEL CORSO

- Comprendere i rischi informatici e le conseguenze per l'organizzazione e le persone.
- Riconoscere messaggi, telefonate, siti e richieste di accesso sospetti.
- Controllare un indirizzo web e interpretare una segnalazione di esposizione dei dati.
- Proteggere credenziali e informazioni, rispettando le istruzioni aziendali.
- Sapere quando e come avvisare i referenti interni, senza nascondere errori o cancellare prove.

PROGRAMMA DEL CORSO

Prima parte Modulo webinar: Venerdì 11 Dicembre 2026

Dalle ore 09,00 alle ore 10,30

Docente: Avv. Prof. Andrea R. Sirotti Gaudenzi

Cybersicurezza e trasformazione digitale nello scenario europeo e internazionale

1. La cybersicurezza: priorità dell'ordinamento europea e nazionale

La sicurezza digitale nell'evoluzione da questione specialistica a priorità per istituzioni, imprese e cittadini. La dimensione transnazionale delle minacce e le risposte fornite dal Legislatore UE. Protezione delle infrastrutture, stabilità economica e sicurezza collettiva. Il rischio dell'«effetto domino»

2. Le disposizioni UE: sicurezza e resilienza digitale

La direttiva NIS2 e l'iter europeo di rafforzamento della sicurezza e della cooperazione. Armonizzazione delle regole, mercato unico digitale e capacità dei sistemi economici di resistere alle perturbazioni. Il rapporto con le altre fonti UE e la disciplina dell'IA.

3. La criminalità informatica e l'economia digitale

L'evoluzione dei modelli criminali nell'ecosistema digitale. Problematiche legate alla territorialità delle condotte, all'individuazione degli autori e alla cooperazione tra Stati nel contrasto agli attacchi. Le fonti internazionali e le risposte nazionali.

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

Le previsioni che coinvolgono imprese e P.A. La protezione dei dati. Rapporti tra disciplina della cybersicurezza e tutela dei dati personali. L'uso dell'intelligenza artificiale e i rischi legati alla cybersicurezza.

Seconda parte Modulo webinar: Venerdì 11 Dicembre 2026

Dalle ore 10,30 alle ore 12,00

Docente: Avv. Gualtiero Roveda

Riconoscere le minacce e proteggere i dati: i comportamenti dei dipendenti

1. Il crimine informatico e le sue conseguenze

Come opera la criminalità informatica e quali informazioni cerca. Ingegneria sociale, vulnerabilità e malware. Danni economici, blocco delle attività e perdita di dati. Il ruolo della formazione del personale nel quadro NIS2 e privacy.

2. Phishing, truffe telefoniche e furto d'identità

Messaggi credibili e false emergenze. Le chiamate della banca e la falsificazione del numero visualizzato. Password, PIN, OTP e conferme nell'app. E-mail, SMS, codici QR, siti contraffatti e inviti nel calendario. Esempi di attacco e precauzioni. I miti da sfatare: il mittente conosciuto, il testo corretto e il lucchetto del browser.

3. Verificare l'esposizione del proprio indirizzo e-mail

Presentazione e utilizzo di Have I Been Pwned. Lettura dei risultati: quali servizi e dati risultano coinvolti. Che cosa fare in caso di esposizione. Password diverse, autenticazione a più fattori e avvisi sulle nuove violazioni. La segnalazione al referente informatico.

4. Riconoscere il sito a cui conduce un collegamento

Dominio e DNS spiegati con esempi. Come leggere un indirizzo web e individuare il dominio effettivo. Nomi ingannevoli e domini quasi identici. Controllo dei link su computer e telefono. Che cosa garantisce HTTPS. Prova pratica di riconoscimento degli indirizzi.

5. I comportamenti da adottare nel lavoro quotidiano

Controllo di mittenti, collegamenti, allegati e richieste insolite. Protezione delle credenziali e richieste di accesso inattese. Software autorizzati e istruzioni aziendali. Segnalazione tempestiva di dubbi ed errori, anche dopo un clic o la comunicazione di un dato. Conservazione degli elementi utili alla verifica.

6. Profili di responsabilità del dipendente nella sicurezza informatica e nella protezione dei dati

Doveri di diligenza, riservatezza e rispetto delle istruzioni aziendali. Uso improprio delle credenziali, accessi non autorizzati e divulgazione di informazioni. Possibili conseguenze disciplinari, risarcitorie e penali. Rilevanza della formazione ricevuta, delle mansioni svolte e della tempestiva segnalazione degli errori.

7. Il fattore umano nella sicurezza

I limiti della sola protezione tecnica. Fiducia eccessiva, abitudini e sottovalutazione degli avvisi. Collaborazione con chi gestisce la sicurezza. Domande dei partecipanti e indicazioni per il test finale.

DESTINATARI

Il corso è rivolto a dirigenti, segretari, amministratori, dipendenti e ai collaboratori di imprese private, pubbliche amministrazioni, società a partecipazione pubblica e in house, cooperative, enti del Terzo settore e studi professionali, con particolare riguardo al personale che utilizza quotidianamente sistemi informatici, applicativi e piattaforme digitali o tratta dati personali e informazioni riservate.

Il corso è inoltre di interesse per responsabili di ufficio, coordinatori del personale e responsabili della formazione, chiamati a promuovere comportamenti consapevoli, il rispetto delle istruzioni interne e la tempestiva segnalazione di anomalie ed errori.

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.

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 e giornalista pubblicista. Esercita la professione 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.

Svolge attività di consulenza e formazione in materia di sicurezza sul lavoro, legislazione alimentare, D.Lgs. 231/2001, protezione dei dati personali, sicurezza informatica, NIS2 e intelligenza artificiale. È stato componente del Comitato scientifico della Scuola Forense di Forlì-Cesena.

Da oltre vent'anni cura le relazioni industriali per un'Associazione nazionale di categoria. È responsabile tecnico della Commissione che stipula il contratto collettivo nazionale del relativo comparto e componente della Commissione paritetica nazionale.

Certificazioni

IDCERT, livello Specialised: Privacy Specialist; DPO / RPD; Digital Competence; IT Security.

Pubblicazioni e attività giornalistica

È autore e coautore di pubblicazioni giuridiche e d'impresa, tra cui La disciplina della sicurezza informatica (Simposio Editore, 2025), e ha partecipato al trattato La disciplina dell'intelligenza artificiale e degli algoritmi avanzati (Zanichelli, 2026). Ha scritto per Guida al Diritto - Il Sole 24 Ore e Altalex. Collabora con Fruitimprese e Consulenza Agricola.

QUOTA SINGOLA DI PARTECIPAZIONE

Iscrizione al corso online

Euro 399,00 + 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 fisso 0541/448562 e cellulare 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.