



CORSO DI FORMAZIONE ONLINE

LA GESTIONE DEGLI INCIDENTI INFORMATICI: RUOLI, PROCEDURE E RESPONSABILITÀ NIS2, GDPR, OBBLIGHI CONTRATTUALI E RESPONSABILITÀ VERSO TERZI

***AMMINISTRATORI, REFERENTE CSIRT, PUNTO DI CONTATTO NIS, DPO E
FUNZIONI AZIENDALI:***

***APPROVAZIONE DEI PIANI, RUOLI, FLUSSI DECISIONALI, NOTIFICHE E
GESTIONE DELL'EMERGENZA***

Martedì 24 NOVEMBRE 2026

Dalle ore 9,00 alle ore 13,00

CODICE MEPA: NO24AEF

PRESENTAZIONE

Un'e-mail compromessa, un attacco ransomware, la perdita di dati o il blocco dei sistemi: un incidente informatico può mettere in difficoltà qualsiasi organizzazione. Le prime decisioni sono determinanti, ma una risposta efficace si prepara prima dell'emergenza, attraverso misure di prevenzione, procedure chiare e persone consapevoli dei propri compiti.

Il corso affronta una domanda concreta: che cosa deve fare un'organizzazione prima, durante e dopo un incidente informatico? Dalla valutazione dei rischi all'attivazione della risposta, dalle notifiche alle autorità al ripristino delle attività, saranno esaminati gli adempimenti e le scelte che consentono di contenere le conseguenze dell'evento e documentare la correttezza dell'operato.

Al centro dell'incontro il coordinamento tra DPO, referente CSIRT, punto di contatto NIS e altre figure della sicurezza digitale: CISO, responsabili IT, amministratori di sistema,

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



responsabili della continuità operativa e fornitori tecnologici, con attenzione al ruolo degli organi di amministrazione e direttivi e, nelle pubbliche amministrazioni, del responsabile per la transizione digitale.

La formazione in materia di sicurezza informatica è anche un preciso adempimento organizzativo.

Per i soggetti NIS, gli organi di amministrazione e direttivi sono tenuti a seguire una specifica formazione e a promuovere periodicamente una formazione coerente per i dipendenti. Il corso si inserisce in questo percorso di aggiornamento e consapevolezza.

Al termine sarà rilasciato a ciascun partecipante un attestato di partecipazione.

Attraverso casi applicativi e l'esame degli orientamenti giurisprudenziali, il corso approfondisce il rapporto tra NIS2, D.Lgs. 138/2024, provvedimenti attuativi ACN e GDPR, distinguendo gli obblighi relativi agli incidenti significativi da quelli riguardanti le violazioni dei dati personali.

Particolare attenzione sarà dedicata alle responsabilità, all'adeguatezza delle misure di sicurezza e alla gestione dei rapporti con lavoratori, clienti e fornitori.

Responsabile scientifico del corso è l'Avvocato Gualtiero Roveda.

PROGRAMMA DEL CORSO

Modulo webinar: *Martedì 24 NOVEMBRE 2026*

Dalle ore 9,00 alle ore 10,30 – Docente: Avv. Prof. Andrea Renato Sirotti Gaudenzi

L'incidente informatico tra obblighi, tutela dei dati e responsabilità

- Riconoscere l'evento: attacco informatico, indisponibilità dei servizi, perdita e divulgazione non autorizzata dei dati.
- Incidente significativo ai fini NIS2 e data breach ai fini GDPR: differenze, sovrapposizioni e conseguenze.
- Il quadro normativo: D.Lgs. 138/2024, disposizioni attuative ACN e disciplina sulla protezione dei dati personali.
- Gli obblighi degli organi di amministrazione e direttivi: approvazione delle misure, supervisione e formazione.
- Ruolo del DPO: autonomia, coinvolgimento tempestivo e compatibilità con altri incarichi.
- Chi risponde dell'incidente? Responsabilità dell'organizzazione e delle figure coinvolte, secondo le rispettive attribuzioni.

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



- Gli orientamenti della Corte di giustizia sull'adeguatezza delle misure di sicurezza, sull'onere della prova e sul risarcimento del danno.
- Indicazioni del Garante e conseguenze operative per imprese ed enti.

Dalle ore 10,30 alle ore 13,00 – Docente: Avv. Gualtiero Roveda

Prima dell'incidente: Prevenzione e organizzazione

- Gli obblighi NIS2: misure di sicurezza e documenti da predisporre
- L'obbligo di adottare e rendere operative le misure di sicurezza di base previste dalla disciplina NIS2. I documenti dell'Appendice C che devono essere approvati dagli organi di amministrazione e direttivi. In particolare: piano di continuità operativa, piano di ripristino in caso di disastro, piano di gestione delle crisi, piano di formazione e piano per la gestione degli incidenti. Rapporti tra politiche, piani, procedure operative e allegati. Adattamento dei modelli alla concreta organizzazione aziendale e prove della loro effettiva attuazione.
- Piano di continuità operativa
- Individuazione dei servizi critici e delle relative dipendenze, soglie di indisponibilità, livelli minimi di servizio e condizioni di attivazione. Soluzioni alternative, risorse, contatti e schede operative. Esempio del gestionale ordini indisponibile: come continuare a lavorare e quando tornare alla normale operatività.
- Piano di ripristino in caso di disastro – Disaster Recovery
- Priorità di recupero, RTO e RPO, dipendenze tecniche e rapporti con i fornitori. Backup utilizzabili, ambienti sicuri e credenziali di emergenza. Schede di ripristino, test, verifica dei risultati e autorizzazione alla riattivazione dei sistemi.
- Piano di gestione delle crisi
- Quando un incidente informatico diventa una crisi e richiede decisioni straordinarie. Responsabile della crisi, gruppo di gestione, sostituti e reperibilità. Canali alternativi di comunicazione, rapporti con l'esterno e portavoce. Registrazione delle decisioni e condizioni per la chiusura della crisi.
- Formazione e preparazione delle persone
- Obblighi formativi e contenuti differenziati in funzione dei ruoli e dei rischi. Istruzioni al personale, formazione dei referenti e coinvolgimento dei fornitori. Registri, attestati, verifiche di apprendimento, esercitazioni e simulazioni.

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



- Piano di gestione degli incidenti, referente CSIRT e matrice RACI
- Perimetro del piano, criteri di attivazione, presa in carico ed escalation. Compiti del referente CSIRT e rapporti con punto di contatto NIS, organi apicali, IT, DPO, funzione legale e fornitori. Utilizzo della matrice RACI per stabilire chi interviene, chi decide, chi deve essere consultato e chi deve essere informato.
- Prepararsi concretamente all'incidente
- Le fasi della gestione dell'incidente secondo il processo ACN: preparazione, rilevamento, risposta, ripristino e miglioramento. Inventario di sistemi e servizi, dipendenze, minacce e vulnerabilità. Disponibilità dei contatti anche fuori rete, reperibilità dei fornitori, backup, log, credenziali e sistemi di accesso di emergenza. Come verificare prima dell'incidente che il piano sia realmente utilizzabile.

Durante l'incidente: Decisioni, interventi e notifiche

- Rilevamento, triage e qualificazione dell'evento
- Distinzione tra evento, incidente e quasi-incidente. Monitoraggio proattivo e reattivo, indicatori di compromissione e anomalie. Analisi degli allarmi e dei falsi positivi. Individuazione dei sistemi coinvolti, dei servizi interessati e delle possibili modalità di attacco.
- Attivazione della risposta e gestione dell'emergenza
- Prima segnalazione, apertura del diario dell'incidente e attivazione dei soggetti competenti. Valutazione iniziale, contenimento, isolamento dei sistemi interessati ed eradicazione della minaccia. Decisioni urgenti e coordinamento tra IT, referente CSIRT, organi aziendali, DPO, legale e fornitori.
- Investigazione e conservazione delle evidenze
- Ricostruzione della sequenza degli eventi. Raccolta e protezione di log, messaggi, file e altre evidenze utili. Delimitazione della compromissione e conservazione delle informazioni necessarie per notifiche, verifiche successive, eventuali contenziosi o procedimenti. Esempio di compromissione della posta elettronica aziendale.
- Incidenti significativi e notifiche NIS
- Criteri per individuare gli incidenti soggetti a notifica e fattispecie ACN IS-1, IS-2, IS-3 e IS-4. Decorrenza dei termini dall'acquisizione dell'evidenza dell'incidente. Pre-notifica, notifica e successive relazioni. Rapporti con CSIRT Italia e possibilità di notifica volontaria degli eventi che non raggiungono le soglie previste.

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



- Data breach GDPR e notifica al Garante
- Quando l'incidente informatico comporta anche una violazione dei dati personali. Valutazione del rischio per le persone, termine di 72 ore e contenuto della notifica. Ruoli di titolare, responsabile e DPO. Comunicazione agli interessati in caso di rischio elevato e documentazione delle decisioni assunte. Coordinamento tra adempimenti GDPR e NIS. Esempio della casella di posta elettronica compromessa.

Dopo l'incidente: ripristino e miglioramento delle procedure

- Ripristino e ritorno alla normale operatività. Recupero dei sistemi e dei servizi secondo le priorità stabilite. Verifica dell'integrità dei backup, bonifica degli ambienti compromessi e riattivazione progressiva. Controlli prima del rientro in produzione e autorizzazione alla riapertura dei servizi. Comunicazioni interne ed esterne sullo stato del ripristino.
- Chiusura dell'incidente e lezioni apprese. Quando un incidente può considerarsi concluso. Relazione finale, ricostruzione delle decisioni e verifica di ciò che ha funzionato e di ciò che deve essere corretto. Individuazione delle cause, delle vulnerabilità emerse e delle misure da adottare. Aggiornamento del piano incidenti, dei piani di continuità, disaster recovery e gestione delle crisi. Nuova formazione e simulazioni alla luce dell'esperienza maturata.

DESTINATARI DEL CORSO

Amministratori, dirigenti, DPO, referenti CSIRT e punti di contatto NIS; CISO e responsabili IT; amministratori di sistema; responsabili legali, compliance, risorse umane e continuità operativa; RTD e funzionari pubblici; avvocati, consulenti e professionisti della protezione dei dati e della sicurezza informatica.

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



DOCENTI DEL CORSO

AVV. PROF. ANDREA RENATO 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 membro del Comitato scientifico del Dipartimento interuniversitario di criminologia clinica, vittimologia e psicopatologia forense del Consorzio universitario Humanitas di Roma. Attualmente, è 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 commerciali edito da Maggioli.

Coordina varie collane edita da diverse case editrici e ha curato numerose pubblicazioni in tema di diritto commerciale, diritto industriale, proprietà intellettuale, diritto internazionale, diritto della concorrenza, diritto sportivo. È responsabile scientifico dell'Istituto nazionale per la formazione continua di Roma e di ADISI di Lugano.

AVV. GUALTIERO ROVEDA

Gualtiero Roveda, avvocato cassazionista e giornalista pubblicista, esercita l'avvocatura nel settore del diritto d'impresa e del lavoro. Cura da oltre vent'anni le relazioni industriali per un'Associazione nazionale di categoria ed è il responsabile tecnico della Commissione che stipula il Contratto Collettivo Nazionale di Lavoro per il comparto di riferimento della stessa. È, altresì, componente della Commissione paritetica nazionale istituita dallo stesso contratto. È il responsabile innanzi alla Direzione Provinciale del Lavoro ex art 12, L. 11 gennaio 1979 dell'organizzazione di uffici di gestione degli adempimenti in materia di lavoro. È stato componente del Comitato Scientifico della Scuola Forense di Forlì-Cesena. Svolge attività di

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



formatore in materia di Sicurezza sul lavoro, Legislazione alimentare, D. Lgs. 231/01 e Privacy. È Organo di vigilanza ex D. Lgs. 231/01 di imprese in ambito privato e pubblico. Ha pubblicato vari testi, tra cui «La fattura commerciale e la gestione del credito» (2003) e il «Manuale operativo del recupero crediti. Profili di diritto civile, processuale, internazionale e fiscale per la gestione legale ed il recupero del credito» (2008). Collabora stabilmente con testate giornalistiche con articoli di carattere giuridico. Ha conseguito le seguenti certificazioni: IDCERT – DIGITAL COMPETENCE: Level specialised; DPO/RPD: Level specialised; IT SECURITY: Level specialised; PRIVACY SPECIALIST: Level specialised.

QUOTA SINGOLA DI PARTECIPAZIONE

Iscrizione al corso online

Euro 399, 00 + IVA (se dovuta)

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

Conto corrente bancario IBAN: IT 74 R 08995 24207 000000092212 intestato ad ACCADEMIA EUROPEA FORMAZIONE S.R.L. c/o Riviera Banca Credito Cooperativo di Rimini e Gradara, filiale di Rimini Città (RN).

ENTI PUBBLICI: 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), con impegno a trasmettere la lettera d'ordine/determina recanti i dati per la fatturazione elettronica.

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.

Società abilitata al Mercato elettronico delle PA - Acquistinretepa

Le adesioni si intenderanno perfezionate con la completa compilazione della domanda di iscrizione al webinar (uno o più moduli), cui seguirà la trasmissione del link di collegamento all'evento ed 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

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



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.

Sarà attivo un servizio di segreteria organizzativa dalle ore 9,00 alle ore 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.

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