Corso di alta formazione
“Cyber risk e difesa aziendale”

Scopo del corso

Fornire alle imprese conoscenze teoriche e consigli pratici utili per aumentare in modo concreto la loro resilienza agli attacchi informatici.

Modalità

Erogazione di un corso composto da interventi formativi in presenza, caratterizzati da un'apertura a una platea ampia (assenza di prerequisiti tecnici) ed erogati in modo compatibile con gli impegni lavorativi dei partecipanti. Il taglio degli interventi formativi sarà divulgativo, prevederà approfondimenti su tematiche di specifico interesse e l’utilizzo di strumenti interattivi per favorire la partecipazione diretta dei discenti.

A chi è rivolto

Personale di imprese di ogni dimensione, con particolare riferimento a:

- personale con competenze e ruoli manageriali, chiamati a definire le priorità e le strategie aziendali
- personale incaricato di definire le politiche aziendali legate alla sicurezza informatica
- personale incaricato di trasformare le politiche di sicurezza informatica in procedure, con impatti concreti sull’organizzazione del lavoro all’interno della imprese
- personale coinvolto nella formazione e selezione del personale aziendale
- personale che tratta dati aziendali e utilizza strumenti informatici aziendali (locali o in Cloud)

Temi

Si discuteranno quattro temi principali:

- L’importanza delle **persone** per la cybersecurity
- La **gestione** della cybersecurity in azienda
- Le **tecnologie** per la cybersecurity
- **Normative e compliance**

Sede del corso

Il corso di terrà presso il nuovo Data Center sito in via Ermanno Gorrieri 31 a Modena.

Programma del corso

Venerdì 27 marzo 2026 14:30-18:30

Durata	Contenuto	Docenti	Tipologia
14:30-15:15	Introduzione al corso	Mirco Marchetti	Lezione frontale
15:15 - 16:15	Testimonianze di aziende vittime di attacchi	Imprenditori vittime di attacchi informatici. Introdotti da Antonio Apruzzese	Testimonianze
16:15 - 16:3	Coffee Break		
16:30-17:00	Il panorama degli attacchi informatici: la prospettiva delle forze dell'ordine	Antonio Apruzzese	Testimonianze
17:00 - 18:30	Attacchi e attaccanti: criminali informatici, ransomware, infostealer	Mirco Marchetti	Lezione frontale e dimostrazioni

Sabato 28 marzo 2026 9:00-13:00

Durata	Contenuto	Docenti	Tipologia
9:00 - 10:50	“Misurare” la sicurezza - progettare e condurre Vulnerability Assessment e Penetration Test	Mauro Andreolini	Lezione frontale e dimostrazioni
10:50 - 11:10	Coffee Break		
11:10 - 13:00	Cybersecurity management ● identificazione dei rischi informatici ● approcci quantitativi e qualitativi per la valutazione dei rischi informatici ● trattamento dei rischi informatici (elusione, esternalizzazione, riduzione, accettazione)	Fabio Cavazzuti	Lezione frontale e esercizi di cybersecurity management

Venerdì 17 aprile 2026 14:30 - 18:30

Durata	Contenuto	Docenti	Tipologia
14:30-16:10	Cybersecurity management e Business Continuity ● sicurezza informatica come strumento per la continuità del business ● business continuity plan ● business recovery plan	Fabio Cavazzuti	Lezione frontale e esercizi di cybersecurity management
16:10 - 16:30	Coffee Break		
16:30 - 17:30	Formare il personale: progettare ed erogare piani di formazione e awareness	Andrea Ruscitti	Discussione di casi di studio
17:30 -18:30	Cybersecurity e AI offensiva	Daniel Rozenek	Discussione di casi di studio

Sabato 18 aprile 2026 9:00 - 13:00

Durata	Contenuto	Docenti	Tipologia
9:00-9:55	Compliance e normative: NIS2, Macchine e Cyber Resilience Act	Andrea Balboni	Lezione frontale e discussione di casi di studio
9:55-10:50	Cybersecurity Monitoring e il ruolo dei Managed Security Service Providers	Bernardino Grignaffini	Lezione frontale e discussione di casi di studio
20 min	Coffee break		
11:10 - 13:00	Tavola rotonda: l'esperienza dei CISO. Modelli organizzativi per la cybersecurity in aziende e pubbliche amministrazioni	CISO di aziende	Tavola rotonda e discussione aperta

Venerdì 8 maggio 2026 14:30-18:30

Durata	Contenuto	Docenti	Tipologia
14:30 - 16:20	La direttiva NIS2: gli adempimenti per le aziende e i modelli organizzativi	Milena Rizzi	Lezione frontale e discussione
16:20 - 16:40	Coffee Break		
16:40 - 18:30	La direttiva NIS2: gli adempimenti per le aziende e i modelli organizzativi	Milena Rizzi	Lezione frontale e discussione

Sabato 9 maggio 2026 9:00-13:00

Durata	Contenuto	Docenti	Tipologia
9:00 - 11:20	Gestione del rischio nella supply chain digitale: selezione dei fornitori, contratti e compliance GDPR	Francesca Molinari	Lezione frontale e discussione di casi di studio
11:20 - 11:40	Coffee Break		
11:40 - 13:00	Il fenomeno dei Data Breach ● stato dell'arte in Italia e in Emilia Romagna ● Prevenzione, gestione e conseguenze	Cosimo Comella	Lezione frontale e discussione di casi di studio

Venerdì 22 maggio 2026 14:30-18:30

Durata	Contenuto	Docenti	Tipologia
14:30 - 15:40	Cybersecurity Management in pubbliche amministrazioni	Francesco Giorgianni	Lezione frontale
15:40 - 16:00	Coffee Break		
16:00 - 18:30	La gestione delle emergenze: come reagire in caso di attacco informatico	Mauro Cicognini	Esercizi di cybersecurity management in situazioni di emergenza

Sabato 23 maggio 2026 9:00-13:00

Durata	Contenuto	Docenti	Tipologia
9:00 - 11:10	Cybersecurity e responsabilità penale: ciò che i vertici aziendali (e i CISO) non possono ignorare	Francesco Diamanti	Lezione frontale e discussione di casi di studio
11:10 - 11:30	Coffee Break		
11:30 - 12:50	Attacchi e criminalità informatica, rapporti tra Forze Dell'ordine e imprese	Ivano Gabrielli	Testimonianza e discussione di casi di studio
12:50 - 13:00	Chiusura del corso e prossime iniziative	Antonio Apruzzese Mirco Marchetti	

Relatori

Mauro Andreolini: Docente di Sviluppo Software Sicuro e Sistemi Operativi presso l'Università di Modena e Reggio Emilia, co-direttore della Cyber Academy e referente per l'Università della Cyber Challenge;
Antonio Apruzzese: Prefetto e già Direttore della Polizia Postale e delle Comunicazioni, docente di Criminalità Informatica presso l'Università di Modena e Reggio Emilia;
Fabio Cavazzuti: CISO, responsabile di Infosecurity e Data Protection in Doxee s.p.a.;
Mauro Cicognini: membro del Comitato Tecnico Scientifico del Clusit, Founding Partner e direttore commerciale di Rexilience S.r.l;
Cosimo Comella: Dirigente dell'Autorità Garante per la Protezione dei Dati Personali, membro del consiglio scientifico della Fondazione ICSA, docente presso l'università LUISS
Francesco Diamanti: Professore di Diritto Penale presso l'Università di Modena e Reggio Emilia, direttore del Centro di Ricerca Interdipartimentale sulla Sicurezza Alimentare (CRISA);

Ivano Gabrielli: Direttore nazionale del Servizio di Polizia Postale e della Sicurezza Cibernetica;
Francesco Giorgianni: Data Protection Officer (DPO) della Fondazione Policlinico Universitario Agostino Gemelli IRCCS;
Mirco Marchetti: Professore di Sicurezza Informatica e Automotive Cyber Security presso l'Università di Modena e Reggio Emilia, Direttore del Centro di Ricerca Interdipartimentale sulla Sicurezza (CRIS);
Francesca Molinari: avvocato e vice procuratore onorario, DPO certificato e docente di Privacy e tutela dei dati presso l'Università di Modena e Reggio Emilia;
Milena Rizzi: Prefetto, Capo Servizio Regolazione dell'Agenzia per la Cybersicurezza Nazionale (ACN)
Andrea Ruscitti: Group Chief Information Officer, Iris Ceramica Group

Interverranno inoltre:

- Imprenditori vittime di attacchi informatici
- CISO e esperti di cyber security provenienti da aziende del territorio

Iscrizioni

Modalità di iscrizione e costi: https://cyber.unimore.it/corsi/cyber-risk-e-difesa-aziendale/