II EDIZIONE
Corso di Alta Formazione in "Cybersicurezza e protezione dei cyber rights"
Cybersecurity and cyber rights protection

A.A. 2025/2026

Venerdì 4 settembre	9.30-11.30	Introduzione al contesto tecnologico. Il concetto di sicurezza informatica e di cyberspazio	
	11.30-13.30	I principi costituzionali e sovranazionali in materia di cybersecurity	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	Quadro normativo di riferimento. La disciplina europea: Direttiva NIS, Direttiva NIS2, Cyber Security Act, Cyber Resilience Act, Cyber Solidarity Act	
	16.15-18.15	Quadro normativo di riferimento. La disciplina italiana: D. lgs. n. 65/2018 (attuazione NIS1), D.lgs. 138/2024 (attuazione NIS2), legge 28 giugno 2024, n. 90, DL 82/2021 (razionalizzazione)	
Venerdì 11 settembre	9.30-11.30	Il perimetro di sicurezza nazionale cibernetica (d.l. n. 105/2019, convertito con modificazioni dalla legge n. 133/2019): individuazione dei soggetti e dei beni ICT	
	11.30-13.30	Il PSNC: obblighi (notifiche di incidente e misure di sicurezza) e Linee Guida	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	Il golden power 'digitale'	
	16.15 - 18.15	Regolamento Cloud. I tre pilastri della strategia cloud Italia: classificazione, qualificazione, PSN (Polo Strategico Nazionale)	

Venerdì 18 settembre	9.30-11.30	Decreto NIS: principi generali, fasi attuative, ambito di applicazione e giurisdizione	
	11.30-13.30	Decreto NIS: governo e supervisione (Autorità coinvolte)	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	Decreto NIS: obblighi. Misure di sicurezza, responsabilità degli Organi di amministrazione e direttivi	
	16.15 – 18.15	Decreto NIS: obblighi. Notifiche di incidente, proporzionalità e gradualità degli obblighi, specifiche di base (Linee Guida NIS sulle specifiche di base)	
Venerdì 25 settembre	9.30-11.30	NIS e DORA. Principi e punti di contatto	
	11.30-13.30	Il ruolo dell'IA nella sicurezza informatica. AI Act: principi generali e governo, pratiche proibite e Code of Practice	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	Comprendere e gestire il CyberRisk: Dalla Teoria alla Pratica: Introduzione alla gestione dei rischi informatici e Identificazione del rischio, Valutazione e Trattamento del rischio, Monitoraggio, Reporting e Comunicazione	
	16.15-18.15	Laboratorio: Esercitazione Pratica che simula un caso reale di valutazione e trattamento del rischio	
Venerdì 2 ottobre	9.30-11.30	Cybersecurity e data breach, come minimizzare i rischi e reagire in caso di attacco	
	11.30-13.30	Laboratorio: Data Masking: dalla data governance a come mascherare i dati in modo sicuro ed efficace, garantendo la privacy e la compliance normativa	

	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	Sistemi informatici e hacking. Computer crimes, data breach e sicurezza informatica	
	16.15-18.15	Laboratorio: Implementazione e Configurazione di un SIEM: Configurare e utilizzare un sistema di gestione degli eventi di sicurezza (SIEM) per monitorare e rispondere agli eventi di sicurezza	
Venerdì 9 ottobre	9.30-11.30	L'importanza della sicurezza in azienda: security governance e management e la predisposizione dei modelli organizzativi sotto il profilo cybercrime	
	11.30-13.30	Tutela dei Database, patrimonio aziendale immateriale e nuovi profili di concorrenza	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	La gestione in concreto di un attacco ransomware (la notifica al Garante, i profili di diritto societario, fiscale, giuslavoristico)	
	16.15-18.15	Il danno da violazione delle infrastrutture di rete e violazione dei dati personali: risarcimento e nuovi prodotti assicurativi	
Venerdì 16 ottobre	9.30-11.30	Sicurezza informatica, continuità operativa e disaster recovery: adempimenti per le amministrazioni	
	11.30-13.30	Laboratorio: Cyber Incident Response: Preparazione e Gestione. Rispondere efficacemente a incidenti di sicurezza attraverso scenari simulati	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	Cybersecurity e data breach. Esame di un caso concreto. Minimizzazione dei rischi e resilienza in caso di attacco. Rapporti con le Autorità	

	16.15-18.15	Laboratorio: Vulnerability Assessment: dalla Scansione alla Mitigazione	
Venerdì 23 ottobre	9.30-11.30	Cybersecurity e PMI. L'elevata esposizione agli attacchi cyber delle piccole e medie imprese e l'importanza della sicurezza in azienda	
	11.30-13.30	Cybersecurity e remediation plan: strumenti e strutture a supporto delle piccole e medie imprese	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	Imprese collegate	
	16.15-18.15	Laboratorio del CISO	
Venerdì 30 ottobre	9.30-11.30	Cybersecurity e Settore pubblico. Le misure di sicurezza tecniche e organizzative per la Pubblica amministrazione.	
	11.30-13.30	Il problema del controllo a distanza dei lavoratori attraverso gli strumenti di cybersecurity e di monitoraggio	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	Laboratorio del Responsabile per la transizione al digitale (RTD) e del Referente per la Cybersicurezza	
	16.15-18.15	Laboratorio del Responsabile per la transizione al digitale (RTD) e del Referente per la Cybersicurezza	