Corso di Alta Formazione in "Cybersicurezza e protezione dei cyber rights"
ENG – *Cybersecurity and cyber rights protection*

Modulo 1 – Fonti e istituzioni della cybersicurezza			
Giovedì 20 marzo	9.30-11.30	I principi costituzionali e sovranazionali della sicurezza dei dati e della riservatezza	
	11.30-13.30	Ordine pubblico e cybersicurezza	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	Il concetto di sicurezza informatica e di Cyberspace	
	16.15 - 18.15	L'evoluzione della rete, i rischi e gli attacchi informatici: introduzione al contesto tecnologico	
Giovedì 27 marzo	10.00-11.30	Presentazione del Corso	
	11.30	Lezione inaugurale	
		Pausa pranzo	
	14.15-16.15	Il ruolo dell'Agenzia per la Cybersicurezza Nazionale nel panorama italiano ed europeo	
	16.15 - 18.15	Normative e regolamenti: la Cybersicurezza tra Direttive Europee e Legislazione Nazionale	

Giovedì 3 aprile	9.30-11.30	Panorama globale della Cybersicurezza: minacce crescenti in un mondo sempre più digitalizzato	
	11.30-13.30	Le radici della “Cyber-in-sicurezza”: le vulnerabilità sistemiche	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	Formazione, Consapevolezza e Responsabilità: costruire una cultura condivisa della cybersicurezza	
	16.15 - 18.15	Difendersi nel Cyberspazio: Best practices per mitigare le principali minacce informatiche	
Modulo 2 – La Cybersicurezza nel contesto tecnologico			
Giovedì 10 aprile	9.30-11.30	Comprendere e gestire il CyberRisk: Dalla Teoria alla Pratica: Introduzione alla Gestione dei Rischi Informatici e Identificazione del Rischio	
	11.30-13.30	Comprendere e gestire il CyberRisk: Dalla Teoria alla Pratica: Valutazione e Trattamento del Rischio	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	Comprendere e gestire il CyberRisk: Dalla Teoria alla Pratica: Monitoraggio, Reporting e Comunicazione	
	16.15-18.15	Laboratorio: Esercitazione Pratica che simula un caso reale di valutazione e trattamento del rischio	

Giovedì 17 aprile	9.30-11.30	Identity Security: La gestione delle identità digitali e normative di riferimento	
	11.30-13.30	Identity Security: Crittografia	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	Identity Security: Identity Management e Identity Governance	
	16.15-18.15	Identity Security: Access Management, Privileged Access Management e User Behavior Analysis	
Giovedì 8 maggio	9.30-13.30	Il ruolo dell'IA nella sicurezza informatica: il panorama delle minacce, le contromisure e il ruolo degli algoritmi e dell'IA nella protezione dei sistemi	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	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.	
	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.	

Modulo 3 - La tutela dei diritti nel cyberspace			
Giovedì 15 maggio	9.30-11.30	L'importanza della protezione dei dati personali: cenni sul Regolamento 2016/679, GDPR	
	11.30-13.30	L'importanza della protezione dei dati personali: analisi dell'art. 32 e ss. del Regolamento 2016/679, GDPR (misure di sicurezza tecniche e organizzative)	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	Laboratorio: Data Masking: dalla data governance a come mascherare i dati in modo sicuro ed efficace, garantendo la privacy e la compliance normativa	
	16.15-18.15	Laboratorio: Data Masking: dalla data governance a come mascherare i dati in modo sicuro ed efficace, garantendo la privacy e la compliance normativa	
Giovedì 22 maggio	9.30-11.30	Computer crimes, data breach e sicurezza informatica	
	11.30-13.30	Computer crimes, data breach e sicurezza informatica: giurisprudenza della Cassazione e provvedimenti dell'Autorità Garante	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	Laboratorio: Cyber Incident Response: Preparazione e Gestione. Rispondere efficacemente a incidenti di sicurezza attraverso scenari simulati.	
	16.15-18.15	Laboratorio: Cyber Incident Response: Preparazione e Gestione. Rispondere efficacemente a incidenti di sicurezza attraverso scenari simulati.	

Giovedì 29 maggio	9.30-11.30	Cybersecurity e data breach. Esame di un caso concreto. Minimizzazione dei rischi e resilienza in caso di attacco. Rapporti con le Autorità	
	11.30-13.30	Cybersecurity e data breach. Esame di un caso concreto. Minimizzazione dei rischi e resilienza in caso di attacco. Rapporti con le Autorità	
	13.30-14.15	*Pausa pranzo*	
	14.15-16.15	Laboratorio: Vulnerability Assessment: dalla Scansione alla Mitigazione	
	16.15 - 18.15	Laboratorio: Vulnerability Assessment: dalla Scansione alla Mitigazione	
		Modulo 4 - Cybersecurity e piccole e medie imprese	
Giovedì 5 giugno	9.30-11.30	L'elevata esposizione agli attacchi cyber delle PMI e l'importanza della sicurezza in azienda	
	11.30-13.30	I driver strategici della sicurezza cibernetica per le PMI: priorità e modelli operativi	
	13.30-14.15	*Pausa Pranzo*	
	14.15-16.15	Fondamenti di cybersecurity: dai concetti base alle figure professionali per l'azienda	
	16.15-18.15	Il cybercrimine e i presidi di prevenzione e protezione: strategie per la mitigazione del rischio informatico	

Giovedì 12 giugno	9.30-11.30	Il quadro normativo sulla sicurezza informatica: gestione del rischio e compliance per le PMI	
	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	Laboratorio: Cyber Personas: analisi degli attacchi alle MPMI e strategie di prevenzione e protezione	
	16.15-18.15	Laboratorio: Cyber Personas: analisi degli attacchi alle MPMI e strategie di prevenzione e protezione	
		Modulo 5 - Cybersecurity e Pubblica amministrazione	
Giovedì 19 giugno	9.30-11.30	Le misure di sicurezza tecniche e organizzative. Il problema del controllo a distanza dei lavoratori attraverso gli strumenti di Cybersecurity e di monitoraggio.	
	11.30-13.30	Approfondimento normativo: Direttiva NIS2, Perimetro di Sicurezza Nazionale Cibernetica, DDL Cyber 2024, Direttiva DORA, AI ACT, ecc.	
	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	

Giovedì 26 giugno	9.30-11.30	Focus su AgID (Agenzia per l'Italia Digitale) e Linee guida in materia di sicurezza, ruoli e responsabilità per le PA.	
	11.30-13.30	Come cambia la sicurezza nel Cloud. Cybersecurity e il Regolamento Unico per le infrastrutture e i servizi cloud per la p.a.	
	13.30-14.15	*Pausa Pranzo*	
	14.15-16.15	La cyber security nel piano triennale per l'informatica delle PA: Esplorare le principali misure e strategie previste dal Piano Triennale e comprendere gli strumenti pratici per migliorare la sicurezza informatica nelle proprie organizzazioni.	
	16.15-18.15	Continuità operativa e disaster recovery: differenza tra i due concetti e come implementarli. Come definire un piano di continuità operativa. Tecniche e strumenti di disaster recovery: soluzioni cloud, backup e ambienti ridondanti.	
	18.15-19.15	**Prova finale**	