

Cybersicurezza e protezione dei cyber rights - Cybersecurity and cyber rights protection

PARTE I - INFORMAZIONI GENERALI

Tipologia di corso

CorsoAltaFormazioneProfessionale

Titolo del corso

Cybersicurezza e protezione dei cyber rights - Cybersecurity and cyber rights protection

PARTE II - REGOLAMENTO DIDATTICO ORGANIZZATIVO

Indirizzo web del corso

https://ideas.uniroma3.it/?page_id=1703

Il Corso di Studio in breve

Il Corso di Alta Formazione in “Cybersicurezza e protezione dei cyber rights” prosegue – fornendo competenze settoriali ancora più specialistiche – il percorso del Master in “Protezione dei dati personali, Cybersicurezza e Diritto delle nuove tecnologie: Data protection officer, Chief information security officer e Chief artificial intelligence officer”, attivato dall'a.a. 2015/2016 presso il Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre, oramai giunto alla undicesima edizione. Il Corso di Alta Formazione – che si fregia del patrocinio dell'Agenzia per la Cybersicurezza Nazionale (ACN) – propone una formazione specialistica sul tema della cybersecurity, con l'obiettivo di far acquisire ai partecipanti elevate competenze, teoriche e pratiche, in materia di sicurezza cibernetica, con riferimento al contesto italiano ed europeo. A tal fine, la proposta didattica si fonda sull'interdisciplinarietà e la contaminazione dei saperi, requisiti essenziali, oggi, per affrontare le sfide poste dalle nuove tecnologie e le vulnerabilità dei sistemi informatici. Per tali ragioni, il Corso si articola in due parti, una generale e una speciale, con un focus su PMI e PPAA. Il programma è, inoltre, arricchito da una serie di laboratori che intendono fornire ai corsisti un risvolto pratico degli insegnamenti impartiti.

Obiettivi formativi specifici del Corso

Il percorso formativo è in grado di assicurare una preparazione adeguata sia dal punto di vista del quadro teorico di riferimento, che delle conoscenze pratico-applicative necessarie a ricoprire la figura professionale di Chief Information Security Officer (CISO). L'obiettivo del Corso è fornire un quadro completo e aggiornato della normativa in materia di sicurezza informatica, nonché delle misure di mitigazione dei rischi e delle conseguenze derivanti dagli incidenti di sicurezza informatica. Ai partecipanti del percorso formativo, dunque, saranno forniti gli strumenti per gestire i profili giuridici, tecnologici e organizzativi, anche attraverso dei laboratori mirati.

Prova finale

Le verifiche consisteranno in prove scritte intermedie, collocate al termine dei singoli moduli didattici, ed in una prova scritta finale inerente agli insegnamenti impartiti.

Obiettivi formativi specifici

Il percorso formativo è in grado di assicurare una preparazione adeguata sia dal punto di vista del quadro teorico di riferimento, che delle conoscenze pratico-applicative necessarie a ricoprire la figura professionale di Chief Information Security Officer (CISO). L'obiettivo del Corso è fornire un quadro completo e aggiornato della normativa in materia di sicurezza informatica, nonché delle misure di mitigazione dei rischi e delle conseguenze derivanti dagli incidenti di sicurezza informatica. Ai partecipanti del percorso formativo, dunque, saranno forniti gli strumenti per gestire i profili giuridici, tecnologici e organizzativi, anche attraverso dei laboratori mirati.

Informazioni utili agli studenti

-

Descrizione modalità di svolgimento

-

Requisiti di ammissione

Scadenza delle domande di ammissione: Domande di ammissione entro il 22 marzo 2026. Iscrizione entro il 12 aprile 2026. Classi di laurea dei titoli di accesso e ogni altro requisito specifico: Laurea triennale, magistrale, specialistica o titolo di studio equipollente in Giurisprudenza, Scienze politiche, Economia, Ingegneria. In presenza di posti disponibili, si valuteranno, ai fini della ammissione, lauree conseguite presso Dipartimenti diversi da quelli sopra indicati, sulla base del percorso formativo dell'interessato. Criteri di selezione nel caso in cui le domande di ammissione superino il numero massimo di ammessi: Curriculum vitae ed eventuale colloquio. Procedure e criteri per il riconoscimento di crediti maturati dagli studenti nel corso degli studi universitari precedenti ai fini di una eventuale riduzione del percorso formativo e delle tasse d'iscrizione: Nessuno.

Numero di posti

50

Durata prevista

3 Mese

Crediti previsti

30

Lingua di insegnamento

ITA

Modalità didattica

Convenzionale

Tasse di iscrizione ed eventuali esoneri

Importo totale
Euro 2500,00

I rata Euro 1500,00 Scad. I rata 12 aprile 2026
II rata Euro 1000,00 Scad. II rata 31 maggio 2026

Euro 2000,00 (per i laureati presso l'Università Roma Tre e per i soggetti iscritti ad Ordini professionali o altri soggetti con i quali sia stata sottoscritta apposita Convenzione)

I rata Euro 1000,00 Scad. I rata 12 aprile 2026
II rata Euro 1000,00 Scad. II rata 31 maggio 2026

Euro 1500,00(per gli ex corsisti del Master in "Protezione dei dati personali, Cybersicurezza e Diritto delle nuove tecnologie: Data protection officer, Chief information security officer e Chief artificial intelligence officer" e per i soggetti che beneficiano della Convenzione PA 110 e lode(lo sconto per tale convenzione è applicabile solo se il DFP selezionerà il corso per l'anno di riferimento).

I rata Euro 1000,00 Scad. I rata 12 aprile 2026
II rata Euro 500,00 Scad. II rata 31 maggio 2026

All'importo della prima rata sono aggiunti l'imposta fissa di bollo e il contributo per il rilascio del diploma o

dell'attestato.

Le quote di iscrizione non sono rimborsate in caso di volontaria rinuncia, ovvero in caso di non perfezionamento della documentazione prevista per l'iscrizione al Corso.

Esonero dalle tasse di iscrizione

È previsto l'esonero dal pagamento della II rata di iscrizione per gli studenti con disabilità documentata pari o superiore al 66%. Per usufruire dell'esonero è# necessario allegare alla domanda di ammissione un certificato di invalidità rilasciato dalla struttura sanitaria competente indicante la percentuale riconosciuta.

Non sono previste borse di studio al di fuori di quelle erogate eventualmente e direttamente ai corsisti dall'INPS, destinate a garantire l'alta formazione e l'aggiornamento professionale qualificato del personale dipendente delle Pubbliche Amministrazioni (Bando a.a. 2025/2026); nonché di quelle eventualmente erogate dal Centro di Ricerca Interdipartimentale Europeo di Studi Avanzati sull'Innovazione Digitale (Innovation Digital European Advanced Studies # IDEAS).

Tassa di iscrizione per uditori

La tassa di iscrizione ai Corsi in qualità di uditori è fissata in euro 2.000,00.

Rilascio titolo congiunto

Titolo normale

Direttore del Corso

Colapietro Carlo

PIANO DELLE ATTIVITA' FORMATIVE

(Insegnamenti, Seminari di studio e di ricerca, Stage, Prova finale)

Anno	Denominazione	SSD	CFU	Ore	Tipo Att.	Lingua
1	20110820 - Cybersecurity e piccole e medie imprese (PMI)	ING-INF/05 IUS/01 IUS/04 IUS/07 IUS/09	6	25	I	ITA
1	20110821 - Cybersecurity e Pubblica amministrazione	ING-INF/05 IUS/09 IUS/10	6	25	I	ITA
1	20110817 - Fonti e istituzioni della cybersicurezza	ING-INF/05 IUS/08 IUS/09 IUS/10 IUS/13 IUS/14	3	15	I	ITA
1	20110818 - La Cybersicurezza nel contesto tecnologico	ING-INF/05 IUS/09 IUS/14	6	30	I	ITA
1	20110819 - La tutela dei diritti nel cyberspace	ING-INF/05 IUS/09 IUS/14 IUS/17	6	30	I	ITA

OBIETTIVI FORMATIVI

20110820 - Cybersecurity e piccole e medie imprese (PMI)

Italiano

Con il modulo in esame si intende calare il tema della cybersecurity nel contesto specifico delle Piccole e medie imprese (PMI). Considerata la loro elevata esposizione agli attacchi cyber, l'obiettivo è quello di fornire alle PMI indicazioni funzionali ad apprestare un'adeguata tutela dei Database e del patrimonio aziendale immateriale. Ci si soffermerà altresì sul tema del risarcimento del danno da violazione delle infrastrutture di rete e da violazione dei dati personali, nonché sulle cc.dd. polizze cyber risk.

Inglese

The module in question aims to place the topic of cybersecurity in the specific context of Small and Medium Enterprises (SMEs). Given their high exposure to cyber attacks, the objective is to provide SMEs with functional indications to provide adequate protection of Databases and intangible corporate assets. We will also focus on the topic of compensation for damages from violation of network infrastructures and violation of personal data, as well as on the so-called cyber risk policies.

20110821 - Cybersecurity e Pubblica amministrazione

Italiano

Il presente modulo, infine, è volto ad approfondire il tema della cybersicurezza nel contesto della Pubblica amministrazione. Inquadrate i compiti e le funzioni delle istituzioni nazionali in materia di cybersecurity (AgID e ACN), ci si soffermerà sugli adempimenti cui le amministrazioni sono chiamate ad ottemperare per assicurare la sicurezza dei sistemi informatici utilizzati. Il programma si chiude con un apposito Laboratorio del Responsabile per la transizione al digitale (RTD).

Inglese

Finally, this module aims to explore the topic of cybersecurity in the context of public administration. Framing the tasks and functions of national cybersecurity institutions (AgID and ACN), we will focus on the obligations administrations are required to comply with to ensure the security of the information systems they use. The program closes with a special Digital Transition Manager (RTD) Workshop.

20110817 - Fonti e istituzioni della cybersicurezza

Italiano

Con il presente modulo, fornita un'introduzione di carattere generale sul concetto di sicurezza informatica e di cyberspace, ed evidenziati i principi costituzionali e sovranazionali fondamentali in materia di sicurezza dei dati e di riservatezza, si vuole delineare il quadro normativo di riferimento, nonché il ruolo delle istituzioni nazionali, europee e internazionali in materia. In particolar modo, ci si soffermerà sulle risposte provenienti dall'UE e dagli altri Paesi dinanzi alle sfide poste dalla cybersicurezza. Ci si soffermerà, altresì, sul tema del perimetro di sicurezza nazionale cibernetica

Inglese

With this module, providing a general introduction to the concept of information security and cyberspace, and highlighting the fundamental constitutional and supranational principles in the field of data security and confidentiality, we want to outline the regulatory framework of reference, as well as the role of national, European and international institutions in this area. In particular, we will focus on the responses from the EU and other countries to the challenges posed by cybersecurity. We will also focus on the topic of the perimeter of national cyber security

20110818 - La Cybersicurezza nel contesto tecnologico

Italiano

Il modulo è volto ad approfondire il concetto di cybersicurezza alla luce dell'attuale contesto tecnologico. Ci si soffermerà sul tema dell'organizzazione della sicurezza e della cybersicurezza aziendale, nonché sulle cc.dd. certificazioni cybersecurity e sui dispositivi industriali. Si tratterà un quadro delle minacce che l'insorgere di nuove tecnologie, come IA o l'Internet of Things, comporta per la tutela dei dati personali. Il modulo è arricchito da un apposito Laboratorio dedicato ai casi d'uso delle tecnologie emergenti per la sicurezza informatica.

Inglese

The module is aimed at deepening the concept of cybersecurity in light of the current technological context. We will focus on the topic of the organization of security and corporate cybersecurity, as well as on the so-called cybersecurity certifications and industrial devices. We will outline the threats that the emergence of new technologies, such as AI or the Internet of Things, entails for the protection of personal data. The module is enriched by a specific Laboratory dedicated

to the use cases of emerging technologies for cybersecurity.

20110819 - La tutela dei diritti nel cyberspace

Italiano

Scopo del modulo è quello di approfondire il tema della protezione dei dati nel cyberspazio. Si illustrerà, anzitutto, l'importanza della protezione dei dati personali, anche mediante l'analisi dell'impatto in materia del Regolamento europeo 2016/679 (GDPR). L'attenzione verrà, inoltre, appuntata sulle problematiche relative alla gestione del rischio digitale, nelle sue molteplici dimensioni. Si approfondiranno, altresì, le questioni di natura penale riguardanti il rapporto tra cybersecurity e computer crimes. Il programma del modulo prevede tre Laboratori che intendono fornire ai corsisti risvolti pratici degli insegnamenti impartiti.

Inglese

The aim of the module is to delve into the topic of data protection in cyberspace. First of all, the importance of personal data protection will be illustrated, also through the analysis of the impact on the matter of the European Regulation 2016/679 (GDPR). Attention will also be focused on the issues related to the management of digital risk, in its multiple dimensions. The criminal issues regarding the relationship between cybersecurity and computer crimes will also be explored. The program of the module includes three Laboratories that aim to provide students with practical implications of the teachings imparted.