Cybersicurezza e protezione dei cyber rights

Cybersecurity and cyber rights protection

PARTE I - INFORMAZIONI GENERALI

Tipologia di corso

Corso di Alta Formazione

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 – che ha ricevuto il patrocino dell'Agenzia per la Cybersicurezza Nazionale (ACN) – propone una formazione specialistica sul tema della cybersecurity, con l'obiettivo di far acquisire ai partecipanti adeguate competenze, teoriche e pratiche, in materia di sicurezza cibernetica. 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 articolerà in due parti e cinque moduli complessivi.

Nella prima parte, quella generale, dopo un'introduzione sul concetto di sicurezza informatica e di cyberspace, si metteranno in evidenza i principi costituzionali e sovranazionali in materia di sicurezza dei dati e della riservatezza, con analisi anche del quadro normativo attualmente vigente, sia in ambito nazionale che sovranazionale. Si approfondirà, inoltre, il ruolo svolto in materia dalle istituzioni nazionali, europee e sovranazionali, con peculiare attenzione alla risposta fornita dall'Unione europea e dagli altri Paesi alle sfide poste dalla cybersecurity, nonché specifico focus riservato anche all'individuazione del perimetro nazionale di sicurezza cibernetica (**Modulo 1**).

Quindi, si affronterà più puntualmente il tema della cybersecurity nel contesto tecnologico, con illustrazione anche degli elementi di base delle informazioni e dell'informatica. Si approfondiranno, inoltre, le tipologie di attacchi informatici, nonché i ruoli, le funzioni, gli ambiti e i rapporti nell'organizzazione della sicurezza e della cybersecurity aziendale, con connessa analisi anche della sicurezza di IoT e dei dispositivi industriali. L'attenzione sarà, infine, specificamente dedicata a ciascuna delle c.d. tecnologie emergenti (**Modulo 2**).

Il Corso affronterà poi la tematica della tutela dei diritti nel c.d. cyberspazio, con attenzione riservata non solo allo studio e valutazione dell'impatto fatto registrare dall'entrata in vigore del Regolamento 2016/679 (GDPR), ma anche alla considerazione e analisi di casi concreti in materia di data breach, tematica rispetto alla quale verrà, altresì, introdotto il discorso delle pronunce giurisprudenziali, per poi, da ultimo, mettersi in evidenza le modalità di acquisizione della prova in caso di attacco informatico e i vantaggi di cui sono connotati i sistemi di cybersecurity che utilizzano l'AI (**Modulo 3**).

Nella seconda parte, quella speciale, il focus sarà riservato ai comparti della Pubblica amministrazione e delle Piccole e medie imprese (PMI). In particolare, nel Modulo inerente alle PMI verrà affrontata la tematica delle modalità di gestione in concreto degli attacchi cyber, a fini di tutela delle informazioni e patrimonio aziendale, nonché dei danni che simili attacchi possono produrre rispetto al patrimonio aziendale immateriale e delle polizze che possono consentirne la neutralizzazione (**Modulo 4**).

Nel modulo dedicato alle Pubbliche amministrazioni, analogamente, a seguito dell'illustrazione dei compiti e delle funzioni delle istituzioni nazionali in materia di cybersecurity, e degli atti frattanto adottati, verranno messe in evidenza le pratiche di sicurezza informatica da attuare, con illustrazione delle modalità di gestione del relativo rischio (**Modulo 5**).

Il programma è, inoltre, arricchito da una serie di laboratori che intendono fornire ai corsisti un risvolto pratico degli insegnamenti impartiti.

Obiettivi formativi specifici

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. Nel corso degli ultimi anni, anche a seguito delle misure per il contenimento della pandemia da Covid-19, le Istituzioni e i privati hanno impresso una notevole accelerazione al processo di trasformazione digitale. Il tema della sicurezza informatica, dunque, è sempre più attuale. Sono quotidiane le notizie di attacchi a soggetti pubblici e privati che portano l'argomento al centro del dibattito pubblico e, negli ultimi tempi, anche politico. Quando si parla di "sicurezza informatica" ci si riferisce all'esigenza di garantire la "disponibilità, integrità e riservatezza delle informazioni". Il tema, dunque, è strettamente legato alla tutela dei diritti delle persone e, in particolare, a quello della privacy, quando i rischi attengono ai dati personali degli interessati, ma, in termini più ampi, ormai riguarda la stessa difesa degli ordinamenti, alla luce del fatto che molti attacchi sono volti a minare la stessa stabilità politica degli Stati. 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

Requisiti di ammissione e modalità di selezione

Classi di laurea dei titoli di accesso e ogni altro requisito specifico: laurea triennale, magistrale, specialistica o titolo di studio equipollente.

In considerazione dell'erogazione gratuita per il corrente anno accademico del Corso di Alta Formazione e del numero limitato di posti a disposizione, la selezione dei partecipanti sarà effettuata:

a) assicurando la massima partecipazione di Pubbliche Amministrazioni (PP.AA.) e Piccole e medie imprese (P.M.I.), garantendone la loro più ampia rappresentazione;

b) selezionando i partecipanti in relazione alle specifiche esigenze di formazione in materia di cybersecurity alla luce della funzione/ruolo svolto all'interno dell'organizzazione di appartenenza.

A tal fine, unitamente alla richiesta di ammissione alla selezione, gli interessati dovranno presentare, secondo le modalità indicate nel *form* per la richiesta di ammissione, la seguente documentazione aggiuntiva (al seguente indirizzo e-mail: corsoaltaformazionecyber@uniroma3.it):

- una lettera motivata di presentazione del candidato dell'Amministrazione/Società a firma del Dirigente/Responsabile della struttura presso cui è incardinato (non inferiore a 5.000 caratteri);

- il Curriculum Vitae et Studiorum (in formato PDF) nel quale siano indicati chiaramente, in distinte sezioni:

  • i titoli di studio posseduti o in corso di conseguimento (laurea triennale, magistrale o vecchio ordinamento, specialistica, Dottorato di ricerca, Master di I e di II livello, Corsi di perfezionamento, ecc.);

  • le esperienze lavorative attuali e, eventualmente, quelle pregresse;

  • le conoscenze linguistiche possedute.

Scadenza del termine per presentare le richieste di ammissione attraverso l'apposito *form* presente sul sito dell'iniziativa (https://ideas.uniroma3.it/?page_id=1703): **10/03/2025** (compreso).

Si rappresenta che il *form* per la richiesta di ammissione al Corso verrà disattivato **in data precedente al 10/03/2025**, nel momento in cui venga raggiunto il numero di domande di ammissione al Corso pari al numero dei disponibili.

Ricevuta la conferma di ammissione all'indirizzo e-mail indicato nel *form*, sarà necessario iscriversi tramite il portale GOMP dell'Università degli Studi Roma Tre, entro il **19/03/2025** (compreso), secondo le indicazioni che verranno fornite.

Descrizione modalità di svolgimento

Il Corso di Alta Formazione è fruibile esclusivamente in presenza, presso il Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre (Via Ostiense, 159-163).

Ai fini del conseguimento del titolo, sono necessari la frequenza dei 2/3 delle lezioni e il superamento dell'esame finale, vertente sui temi trattati durante il Corso.

Numero di posti

50 posti in presenza. In accordo con l'Agenzia per la cybersicurezza nazionale, nell'ambito del rafforzamento delle competenze del personale delle amministrazioni rappresentate nel **Nucleo per la cybersicurezza**, istituito presso la stessa ACN, è stata destinata – all'interno dei complessivi 50 posti – una **riserva di posti** a quel personale. A tal fine, in sede di iscrizione, dovrà essere indicata, nell'apposita sezione, l'appartenenza ad

una delle predette amministrazioni.

Durata prevista

3 mesi (dal 20/03/2025 al 26/06/2025).

Crediti previsti

30

Lingua di insegnamento

Italiano

Modalità didattica

Didattica frontale Tasse di iscrizione ed eventuali esoneri

https://www.uniroma3.it/didattica/post-lauream/

Il Corso, esclusivamente per l'A.A. 2024-2025, sarà erogato gratuitamente, in quanto finanziato con i fondi del Progetto PNRR, denominato HARD DISC.

In sede di iscrizione il corsista è, comunque, tenuto a versare l'imposta fissa di bollo e il contributo per il rilascio del diploma, pari ad euro 31,00 (trentuno/00).

Direttore del Corso

Prof. 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	**20110817 - Fonti e istituzioni della cybersicurezza**	IINF-05/A GIUR-05/A GIUR-06/A GIUR-09/A GIUR-10/A	7	35	I	ITA
1	**20110818 - La Cybersicurezza nel contesto tecnologico**	IINF-05/A GIUR-05/A GIUR-10/A	7	35	I	ITA
1	**20110819 - La tutela dei diritti nel cyberspace**	IINF-05/A GIUR-05/A GIUR-10/A GIUR-14/A	7	35	I	ITA
1	**20110820 - Cybersecurity e piccole e medie imprese (PMI)**	IINF-05/A GIUR-01/A GIUR-02/A GIUR-04/A GIUR-05/A	4	20	I	ITA
1	**20110821 - Cybersecurity e Pubblica amministrazione**	IINF-05/A GIUR-05/A GIUR-06/A	5	25	I	ITA

OBIETTIVI FORMATIVI

20110817 - Fonti e istituzioni della cybersicurezza

Italiano

Con il I 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 dinnanzi alle sfide poste dalla cybersicurezza. Ci si soffermerà, altresì, sul tema del perimetro di sicurezza nazionale cibernetica.

Inglese

With Module I, provided a general introduction on the concept of cybersecurity and cyberspace, and highlighted the basic constitutional and supranational principles on data security and privacy, the aim is to outline the relevant regulatory framework, as well as the role of national, European and international institutions in this regard. In particular, we will focus on the responses from the EU and other countries in the face of the challenges posed by cybersecurity. We will also address the issue of the national cybersecurity perimeter.

20110818 - La Cybersicurezza nel contesto tecnologico

Italiano

Il II 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 traccerà 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

Module II is aimed at exploring the concept of cybersecurity in light of the current technological environment. It will focus on the topic of security organization and enterprise cybersecurity, as well as on the so-called cybersecurity certifications and industrial devices. An overview will be drawn of the threats that the rise of new technologies, such as AI or the Internet of things, poses to the protection of personal data. The module is enhanced by a special Lab dedicated to use cases of emerging cybersecurity technologies.

20110819 - La tutela dei diritti nel cyberspace

Italiano

Scopo del III 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 purpose of Module III is to delve into the topic of data protection in cyberspace. First and foremost, the importance of personal data protection will be illustrated, including through the analysis of the impact on the subject of European Regulation 2016/679 (GDPR). Attention will, in addition, be focused on issues related to digital risk management, in its many dimensions. Issues of a criminal nature concerning the relationship between cybersecurity and computer crimes will also be explored. The module program includes three Workshops that are intended to provide the students with practical implications of the teachings given.

20110820 - Cybersecurity e piccole e medie imprese (PMI)

Italiano

Con il IV modulo 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

Module IV aims to drop the topic of cybersecurity into the specific context of Small and Medium Enterprises (SMEs). Given their high exposure to cyber-attacks, the goal is to provide SMEs with functional guidance to prepare adequate protection of Databases and intangible business assets. There will also be a focus on the topic of compensation for damages from network infrastructure breaches and personal data breaches, as well as the so-called cyber risk policies.

20110821 - Cybersecurity e Pubblica amministrazione

Italiano

Il V modulo, infine, è volto ad approfondire il tema della cybersicurezza nel contesto della Pubblica amministrazione. Inquadrati 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, Module V is aimed at delving into the topic of cybersecurity in the context of public administration. Framing the tasks and functions of the national cybersecurity institutions (AgID and NCA), 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's Workshop (RTD).