



UNICUSANO

Università degli Studi Niccolò Cusano - Telematica Roma

| | |
|---|---|
| Insegnamento | Cybersecurity e protezione dei dati |
| Livello e corso di studio | Corso di laurea magistrale in giurista d'impresa |
| Settore scientifico disciplinare (SSD) | IUS 01 |
| Anno accademico | 2025-2026 |
| Anno di corso | |
| Numero totale di crediti | 9 |
| Propedeuticità | Non presente |
| Docente | Fabio Di Resta Corso di Laurea in Giurisprudenza Nickname: fabio.diresta Email: fabio.diresta@unicusano.it Orario di ricevimento: Consultare il calendario alla pagina seguente del nostro sito verificando gli orari di Videoconferenza http://www.unicusano.it/calendario-lezioni-in-presenza/calendario-area-ingegneristica |
| Presentazione | <i>Il corso in Cybersecurity e protezione dei dati è suddiviso in due macroaree, la prima riferita alla Cybersecurity, nelle lezioni vengono descritti gli elementi fondamentali della materia con numerosi casi di studio in modo che lo studente possa immediatamente cimentarsi con le fattispecie pratiche. La prime lezioni esaminano gli elementi definitori della Cybersecurity, seguono alcune lezioni sulle nozioni tecniche e sugli istituti giuridici coinvolti nella trattazione della materia. Vengono pertanto esaminate le fonti normative europee e nazionali nonché i principi e criteri che caratterizzano la materia della Cybersecurity. In tale contesto, si analizza le principali differenze e le analogie con la diversa materia della protezione dei dati personali, tenendo in conto dello scopo, del metodo adottato dal legislatore e le fonti normative. La seconda macroarea è riferita invece a quadro normativo sulla protezione dei dati personali, dalle fonti internazionali, alle fonti del diritto europeo alle fonti normative nazionali. In tale contesto, sono previste ventiquattro lezioni, anche in questo caso i numerosi casi di studio presentati forniscono allo studente la possibilità di applicare la fattispecie astratta della disposizione normativa alla fattispecie pratica. Le prime lezioni introduttive illustrano le nozioni fondamentali della materia per successivamente concentrarsi sui principi e criteri della protezione dei dati personali.</i> |
| Obiettivi formativi | Il corso in Cybersecurity e protezione dei dati ha i seguenti obiettivi formativi: <ol style="list-style-type: none"> 1. Rivedere le basi della cybersecurity e della protezione dei dati personali 2. Illustrare i principi e criteri principali della cybersecurity 3. Illustrare i principi e criteri principali della protezione dei dati personali 4. Illustrare casi di studio sia ambito di Cybersecurity che in ambito protezione dei dati personali 5. Trasferire allo studente una abilità di analisi delle fattispecie concrete relativamente all'ambito delle due discipline trattate |
| Prerequisiti | Non sono previste propedeuticità per l'insegnamento. |
| Risultati di apprendimento attesi | <p>Conoscenza e capacità di comprensione Lo studente al termine del Corso avrà dimostrato di conoscere gli argomenti di Cybersecurity e di protezione dei dati personali, ed avrà acquisito la capacità di analisi degli stessi. Inoltre, lo studente acquisirà la conoscenza del quadro normativo dell'insegnamento, inclusi, l'analisi del rischio in ambito di cybersecurity e ambito di rischi inerente al trattamento dei dati personali, i soggetti passivi degli obblighi previsti dalle normative applicabili, le responsabilità giuridiche relative.</p> <p>Applicazione delle conoscenze Lo studente sarà in grado di utilizzare la conoscenza delle due discipline trattate durante le lezioni; sarà inoltre in grado di analizzare fattispecie concreti di incidenti di sicurezza sia ambito di cybersecurity che di protezione dei dati, individuando i requisiti normativi applicabili sia in termini preventivi, come per esempio, i requisiti dalla data protezione protection by design e la cybersecurity by design.</p> <p>Capacità di trarre conclusioni</p> |

| | |
|---|---|
| | <p>Lo studente sarà in grado di individuare i soggetti passivi degli obblighi normativi: titolare del trattamento, contitolare del trattamento, responsabili del trattamento, anche con riguardo all'organizzazione interna del soggetto con specifico riguardo agli autorizzati e ai designati al trattamento dei dati. Per quanto concerne la cybersecurity, lo studente sarà in grado di comprendere la rilevanza del rischio relativo alle reti ed ai sistemi informativi e la rilevanza di individuare le misure di sicurezza volte alla mitigazione del rischio.</p> <p>Abilità comunicative</p> <p>Lo studente sarà in grado di descrivere e sostenere conversazioni su problemi di dinamica e cinematica di sistemi meccanici piani, individuando correttamente le grandezze fisiche rilevanti, e adoperando una terminologia adeguata.</p> <p>Capacità di apprendere</p> <p>Lo studente al termine del Corso avrà conoscenza delle nozioni fondamentali necessarie comprendere da una parte i rischi inerente alle informazioni gestite da parte delle infrastrutture critiche e connesse alle funzioni essenziali dello Stato e dall'altra, in termini di protezione dei dati, la tutela dei diritti e delle libertà fondamentali degli interessati che concreto si atteggiavano anche come diritto al controllo dei propri dati personali sia nella forma dei diritti di accesso, nel diritto all'esattezza dei dati, nel diritto all'integrità dei dati, alla portabilità degli stessi ed infine ad opporsi a trattamenti dei propri dati quando questi trattamenti diventano illegittimi.</p> |
| Organizzazione dell'insegnamento | <p>Il corso è sviluppato attraverso le lezioni preregistrate audio-video che compongono, insieme a slide e dispense, i materiali di studio disponibili in piattaforma.</p> <p>Sono poi proposti dei test di autovalutazione, di tipo asincrono, che corredano le lezioni preregistrate e consentono agli studenti di accertare sia la comprensione, sia il grado di conoscenza acquisita dei contenuti di ognuna delle lezioni.</p> <p>In particolare, il Corso di Cybersecurity e protezione dei dati prevede 8 Crediti formativi. Il carico totale di studio per questo modulo di insegnamento è compreso tra 220 e 250 ore così suddivise in:</p> <p>circa 160 ore per la visualizzazione e lo studio del materiale videoregistrato (20 Ore videoregistrate di Teoria e analisi di casi di studio presentate durante la lezione).</p> <p>Circa 10 ore di Didattica Interattiva per l'esecuzione dei test di autovalutazione.</p> <p>Si consiglia di distribuire lo studio della materia uniformemente in un periodo di 10 settimane dedicando tra le 15 alle 20 ore di studio a settimana</p> |
| Contenuti del corso | <p>Modulo 1 – Parte sulla Cybersecurity</p> <p>Le lezioni teorico pratiche videoregistrate per un impegno del 30% del totale di ore previste dall'insegnamento: Analisi dei concetti fondamentali sulla Cybersecurity e la protezione dei dati personali - Inquadramento storico della cybersecurity: dai conflitti del XX secolo alla cyberwar - Analisi del rischio in ambito cybersecurity e la rilevanza del settore bancario - Analisi degli elementi della cybersecurity: il web, internet e la nozione di RID. La Cybersecurity nel contesto non giuridico e nel giuridico - la protezione dei dati - Schema di analisi in ambito protezione dei dati: i sei quesiti sulla protezione dei dati - aspetti strettamente connessi della cybersecurity - lezione su Cybersecurity e protezione dei dati: il Cybersecurity Act, ENISA e ACN - Lezione su Cybersecurity e la protezione dei dati: pandemia e cybersecurity: rischi connessi alla pandemia e l'approccio proattivo - La cybersecurity e la protezione dei dati: il contact tracing (CT), aspetti di cybersecurity e protezione dei dati - Lezione su cybersecurity e protezione dei dati: analisi del quadro normativo sui servizi di pagamento: normativa tecnica e autenticazione forte - Analisi dei crimini informatici: frode informatica e aggravante della frode, accesso abusivo al sistema informatico - Analisi della violazione dei dati (c.d. Data Breach): presupposti e adempimenti connessi previsti dal GDPR - Lezione Cybersecurity e protezione dei dati: servizi: recepimento. NIS e Perimetro di sicurezza nazionale - Analisi dei crimini informatici: frode informatica e aggravante della frode, accesso abusivo al sistema informatico - d.lgs. 11/2010 sui servizi di pagamento e responsabilità degli intermediari (Istituto di credito e prestatori di servizi di pagamento). Il quadro normativo sulla cybersecurity viene completato con il materiale rilevante sulla nuova direttiva (UE) 2022/2555 (c.d. Direttiva NIS 2), che è andata ad abrogare la direttiva NIS 1, anche con riferimento al decreto di recepimento della Direttiva NIS 2, il d.lgs. 138/2024 e la legge n. 90 del 18 giugno 2024.</p> <p>Modulo 2 – Parte sulla Protezione dei dati personali</p> <p>24 lezioni teorico pratiche videoregistrate per un impegno del 50% del totale di ore previste dall'insegnamento: Analisi del quadro normativo complessivo sulla protezione dei dati personali - Scopo e ambito applicativo della normativa sulla protezione dei dati personali - Principi applicabili sulla protezione dei dati personali: principi applicabili al trattamento dei dati - Principi di liceità sulla protezione dei dati personali - Analisi dei requisiti del Consenso sulla protezione dei dati personali: articolo 7 del GDPR - Analisi delle garanzie del GDPR per il trattamento di categorie particolari dei dati personali - Seconda parte della lezione sulle garanzie previste dal GDPR in materia di trattamento di categorie particolari di dati personali - Garanzie in ambito trattamento dati giudiziari - Lezione sul livello di sicurezza adeguato al rischio inerente al trattamento dei dati: valutazione del rischio e criterio di efficacia delle misure di sicurezza nel quadro delle responsabilità generali del trattamento dei dati personali - Il principio della data protezione protection by design e by default - le responsabilità generali del titolare del trattamento dei dati personali - nozione di rischio di pregiudizio sui diritti e libertà fondamentali in termini di gravità dell'evento - Analisi della autonoma titolarità del trattamento e le responsabilità generali dello</p> |

| | |
|---|---|
| | <p>stesso: i soggetti passivi degli obblighi previsti dal GDPR - L'accordo sulla protezione dei dati personali, il responsabile del trattamento, ambito applicativo, presupposti, distribuzione dei compiti e responsabilità - articolo 28 GDPR prima - Analisi degli elementi del contratto sulla protezione dei dati personali - responsabile della trattamento dei dati seconda parte - aspetti connessi alle responsabilità amministrative solidali delle figure che occupano una posizione apicale - L'organizzazione sulla protezione dei dati all'interno del titolare del trattamento: distribuzione dei compiti e responsabilità tra gli autorizzati al trattamento e i designati - art. 29 GDPR e art. 2 quaterdecies del Codice della Privacy - L'esercizio dei diritti degli interessati: diritto di accesso ai dati e gamma dei diritti dell'interessato, dal diritto all'esattezza, all'integrità, all'aggiornamento, all'opposizione dei dati, alla portabilità dei dati - analisi dei compiti e funzioni – La tutela giurisdizionale nell'ambito della protezione dei dati personali: il risarcimento del danno e la violazione dei diritti e libertà fondamentali - Analisi critica della richiesta di risarcimento del danno da trattamento illecito dei dati, danni materiali e immateriali, il nesso causale - Analisi del consenso al trattamento ambito applicativo e presupposti, cenni sul consenso del minore - Analisi del Consenso e del consenso del minore di età nella società dell'informazione - La prestazione del consenso del minore articolo 2 quinquies del codice della privacy - Analisi dei rischi e Valutazione di Impatto - Lezione sul Responsabile della protezione dei dati _ Data Protection Officer (DPO) - Lezione sul Responsabile della protezione dei dati: analisi dell'obbligatorietà delle designazioni del DPO</p> |
| Materiali di studio | <p>· MATERIALI DIDATTICI A CURA DEL DOCENTE</p> <p>Il materiale didattico presente in piattaforma è suddiviso in due macroaree suddivise rispettivamente i moduli per la cybersecurity e n. 24 moduli per la protezione dei dati personali. Essi ricoprono interamente il programma e ciascuno di essi contiene dispense, slide e videolezioni. Tale materiale contiene tutti gli elementi necessari per affrontare lo studio della materia.</p> <p>Testi consigliati: F. Di Resta, Privacy, Data Protection, Cybersecurity e Artificial Intelligence – Aggiornato con l'analisi della nuova normativa sul whistleblowing, ed. Duepuntozero, giugno 2024. F. Di Resta, Privacy, protezione dei dati e Cybersecurity, ed. Duepuntozero, 2021. I.Corradini e F. Di Resta, Cybersecurity, Digital Forensics e Data Protection, ed. Themis, 2021.</p> |
| Modalità di verifica dell'apprendimento | <p>L'esame consisterà nello svolgimento di una prova scritta e/o nel sostenimento di una orale (modalità di verifica che può essere svolta presso la sede centrale di Roma) tendente ad accertare le capacità di analisi, la proprietà di linguaggio e la capacità di rielaborazione dei concetti acquisiti.</p> <p>La prova scritta prevede 3 domande a risposta multipla e 3 aperte (di natura teorica e/o applicativa) che riguardano l'intero programma dell'insegnamento. Alle 3 domande a risposta multipla relative ai contenuti del programma d'esame viene attribuito il valore di 2 punti per risposta corretta; alle 3 aperte viene assegnato un punteggio massimo pari a 8 punti in base alla verifica dei docenti sui risultati di apprendimento attesi. In alternativa.</p> <p>La prova orale consiste in un colloquio teso ad accertare il livello di preparazione dello studente. Quest'ultimo normalmente si snoda in 3 domande (di natura teorica e/o applicativa) che riguardano l'intero programma dell'insegnamento.</p> <p>In ambedue le modalità d'esame, particolare attenzione nella valutazione delle risposte viene data alla capacità dello studente di rielaborare, applicare e presentare con proprietà di linguaggio il materiale presente in piattaforma.</p> |
| Criteri per l'assegnazione dell'elaborato finale | <p>L'assegnazione dell'elaborato finale avverrà sulla base di un colloquio con il docente in cui lo studente manifesterà i propri specifici interessi in relazione a qualche argomento che intende approfondire; non esistono preclusioni alla richiesta di assegnazione della tesi e non è prevista una media particolare per poterla richiedere.</p> |
| Erasmus | <p>Erasmus students shall read the attached programme. Students intentioned to discuss a dissertation on this subject matter are invited to send an email to the professor in order to evaluate specific interests with him and in order to go through the specific topic of the dissertation.</p> |