Insegnamento	Diritto per la sicurezza delle informazioni (Information Security Law)
Livello e corso di studio	Laurea magistrale in Giurisprudenza
Settore scientifico disciplinare (SSD)	IUS/16
Anno di corso	5
Anno Accademico	2021-2022
Numero totale di crediti	5
Propedeuticità	Nessuna. Tuttavia si consiglia approfondire la conoscenza dei concetti fondamentali di Diritto penale e di Diritto processuale penale.
Docente	Isabella Alessandrucci Facoltà: Giurisprudenza Nickname: alessandrucci.isabella Email: isabella.alessandrucci@unicusano.it Orario di ricevimento: la Prof. Isabella Alessandrucci riceve gli studenti nei giorni di esame dopo aver concluso il medesimo, previa richiesta dello studente inoltrata alla docente in piattaforma. Consultare gli Avvisi del Corso.
Presentazione	Il corso di Diritto per la sicurezza delle informazioni (Information Security Law) sviluppa le competenze giuridiche necessarie per affrontare e gestire la rivoluzione digitale in atto nei sistemi organizzativi complessi, sia privatistici che afferenti alla pubblica amministrazione. Il Corso si rivolge a tutti gli studenti di giurisprudenza che intendono specializzarsi nella transizione sia sui processi aziendali che sui modelli organizzativi, imparando ad identificare e gestire gli aspetti giuridici attinenti alla sicurezza delle informazioni, alla cybersecurity, alla data quality e alla data governance e la loro valenza probatoria endoprocessuale. Il Corso affronta i temi afferenti la Data Protection, l'Internet of Things, la privacy nel Cloud Computing, Big Data & Analytics, Machine Learning in ottica giuridica. Le *E-tivity* associate al corso sviluppano le competenze e le abilità necessarie ad affrontare le questioni afferenti alla transizione digitale.
Obiettivi formativi	Il corso di Diritto per la sicurezza delle informazioni (Information Security Law) ha l'obiettivo di illustrare allo studente: 1. la protezione dei dati personali nei sistemi informativi e documentali 2. la sicurezza delle infrastrutture strategiche (Direttiva NIS - Network and Information Security, Perimetro di sicurezza nazionale, Golden Power) 3. il valore probatorio dei documenti digitali e l'acquisizione della digital evidence (Digital Forensic - ISO/IEC 27037) 4. Modelli organizzativi 231 e Best Practices (ISO/IEC 27001, ISO/IEC 27018, ISO/IEC 27701) 5. i profili giuridici della trasformazione digitale collegata alla IoT, AI, Blockchain, Big Data
Prerequisiti	Prima del sostenimento dell'insegnamento a scelta si consiglia di approfondire la **conoscenza** dei concetti fondamentali di **Diritto penale** e di **Diritto processuale penale**. Al riguardo, si consiglia di rivedere tali nozioni, estremamente utili per l'apprendimento e l'approfondimento degli sviluppi del Diritto per la sicurezza delle informazioni (Information Security Law).
Risultati di apprendimento attesi	**Conoscenza e capacità di comprensione** Lo studente al termine del corso avrà conseguito la conoscenza delle nozioni fondamentali di Diritto per la sicurezza delle informazioni (Information Security Law) e, in particolare, degli argomenti indicati analiticamente nei Contenuti del corso. **Applicazione della conoscenza** Lo studente sarà in grado di utilizzare nozioni e istituti afferenti il Diritto per la sicurezza delle informazioni

	(Information Security Law) per analizzare e comprendere lo sviluppo giurisprudenziale e dottrinale insiti nei casi pratici proposti nelle e-tivity. **Autonomia di giudizio** Il corso si prefigge l'obbiettivo di fornisce conoscenze approfondite di Diritto per la sicurezza delle informazioni (Information Security Law) conferendo, allo studente, autonomia di giudizio ed abilità comunicative sugli argomenti proposti. **Abilità comunicative** Il corso consente l'acquisizione della padronanza di un linguaggio tecnico e di una terminologia specialistica adeguati nonché lo sviluppo di abilità comunicative, sia orali che scritte. **Capacità di apprendere** L'apprendimento delle nozioni e degli istituti fondamentali di Diritto per la sicurezza delle informazioni (Information Security Law) consentiranno allo studente di affrontare l'analisi e di esprimere un giudizio maturo sull'insegnamento giuridico.
Organizzazione dell'insegnamento	Il corso di **Diritto per la sicurezza delle informazioni (Information Security Law)** è sviluppato secondo una didattica erogativa e una didattica interattiva. La didattica erogativa (DE) comprende **lezioni audio-video preregistrate del docente** disponibili nella piattaforma, che illustrano i contenuti del corso e che sono integrati da slide e dispense. La **didattica interattiva** (DI) è svolta *online* e comprende: - **messaggi *email*** in cui gli studenti interagiscono con il docente e/o tutor; - **test di autovalutazione** di tipo asincrono che corredano le lezioni preregistrate e consentono agli studenti di accertare la comprensione e il grado di conoscenza acquisita dei contenuti di ciascuna lezione; - il ***forum*** della **"classe virtuale"** che costituisce uno spazio di discussione asincrono nel quale i docenti e/o i tutor individuano le ***e-tivity***, consistenti in casi giurisprudenziali da esaminare al fine di applicare le nozioni teoriche fornite, nelle quali gli studenti interagiscono fra loro e con i docenti e/o tutor, ricevendo riscontri e valutazioni formative. L'insegnamento di **Diritto per la sicurezza delle informazioni (Information Security Law)**, che consta di 5 CFU (Crediti Formativi Universitari), prevede un carico totale di studio di almeno **125 ore** così suddivise: • circa **105 ore** per la visualizzazione delle lezioni preregistrate e lo studio degli argomenti oggetto delle lezioni medesime; • circa **20 ore** di didattica interattiva, di cui 5 ore dedicate a **2 *e-tivity***. Si consiglia di distribuire lo studio della materia uniformemente in un periodo di 6 settimane, dedicando circa 20 ore di studio a settimana.
Contenuti del corso	L'insegnamento di Diritto per la sicurezza delle informazioni (Information Security Law) è articolato in **15 Lezioni** ed è suddiviso in **5 Moduli**: **Lezione introduttiva** (1 lezione di teoria videoregistrata per un impegno di 7 ore + 1 ora di didattica interattiva – Settimana 1) **Modulo 1** – Durante il primo Modulo si acquisisce conoscenza teorica e pratica della normativa in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679 (General Data Protection Regulation - GDPR), del Codice Privacy (D.Lgs. 196/2013 come modificato dal D.Lgs. 101/2018) e dei provvedimenti emanati, nel tempo, dall'Autorità Garante e dall'European Data Protection Board (EDPB - Comitato europeo per la protezione dei dati). Verranno analizzati le implicazioni attinenti al principio di Accountability, di Privacy by Design e di Privacy by Default, nonché quelle afferenti alla mappatura dei trattamenti e all'identificazione di un possibile modello organizzativo che identifichi Titolari, Responsabili e Autorizzati al trattamento dei dati personali con le relative responsabilità. Infine, verranno affrontati i temi legati alla selezione ed al grado di rilevanza delle Misure di sicurezza per la protezione dei dati personali. 2 lezioni di teoria videoregistrata per un impegno di 14 ore + 1 ora di didattica interattiva – Settimana 1 **Modulo 2** – Il secondo Modulo è finalizzato all'esame e alla comprensione del quadro normativo volto alla

	realizzazione di un unico mercato digitale volto ad assicurare un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione. Verranno analizzate la normativa che disciplina l'identificazione del perimetro di sicurezza delle infrastrutture strategiche nazionali e le sue ripercussioni applicative: dalla Direttiva NIS (Direttiva (UE) 2016/1148), recepita con D.Lgs. n. 65/2018, sino al Decreto-legge n. 105/2019 ed al provvedimento relativo al Golden Power nonché al Regolamento (UE) 2019/881 (c.d. Cybersecurity Act). 6 lezioni di teoria videoregistrate per un impegno di 42 ore + 4 ore di didattica interattiva – Settimana 2 **Modulo 3** – Nel corso del terzo Modulo saranno affrontate le tematiche legate alla valenza probatoria della digital evidence raccolta durante le indagini. Si approfondiranno le tecniche di digital forensic necessarie per assicurare l'integrità, l'autenticità e non ripudiabilità delle prove digitali e volte a garantire la catena di conservazione del reperto digitale nel rispetto di quanto richiesto dalla legge 48/2008 e dagli standard di settore (ISO/IEC 27037:2012). Verranno affrontate anche le relative conseguenze sanzionatorie processuali nel caso di mancato rispetto delle regole di garanzia in sede di acquisizione della prova digitale 2 lezioni di teoria videoregistrate per un impegno di 14 ore + 2 ore di didattica interattiva – Settimana 3 **Modulo 4** – L'adozione volontaria di alcuni standard di riferimenti (ISO/IEC 27001:2013 concernente la sicurezza delle informazioni; ISO/IEC 27018:2019 relativa alla privacy nel cloud quale "Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors") garantiscono la conformità normativa agli obblighi imposti. In particolare, nel quarto Modulo saranno esaminate le possibili misure di mitigazione volte a ridurre i rischi di perdita di disponibilità, riservatezza ed integrità delle informazioni digitali e non cui l'azienda o l'ente possono essere esposti. Parimenti l'adozione di un Modello Organizzativo di gestione e controllo ex D. Lgs. 231 costituisce lo strumento di conformità normativa 2 lezioni di teoria videoregistrate per un impegno di 14 ore + 2 ore di didattica interattiva – Settimana 4 Etivity 1 – Analisi di un caso giurisprudenziale e discussione dei princìpi di diritto ricavabili (8 ore – Settimana 5) **Modulo 5** – La società moderna si basa in gran parte su un continuo scambio di dati. Durante questo Modulo saranno esaminate le implicazioni connesse a tale crescita di dati, alla possibilità di acquisirli, conservarli ed incrociarli per scopi di analisi profilata e predittiva con l'incremento dei big data e delle nuove tecnologie legate all'Intelligenza Artificiale, all'Internet delle Cose e al Blockchain. 2 lezioni di teoria videoregistrate per un impegno di 14 ore + 2 ore di didattica interattiva – Settimana 6 Etivity 2 – Analisi di un caso giurisprudenziale e discussione dei princìpi di diritto ricavabili (2 ore – Settimana 6)
Materiali di studio	Il materiale didattico presente in piattaforma è suddiviso in 5 moduli. Essi ricoprono interamente il programma e ciascuno di essi contiene dispense, slide e videolezioni in cui il docente commenta le slide. Tale materiale contiene tutti gli elementi necessari per affrontare lo studio della materia. Testi consigliati, oltre ai materiali didattici presenti in piattaforma: a) G. Ziccardi e P. Pirri, Tecnologia e Diritto – Informatica Giuridica Avanzata - Volume III – Giuffrè, 2019 Per lo studio della materia è indispensabile l'utilizzo delle fonti normative richiamate.
Modalità di verifica dell'apprendimento	L'esame consiste nello svolgimento di una **prova scritta o orale** entrambe tendenti ad accertare la conoscenza e la capacità di comprensione delle nozioni, delle categorie e degli istituti fondamentali di Diritto per la sicurezza delle informazioni (Information Security Law), come analiticamente individuati nei Contenuti dell'insegnamento. La prova **orale** consiste in un colloquio con almeno 3 domande con il docente e i collaboratori di Cattedra tendente ad appurare la maturità di preparazione dello studente. La prova **scritta** prevede 3 quiz a risposta multipla e 3 domande aperte. In entrambi i casi costituiscono oggetto dell'esame finale di profitto anche gli argomenti delle **2 *e-tivity***: saranno dedicate a questi i 3 quiz a risposta multipla e 1 delle domande del colloquio orale. Saranno verificate nelle sessioni di esame di settembre-ottobre le *e-tivity* inserite nel precedente bimestre luglio-agosto, e dunque nelle sessioni di novembre-dicembre quelle inserite nel bimestre settembre-ottobre, di gennaio-febbraio quelle inserite nel bimestre novembre-dicembre, di marzo-aprile quelle inserite nel bimestre gennaio-febbraio, di maggio-giugno quelle inserite nel bimestre marzo-aprile, di luglio quelle inserite nel bimestre maggio-giugno.
Criteri per l'assegnazione	L'assegnazione della tesi di laurea potrà avvenire solo dopo che lo studente avrà sostenuto l'esame di profitto della materia con votazione. Lo studente al momento della richiesta di assegnazione della tesi dovrà indicare

dell'elaborato finale	motivatamente almeno due argomenti su cui sviluppare la tesi. Il docente assegnerà il titolo in relazione alla preferenza manifestata dallo studente, alla difficoltà del tema e ai tempi necessari per svilupparlo che, comunque, per il grado di profondità di ricerca richiesto, impegnerà lo studente per non meno di sei mesi effettivi di lavoro.