Cybersecurity (2024)

Il corso

Codice corso: 29389
Classe di laurea: LM-66
Durata: 2 anni
Lingua: ENG
Modalità di erogazione:
Dipartimento: INFORMATICA

Presentazione

Il corso di studio in Cybersecurity si caratterizza per un’offerta didattica interdisciplinare che raccoglie contributi dell’informatica, dell’ingegneria, della statistica, delle scienze giuridico?economiche e organizzative, insieme a conoscenze specifiche dei principali domini applicativi di protezione contro i cyber-attacchi. In particolare, la laurea magistrale in Cybersecurity offre le conoscenze professionali adeguate, sia dal punto di vista tecnologico che normativo, per supervisionare e coordinare le politiche di sicurezza nell’ambito di complessi sistemi informatici, organizzare la protezione da cyber-attacchi, e gestire il recupero in caso di attacco avvenuto con successo.

Percorso formativo

Curriculum unico

1º anno

Insegnamento	Semestre	CFU	Lingua
1047622 | CRYPTOGRAPHY	1º	6	ENG

Obiettivi formativi

Obiettivi Generali
Lo scopo dell'insegnamento è quello di insegnare i fondamenti della crittografia, che è la componente principale per la sicurezza nelle applicazioni digitali odierne.

Obiettivi Specifici
Gli studenti impareranno la metodologia della sicurezza dimostrabile, che permette di dimostrare la sicurezza dei moderni crittosistemi in senso matematico.

Conoscenza e Comprensione
-) Conoscenza dei fondamenti matematici della crittografia moderna.
-) Conoscenza delle principali assunzioni crittografiche, su cui si basa la sicurezza dei moderni crittosistemi.
-) Conoscenza degli schemi crittografici usati nella vita reale. Comprensione delle loro proprietà (teoriche e pratiche).

Applicazione di Conoscenza e Comprensione
-) Come selezionare la giusta primitiva crittografica per una data applicazione.
-) Come analizzare la sicurezza di un dato crittosistema.

Autonomia di Giudizio
Gli studenti saranno in grado di giudicare se una data primitiva crittografica è sicura oppure no.

Abilità Comunicative
Come descrivere la sicurezza di una costruzione crittografica nel linguaggio della sicurezza dimostrabile.

Capacità di Apprendimento Successivo
Gli studenti interessati alla ricerca verranno a conoscenza di alcuni problemi aperti nell'area, ed otterranno le basi necessarie per studi più approfonditi in materia.

1027171 | NETWORK INFRASTRUCTURES	1º	6	ENG

Obiettivi formativi

?Il corso presenta i concetti di base, i protocolli e le architetture delle attuali infrastrutture di rete. Particolare attenzione è dedicata alla rete di accesso a banda larga, alla rete di trasporto ottica e alle reti wireless di nuova generazione. Inoltre, vengono descritte le principali tecnologie per il supporto della Qualità di Servizio in una infrastruttura di rete.

Risultati di apprendimento attesi
Alla fine del corso gli studenti avranno conoscenze sulle principali tecnologie ed infrastrutture di reti di comunicazioni tra cui: xDSL, PON, LTE, 5G, SDH, OTN, SDN. Inoltre saranno in grado di configurare ed analizzare reti IP e relativi protocolli grazie alle conoscenze acquisite utilizzando il tool Netkit. Specifici progetti svolti durante il corso permetteranno agli studenti di applicare le conoscenze acquisite a scenari e applicazioni di rete innovativi.

1022807 | DISTRIBUTED SYSTEMS	1º	6	ENG

Insegnamento	Semestre	CFU	Lingua

Obiettivi formativi

I sistemi distribuiti sono alla base di qualiasi applicazione informatica moderna. Il corso si propone di fornire agli studenti una chiara caratterizzazione della concorrenza in un sistema distribuito considerando le caratteristiche di tale sistema come guasti, latenza variabile nelle comunicazioni e assenza di un riferimento temporale globale. Successivamente si analizzeranno i principali modelli di sistema e le astrazioni di base per la comunicazione e la sincronizzazione. Infine si forniranno i concetti legati al consenso distribuito ed ai sistemi di tipo distributed ledger.

Risultati di apprendimento attesi
Lo studente sarà in grado di progettare sistemi e algoritmi distribuiti al di sopra di diversi modelli di sistema (sincrono, asincrono e parzialmente sincrono) capendo impossibilità e limitazioni nelle prestazioni. Inoltre avrà la capacita di analizzare sistemi e piattaforme reali attraverso modelli astratti più facili da trattare.

1055043 | STATISTICS	1º	6	ENG

Obiettivi formativi

Il corso prevede argomenti e temi di utilità e rilevanza specifica per la Cybersecurity. Fa massivo utilizzo di attività pratiche di programmazione in classe al computer, con linguaggi ad oggetti e IDE di ultima generazione, e con implementazione di algoritmi statistici, metodi Monte Carlo e simulazioni statistiche.
Prevede, inoltre, attività di ricerca individuale e creazione di blog online personali, contenenti ricerche e approfondimenti sui temi affrontati a lezione.

Conoscenza e Comprensione
Comprendere i concetti statistici fondamentali tra cui il campionamento, la sperimentazione, la variabilità, distribuzione, l'associazione, la causalità, le tecniche di stima puntale e intervallare, i test di ipotesi e il concetto
di significatività. Esaminare e analizzare argomenti statistici e apprezzare la rilevanza e l'importanza delle statistiche.

Applicazione della conoscenza e comprensione
Lo studente acquisirà le seguenti competenze: raccolta, organizzazione e interpretazione di dati numerici; interpretare e comunicare i risultati di un'analisi statistica. Comprendere e prendere decisioni informate basate sull'analisi quantitativa.

A SCELTA DELLO STUDENTE	1º	12	ITA
1055055 | CYBER AND COMPUTER LAW	2º	6	ENG

Obiettivi formativi

Obiettivi
L’obiettivo del corso è quello di approfondire i principali temi di regolazione giuridica delle attività informatiche, nelle imprese e nella pubblica amministrazione, con riferimento ai temi della sicurezza informatica e del Cybercrime, della regolamentazione europea sulla elaborazione e del trattamento dei dati personali e sul commercio elettronico e proprietà intellettuale in materia informatica. Si presenteranno anche gli strumenti giuridici, protocolli e standard della cooperazione europea nel contrasto al cybercrime. Il corso è strutturato in moduli di approfondimento anche con esame di casi pratici.

Conoscenza e comprensione
Al termine del corso lo studente è in grado di identificare e di sviluppare le principali conoscenze giuridiche in materia di elaborazione dati e quindi di operare efficacemente nell'ambito di amministrazioni pubbliche nel rapporto con uffici giudiziari o di polizia. Inoltre è in grado di partecipare efficacemente a gruppi di lavoro o squadre investigative comuni avendo chiare le indispensabili nozioni e responsabilità giuridiche. Il corso consente di raccordare competenze tecnologiche informatiche e competenze organizzative economiche e giuridiche riguardanti l’uso dell’informatica o di strumenti informatici in ambito aziendale e pubblico.

Capacità di applicare conoscenza e comprensione
Per la realizzazione degli obiettivi formativi le attività didattiche si articolano in moduli di approfondimento tematico, per la definizione e l’intervento in specifici contesti o in particolari situazioni di rischio o di emergenza e per comprendere le esigenze degli operatori, saranno previste inoltre iniziative comuni con altri corsi di studio sui temi della sicurezza, della resilienza e della metodologia di acquisizione di tracce e prove di reati informatici anche in ambiente internazionale.

Insegnamento	Semestre	CFU	Lingua
1055682 | ETHICAL HACKING	2º	9	ENG

Obiettivi formativi

Obiettivi generali
Gli hacker etici sono una categoria di professionisti sempre più richiesta da aziende e governi consapevoli della necessità di proteggere efficacemente le proprie infrastrutture da possibili cyberattacks. Il corso affronta i fondamenti dell'hacking etico. In particolare, si parte dallo studio sistematico delle metodologie e degli strumenti utilizzati dagli hacker per eseguire i vari attacchi nel cyberspace. Successivamente, si illustra come il professionista di hacking etico possa svolgere una serie di attività lecite e utili sottoponendo i sistemi informatici a test di vulnerabilità. Tali test hanno il fine di valutare e comprovare la cybersecurity di una organizzazione e di aiutare i proprietari e i dirigenti a prendere coscienza e risolvere i loro problemi di cybersecurity. Particolare attenzione viene dedicata all'applicazione pratica delle nozioni apprese.

Obiettivi specifici
Il corso spiega in dettaglio cosa fanno gli hacker, come le attività di hacking avvengono, come gli hacker riescono abusivamente ad introdursi in un sistema informatico protetto da misure di sicurezza, e come difendersi.

Conoscenza e comprensione
Comprendere i concetti e i limiti dell'hacking etico. Tali concetti includono:
Casing the Establishment: le tecniche di hacking utilizzate per l'enumerazione completa del sistema target.
Endpoint e Server Hacking: gli obiettivi finali di qualsiasi hacker inclusi gli Advanced Persistent Threat.
Hacking delle infrastrutture: il modo in cui gli hacker attaccano gli apparati ai quali si collegano i nostri sistemi.
Application e Data Hacking: attacchi ai web/database e le tecniche di mobile hacking.
Le contromisure che possono essere utilizzate per ostacolare le attività degli hacker sui sottosistemi considerati. Standard di esecuzione dei test di penetrazione.

Applicazione di conoscenza e comprensione
Alla fine del corso, gli studenti avranno la capacità di analizzare sistemi informativi aziendali complessi ed ottenere una migliore comprensione delle vulnerabilità dell'organizzazione. Produrre report in modo da fornire il massimo valore ai dirigenti dell'organizzazione di destinazione.

Capacità di giudizio
Gli studenti svilupperanno le capacità di inquadrare le attività di hacking etico in modo da non violare la normativa vigente. Capacità di seguire un codice di condotta etico e di offrire garanzie sulle buone intenzioni nel condurre le attività di penetration testing dei sistemi.

Capacità comunicative
Gli studenti impareranno a documentare le loro scelte, anche attraverso l'uso di strumenti di generazione di rapporti automatizzati. Avranno anche acquisito la capacità di preparare presentazioni relative ad argomenti scientifici.

Capacità di proseguire l'apprendimento in modo autonomo
Le nozioni acquisite durante il corso forniranno agli studenti una solida base di conoscenza per poter ulteriormente approfondire gli aspetti più tecnici, e per mantenersi autonomamente informati sui continui sviluppi e aggiornamenti del hacking etico.

Group C

2º anno

Insegnamento	Semestre	CFU	Lingua
1055681 | MALWARE ANALYSIS AND INCIDENT FORENSICS	1º	9	ENG

Insegnamento	Semestre	CFU	Lingua

Obiettivi formativi

Gli odierni scenari legati alla cyber security ci testimoniano la sempre più pervasiva presenza di software malevolo utilizzato per perpetrare attacchi informatici. Il corso si propone di fornire agli studenti le conoscenze, i metodi e gli strumenti di base per analizzare, identificare, categorizzare e comprendere il comportamento dei software malevoli. Il corso adotterà un approccio pratico, con una importante componente di applicazione a casi reali.

Risultati di apprendimento attesi
Lo studente sarà in grado di analizzare sia in modo manuale, che tramite l'uso di strumenti automatizzati software malevolo di diversa natura per identificarne tutte le caratteristiche salienti. Sarà in grado di estrarne queste caratteristiche e relazionarle con basi di conoscenza esistenti. Infine, lo studente sarà in grado di contestualizzare queste attività nell'ambito di un processo complessivo di threat intelligence e gestione degli incidenti causati da tali software malevoli.

1055061 | SECURITY GOVERNANCE	1º	6	ENG

Obiettivi formativi

Obiettivi Generali

Essere in grado di analizzare e progettare processi per la gestione della sicurezza cibernetica.

- Conoscenza e comprensione

L’obiettivo principale dell'insegnamento è di fornire un’introduzione a tutte le tematiche relative alla gestione della cybersecurity. In particolare, verrà mostrato allo studente come il problema della cybersecurity sia verticale rispetto all'organizzazione aziendale e che per tanto la sua gestione ne impatta diversi livelli.
Verranno analizzati aspetti legati alle normative, ai regolamenti e agli standard sia Internazionali che Nazionali. Verrà poi discusso come, dal punto di vista metodologico, questi aspetti vengano recepiti e messi in atto attraverso la definizione di appositi framework per la gestione della cybersecurity.

- Applicare conoscenza e comprensione

Un altro aspetto fondamentale del corso sarà quello di fornire allo studente metodologie e strumenti per poter affrontare problemi aperti rispetto all'analisi, verifica e certificazione della cybersecurity.

- Capacità critiche e di giudizio

Lo studente acquisirà gli strumenti necessari per poter analizzare, valutare e comparare diverse situazioni e progettare le opportune contromisure per migliorare lo stato di sicurezza della realtà analizzata.

- Capacità comunicative

Lo studente apprenderà il linguaggio specifico del settore.

- Capacità di apprendimento

Lo studente sarà in grado di far proprie e riapplicare tutte le metodologie discusse durante il corso

AAF1803 | CYBER SECURITY SEMINARS	2º	6	ENG

Obiettivi formativi

Le organizzazioni oggi si trovano ad affrontare una crescente sofisticazione e persistenza degli attacchi informatici - da governi stranieri, dalla criminalità organizzata, dagli hacktivisti e dagli insider dall'interno dell'organizzazione.
L'obiettivo del corso è descrivere le principali sfide critiche per la protezione dei sistemi e delle risorse informative - informazioni finanziarie, dati dei clienti, proprietà intellettuale - e le implicazioni di non riuscire a farlo.

AAF1028 | PROVA FINALE	2º	30	ITA

Insegnamento	Semestre	CFU	Lingua

Obiettivi formativi

La prova finale consiste nella discussione di una tesi di laurea magistrale, costituita da un documento scritto in lingua inglese, che presenta i risultati di uno studio originale condotto su un problema di natura applicativa, sperimentale o di ricerca. La preparazione della tesi si svolge sotto la direzione di un docente nel secondo anno del corso.

La prova finale permette di valutare la capacità di applicare le conoscenze apprese a un problema specifico, la capacità di prendere decisioni autonome e di comunicare gli aspetti metodologici e tecnici del lavoro svolto.

Group C

Gruppi opzionali

Lo studente deve acquisire 18 CFU fra i seguenti esami

Insegnamento	Anno	Semestre	CFU	Lingua
1041792 | BIOMETRIC SYSTEMS	1º	1º	6	ENG

Obiettivi formativi

Obiettivi generali:
Essere in grado di progettare e valutare un sistema biometrico o multibiometrico

Obiettivi specifici:
Conoscere le caratteristiche e le tecniche fondamentali relative alle biometrie fisiche come volto, impronte, iride, ecc., e comportamentali come camminata, firma (caratteristiche dinamiche), stile di battitura, ecc. Conoscere le caratteristiche dell'architettura di un sistema biometrico: sistemi unimodali e multimodali. Essere in grado di valutare le prestazioni di un sistema biometrico in base alla modalità adottata: verifica, identificazione. Essere in grado di valutare/garantire la robustezza di un sistema biometrico rispetto ad attacchi di spoofing (furto di identità).

Conoscenza e comprensione:
Fondamenti teorici della progettazione di un sistema biometrico e delle tecniche di estrazione/confronto delle caratteristiche specifiche per i principali tratti biometrici.

Applicare conoscenza e comprensione:
Essere in grado di progettare ed implementare una applicazione di riconoscimento biometrico per almeno uno tratto biometrico.

Capacità critiche e di giudizio:
Essere in grado di valutare le prestazioni e la robustezza agli attacchi di un sistema biometrico. Essere in grado di trasferire tecniche e protocolli in contesti diversi.

Capacità comunicative:
Essere in grado di comunicare/condividere i requisiti di un sistema biometrico, le modalità operative più adatte ad una certa applicazione, e le misure di performance del sistema

Capacità di apprendimento:
Essere in grado di approfondire autonomamente gli argomenti presentati nel corso, relativamente a tecniche e metodi specifici/complessi o a tratti biometrici non presenti tra gli argomenti.

1054960 | Computer systems and programming	1º	1º	6	ENG

Insegnamento	Anno	Semestre	CFU	Lingua

Obiettivi formativi

Obiettivi Generali
Obiettivo del corso è fornire gli strumenti fondamentali della programmazione di sistema.

Obiettivi Specifici
Gli studenti saranno in grado di sviluppare autonomamente del codice in grado di interagire con il sistema operativo e sfruttarne i servizi.

Conoscenza e Comprensione
-) Conoscenza del linguaggio C e dei strumenti normalmente impiegati nell'ambiente di sviluppo (compilatore, preprocessore, debugger, make, etc.)
-) Conoscenza delle funzioni fondamentali del sistema operativo e dei suoi moduli principali (Scheduler, Virtual Memory Manager, Filesystem ..).
-) Conoscenza delle principali primitive di sistema per la creazione la sincronizzazione di processi e thread, lo scambio di messaggi ed informazioni.
-) Conoscenza delle primitive per la programmazione di rete (socket).

Applicazione di Conoscenza e Comprensione
-) Come utilizzare le primitive fornite dal sistema operativo ed integrarle, in modo corretto, nel codice.
-) Come scegliere il componente di SO e le funzioni più adatte, in base alle esigenze delle applicazioni ed alla loro modalità di esecuzione.

Autonomia di Giudizio
Gli studenti saranno in grado di determinare la complessità e la modalità di implementazione di un'applicazione di sistema.

Abilità Comunicative
Descrivere l'interazione di una applicazione con il sistema operativo e spiegare le motivazioni alla base delle scelte.

Capacità di Apprendimento Successivo
Gli studenti interessati potranno proseguire l'apprendimento esaminando, nei suoi dettagli, l'architettura e l'interfaccia di programmazione del sistema operativo.

1047642 | SECURITY IN SOFTWARE APPLICATIONS	1º	1º	6	ENG

Insegnamento	Anno	Semestre	CFU	Lingua

Obiettivi formativi

Obiettivi generali

I fondamenti della sicurezza nei programmi software

Obiettivi specifici

Metodologie e strumenti per trovare e rimuovere le vulnerabilità più comuni del software e per sviluppare software senza falle di sicurezza

Conoscenza e comprensione

conoscenza e capacità di comprensione delle tecniche più efficaci per la rimozione di vulnerabilità dal codice e per sviluppare software che soddisfi specifiche politiche di sicurezza.

Applicare conoscenza e comprensione

Essere in grado di applicare e trasferire la propria conoscenza delle metodologie alla scelta delle tecniche e strumenti appropriati risolvere problemi di sicurezza del software

Autonomia di giudizio

Capacità d'interpretazione autonoma per proporre soluzioni appropriate a problemi di sicurezza software congruenti con le tecnologie disponibili.

Abilità comunicative

Capacità di presentare e di argomentare le proprie scelte in merito alle metodologie ed agli strumenti utilizzati per le soluzioni proposte, sia con colleghi che con utenti

Capacità di apprendimento successivo

Capacità di apprendere e approfondire nuove tecniche nell'ambito della sicurezza software informatica sia degli aspetti metodologici sia di quelli tecnologici

1047623 | DATA AND NETWORK SECURITY	1º	2º	6	ENG

Obiettivi formativi

Lo scopo di Data and Network Security è quello di esporre le problematiche e le soluzioni più aggiornate in un settore come quello della cybersecurity che è in rapida evoluzione.
Gli studenti verranno a conoscenza dei principali problemi aperti di ricerca, ed otterranno le basi necessarie per studi più approfonditi in materia e per tenersi al passo con gli sviluppi nel campo.

1055047 | ECONOMICS OF TECHNOLOGY AND MANAGEMENT	1º	2º	6	ENG

Insegnamento	Anno	Semestre	CFU	Lingua

Obiettivi formativi

Conoscenza e comprensione
Vengono illustrati gli strumenti essenziali per analizzare i processi decisionali delle imprese. In particolare, lo studente comprende le nozioni di base relative:
• all'analisi microeconomica dell'impresa,
• alle forme istituzionali e organizzative delle imprese,
• alle strategie di innovazione tecnologica,
• alla valutazione economico-finanziaria dei progetti di investimento
• al bilancio d'impresa.

Capacità di applicare conoscenza e comprensione
Lo studente è in grado di applicare metodi e modelli di base della microeconomia, della teoria dell'organizzazione e di finanza aziendale al fine di:
• individuare le determinanti delle principali scelte strategiche dell'impresa,
• analizzare l'interazione tra l'evoluzione tecnologica e strutturale dell'industria e le strategie delle imprese,
• valutare la redditività di un progetto di investimento,
• interpretare il bilancio di un'impresa.

Autonomia di giudizio
La combinazione di lezioni teoriche frontali ed esercitazioni pratiche mirate alla discussione e alla soluzione di specifici problemi consente agli studenti di acquisire la capacità di valutare potenzialità e limiti dei modelli teorici ai fini della formulazione delle strategie delle imprese.

Abilità comunicative
Al termine del corso, gli studenti sono in grado di illustrare e spiegare le principali tesi e argomentazioni della microeconomia dell'impresa, della teoria dell'organizzazione e della finanza aziendale a una varietà di interlocutori eterogenei per formazione e ruolo professionale. L'acquisizione di tali capacità viene verificata e valutata in occasione dell'esame finale, mediante la prova scritta e l'eventuale prova orale.

Capacità di apprendimento
Lo studente acquisisce la capacità di condurre in autonomia studi individuali su argomenti specifici di microeconomia, di teoria dell'organizzazione e di finanza aziendale. Durante il corso, lo studente è stimolato ad approfondire argomenti di particolare interesse mediante la consultazione di materiale bibliografico supplementare, quali articoli accademici, libri specialistici e siti internet. L'acquisizione di tali capacità viene verificata e valutata in occasione dell'esame finale (mediante la prova scritta e l'eventuale prova orale), nell'ambito del quale lo studente può essere chiamato ad analizzare e risolvere problemi nuovi sulla base degli argomenti trattati e del materiale di riferimento distribuito durante il corso.

1047634 | INTERNET OF THINGS	1º	2º	6	ENG

Insegnamento	Anno	Semestre	CFU	Lingua

Obiettivi formativi

Obiettivi generali:
Il corso illustra gli aspetti metodologici, teorici e pratici relativi alla progettazione di reti wireless e Internet delle cose. Il corso prevede un laboratorio.

Obiettivi specifici
Introduzione alle reti wireless, architetture e protocolli usati nelle reti cellulari info al 5G e nei sistemi Internet delle cose, analisi delle soluzioni di ricerca relative ad alcune
delle sfide per la realizzazione dei sistemi internet delle cose (abbattimento del consumo energetico, integrazione del mondo IoT e della robotica, sicurezza delle informazioni).

Struttura sintetica del corso
- Introduzione alle reti radio
- Dai sistemi cellulari 2G al 5G
- Protocolli per sensing systems: protocolli di MAC, routing, localizzazione e sincronizzazione
- Verso l'Internet delle cose: caratteristiche e problematiche, protocolli standard e tecnologie, scelte progettuali per diversi ambiti verticali, sfide ancora aperte
- Aspetti avanzati dell'IoT: zero-power IoT; aspetti di sicurezza; uso di blockchain in applicazioni IoT; ottimizzazione di sistemi mediante tecniche di machine learning; integrazione di
robotica e IoT systems (esempio dell'Internet of Underwater Things).
-Lab di programmazione IoT

Conoscenze e comprensione:
Alla fine del corso lo studente saprà leggere e comprendere articoli scientifici, documenti tecnici e standard del settore; avrà compreso i trade-off prestazionali associati a diverse scelte progettuali.
Sarà quindi in grado di progettare futuri sistemi wireless e IoT. Avrà fatto prime esperienze pratiche relative alla programmazione e valutazione sperimentale di tali sistemi.

Applicazione di conoscenza e comprensione:
Gli studenti saranno in grado di partecipare alla progettazione di futuri sistemi e applicazioni IoT e di sistemi 5G.

Capacità di giudizio:
Gli studenti svilupperanno le capacità di analisi necessarie per valutare diverse scelte progettuali alternative selezionando la migliore per ogni specifico scenario applicativo e tipo di tecnologia.

Capacità di comunicazione:
Gli studenti impareranno ad analizzare e presentare articoli scientifici, idee di ricerca o soluzioni tecniche di settore, descrivendole in modo sintetico ed accurato, con un linguaggio tecnico
adeguato.

Capacità di apprendimento:
Gli studenti acquisiranno sia competenze teoriche che pratiche relative alla progettazione dei sistemi wireless e IoT.

10589555 | PRACTICAL NETWORK DEFENSE	1º	2º	6	ENG

Insegnamento	Anno	Semestre	CFU	Lingua

Obiettivi formativi

Obiettivi generali
Il corso affronta i fondamenti delle metodologie e degli strumenti per la protezione delle reti di calcolatori. Particolare attenzione viene dedicata all'applicazione pratica delle nozioni apprese.

Obiettivi specifici
Il corso affronta le relazioni fra i meccanismi di funzionamento delle reti di calcolatori e gli attacchi informatici, i meccanismi per la possibile identificazione e soppressione degli attacchi e la relativa implementazione mediante l'uso di adeguate strategie di progettazione e di strumenti specifici.

Conoscenza e comprensione
Elencare le minacce più ricorrenti dovute all'uso di specifici protocolli all'interno delle reti di elaboratori. Spiegare i meccanismi più utilizzati dagli attaccanti maliziosi e dai progettisti di malware per compromettere la sicurezza di un sistema di elaboratori. Spiegare i meccanismi di base utilizzati per l'identificazione dei tentativi di intrusione negli elaboratori e nelle reti.

Applicazione di conoscenza e comprensione
Alla fine del corso gli studenti saranno in grado di realizzare il monitoraggio del traffico scambiato nelle reti, di applicare una policy di sicurezza, di realizzare una scansione delle stazioni all'interno di una rete di elaboratori e una ricerca delle vulnerabilità di una rete di elaboratori. Gli studenti svilupperanno la capacità di selezionare le regole appropriate per proteggere una rete mediante firewall, selezionare i meccanismi più appropriati per proteggere un sistema di elaboratori collegati tramite rete e di eseguire le scelte di progettazione più opportune per implementare una strategia di "difesa in profondità", usando reti isolate e strumenti dedicati (VPN,proxy e firewall).

Capacità di giudizio
Gli studenti svilupperanno le capacità di analisi necessarie per valutare diverse alternative durante il processo di progettazione di una rete di elaboratori, con particolare riferimento alla valutazione delle scelte architetturali e dei rischi che possono comportare e agli obiettivi di sicurezza che il sistema vuole perseguire.

Capacità comuncative
Gli studenti impareranno a documentare le loro scelte, anche attraverso l'uso di strumenti di generazione di rapporti automatizzati. Avranno anche acquisito la capacità di preparare presentazioni relative ad argomenti scientifici.

Capacità di proseguire l'apprendimento in modo autonomo
Le nozioni acquisite durante il corso forniranno agli studenti una solida base di conoscenza per poter ulteriormente approfondire gli aspetti più tecnici, esplorare le alternative non affrontate per motivi di tempo e per mantenersi autonomamente informati sui continui sviluppi e aggiornamenti della sicurezza informatica applicata alle reti.

1054962 | SECURE COMPUTATION	1º	2º	6	ENG

Insegnamento	Anno	Semestre	CFU	Lingua

Obiettivi formativi

Obiettivi Generali
Lo scopo del corso è quello di fornire una panoramica sulle più avanzate tecniche crittografiche e le loro applicazioni.

Obiettivi Specifici
Gli studenti impareranno il concetto di computazione sicura, che consente ad una rete di giocatori malfidati, ognuno con il proprio input segreto, di eseguire un protocollo distribuito per valutare l'output di una funzione sui propri input in modo sicuro, cioè senza rivelare nulla oltre a quello che l'output della funzione rivela. La computazione sicura è un'astrazione di molte applicazioni importanti, incluso il voto elettronico, le aste digitali, le crittovalute, la conoscenza nulla, etc.

Conoscenza e Comprensione
-) Conoscenza di strumenti crittografici avanzati, incluso la conoscenza nulla, gli impegni digitali, e la cifratura pienamente omomorfa.
-) Conoscenza dei fondamenti della computazione sicura, in particolare come definire la sicurezza dei protocolli interattivi.
-) Comprensione dei principi di funzionamento dei libri mastri distribuiti e delle crittovalute.

Applicazione di Conoscenza e Comprensione
-) Come analizzare la sicurezza dei protocolli interattivi.
-) Come progettare protocolli interattivi sicuri.
-) Come programmare "contratti intelligenti" sicuri.

Autonomia di Giudizio
Gli studenti saranno in grado di valutare il livello di sicurezza delle applicazioni crittografiche avanzate.

Abilità Comunicative
Come descrivere la sicurezza dei protocolli interattivi per il voto digitale, le crittovalute, e la computazione sicura in generale.

Capacità di Apprendimento Successivo
Gli studenti interessati alla ricerca verranno a conoscenza di alcuni problemi aperti nell'area, ed otterranno le basi necessarie per studi più approfonditi in materia.

1054963 | SYSTEMS AND CONTROL METHODS FOR CYBER-PHYSICAL SECURITY	1º	2º	6	ENG

Insegnamento	Anno	Semestre	CFU	Lingua

Obiettivi formativi

Obiettivi generali
Il corso si propone di fornire concetti e metodologie di base della teoria del controllo, della ricerca operativa e della teoria dei giochi, che costituiscono un quadro analitico per la modellizzazione dei sistemi cyber-fisici e dei principali tipi di attacchi ai sistemi cyber-fisici (ad esempio: "denial of service", "replay attack", "covert attack", "false data injection") e per la soluzione di giochi di sicurezza e problemi decisionali. Il corso riassumerà un certo numero di tali metodologie e mostrerà come la loro applicazione sia in grado di affrontare i problemi di cybersecurity in numerosi casi d'uso di esempio.

Obiettivi specifici

Conoscenza e comprensione:
Gli studenti apprenderanno metodologie per modellare e risolvere i problemi di sicurezza nei sistemi ciber-fisici attraverso la teoria del controllo, la teoria dei giochi e le metodologie di ricerca operativa.

Applicare conoscenza e comprensione:
Al termine del corso, lo studente sarà in grado di ricavare modelli matematici astratti per un'ampia classe di sistemi ciber-fisici e per analizzare, a partire da questi modelli, alcune importanti proprietà riguardanti la sicurezza.

Capacità critiche e di giudizio:
Lo studente sarà in grado di affrontare i problemi della cybersecurity attraverso la teoria del controllo, la teoria dei giochi e le metodologie di ricerca operativa.

Abilità comunicative:
Le attività del corso consentono allo studente di essere in grado di comunicare / condividere i principali problemi relativi ai problemi di cybersecurity nei sistemi ciber-fisici e le possibili scelte progettuali per la loro soluzione.

Capacità di apprendimento:
L'obiettivo del corso è quello di sensibilizzare gli studenti su come affrontare i problemi di controllo e decisionali nel contesto dei problemi di sicurezza informatica nei sistemi ciber-fisici.

1044415 | MOBILE APPLICATIONS AND CLOUD COMPUTING	2º	1º	6	ENG

Insegnamento	Anno	Semestre	CFU	Lingua

Obiettivi formativi

Conoscenza e capacità di comprensione.
Il corso mira a fornire le conoscenze necessarie per la comprensione: (i) delle specificità delle applicazioni per dispositivi mobili (app mobili) rispetto a applicazioni desktop; (ii) dei principali pattern di progettazione per le app mobili; (iii) le principali problematiche legate alla sicurezza; (iv) dell'utilizzo dei principali servizi cloud di backend per applicazioni mobili; (v) delle metodologie di progettazione e sviluppo di semplici servizi di backend dispiegati su cloud; (vi) della classificazione dei modelli di servizio cloud

Capacità di applicare conoscenza e comprensione.
Lo studente dovrà essere in grado di progettare, sviluppare e testare applicazioni native per sistemi operativi android che interagiscano con servizi cloud usando i principali strumenti di sviluppo, test e progettazione ufficiali. Lo studente dovrà essere inoltre in grado di progettare/sviluppare e testare propri semplici servizi dispiegati su piattaforme cloud, di supporto alle applicazioni mobili

Autonomia di giudizio.
In base alle competenze acquisite, lo studente dovrà essere in grado di valutare i vantaggi e gli svantaggi delle tecnologie con cui è possibile sviluppare app (applicazioni native, ibride e web based), valutare/scegliere in modo ottimale e critico le funzionalità di supporto cloud per il funzionamento di applicazioni mobili; giudicare la fattibilità, complessità e le implicazioni di nuove possibili applicazioni, anche indicate da terzi. Inoltre, dovrà essere in grado di aggiornarsi autonomamente in base alle possibili future tecnologie relative ad app mobili o servizi cloud.

Abilità comunicative.
Lo studente dovrà essere in grado di motivare le scelte tecnologiche, metodologiche ed architetturali ad altre persone del settore, nonché di presentare, anche a persone non esperte, il funzionamento e le caratteristiche di possibili nuove applicazioni

Capacità di apprendimento.
Per stimolare la capacità di apprendimento verranno effettuati esercitazioni pratiche sui diversi argomenti trattati e verrà richiesto di usare criticamente informazioni disponibili per specifici problemi su varie piattaforme di discussione (es. Stack Overflow, siti ufficiali, blog, etc.)

1055050 | RISK MANAGEMENT	2º	1º	6	ENG

Insegnamento	Anno	Semestre	CFU	Lingua

Obiettivi formativi

Obiettivi generali
Il corso affronta la valutazione dei rischi cyber che possono danneggiare un Sistema informativo aziendale, le metodologie per mitigare tali rischi e le necessarie contromisure da applicare con l'obiettivo di rendere sicura l'azienda o istituzione pubblica dal punto di vista informatico.

Obiettivi specifici
Il corso affronta le relazioni fra i meccanismi di funzionamento dei sistemi informativi e delle reti di calcolatori e le minacce informatiche cui possono essere soggetti, i meccanismi per la identificazione e contrasto degli attacchi e la relativa implementazione mediante l'applicazione di specifiche contromisure per ridurre il rischio cyber. Particolare attenzione viene dedicata all'applicazione pratica delle nozioni apprese attraverso l'analisi di casi di studio e esercitazioni. Il riferimento di base per l'insegnamento di Risk Management e' lo standard ISO 27005, complementato dal NIST SP 800-30 framework.

Conoscenza e comprensione
Analizzare le minacce più ricorrenti e pericolose, mettendole in relazione con le vulnerabilitá dei sistemi e delle reti su cui le minacce possono generare un impatto. Valutare i rischi aziendali conseguenti a tale impatto e raccomandare l'attuazione di relative contromisure; in alternativa, suggerire i criteri per la accettazione dei rischi in tal modo individuati. Spiegare i meccanismi di base utilizzati per l'identificazione dei tentativi di intrusione negli elaboratori e nelle reti. Determinare e stabilire i processi di miglioramento continuo.

Applicazione di conoscenza e comprensione
Alla fine del corso gli studenti saranno in grado di identificare e valutare i rischi che possono influenzare il funzionamento e la sicurezza di un sistema informativo e i relativi impatti. Sulla base delle metodologie di analisi e gestione dei rischi apprese nel corso, gli studenti svilupperanno la capacità di identificare e selezionare le contromisure appropriate per proteggere il sistema informativo, sotto il punto di vista sia tecnico che amministrativo, determinando il miglior profilo di governance del processo della sicurezza.

Capacità di giudizio
Gli studenti svilupperanno le capacità di analisi necessarie per valutare diverse alternative durante il processo di identificazione dei rischi di sicurezza di un Sistema informativo, con particolare riferimento alla valutazione delle scelte architetturali e dei rischi che possono comportare e agli obiettivi di sicurezza imposti al sistema in relazione al livello di sensibilità delle informazioni da esso gestite.

Capacità comunicative
Gli studenti impareranno a documentare le loro scelte, anche attraverso l'uso di strumenti di generazione di rapporti automatizzati. Avranno anche acquisito la capacità di preparare presentazioni relative ad argomenti legati alla sicurezza.

Capacità di proseguire l'apprendimento in modo autonomo
Le nozioni acquisite durante il corso forniranno agli studenti una base di conoscenza per poter ulteriormente approfondire gli aspetti più tecnici, e per mantenersi autonomamente informati sui continui sviluppi e aggiornamenti della valutazione dei rischi di sicurezza informatica dei sistemi e delle reti.

10600490 | BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGIES	2º	1º	6	ITA

Insegnamento	Anno	Semestre	CFU	Lingua

Obiettivi formativi

Obiettivi generali:
Le blockchain costituiscono un paradigma nuovo e rivoluzionario per la gestione distribuita dei sistemi transazionali. Una blockchain è un protocollo per la gestione di ledger distribuiti, ossia per la memorizzazione decentralizzata di una sequenza di transazioni (ledger) a prova di manomissione, mantenuta e verificata dai nodi che partecipano alla rete. Una combinazione di reti peer-to-peer, consenso automatico, crittografia e meccanismi di mercato è al centro delle blockchain, che garantiscono così l'integrità e la trasparenza dei dati. Un numero crescente di piattaforme blockchain fornisce il supporto per i cosiddetti smart contract, ossia codice eseguibile che esprime come condurre attività di business tra le parti contraenti (ad esempio, trasferire beni digitali se una condizione è soddisfatta). La progettazione di un'applicazione sicura, verificabile ed efficiente basata su blockchain richiede la capacità di architettare correttamente le strutture comportamentali tra le parti coinvolte. Il corso copre in dettaglio i principi e le tecnologie alla base delle piattaforme blockchain e le proprietà che garantiscono, da un lato, e mira a fornire i mezzi per la creazione e l'analisi di soluzioni e applicazioni basate su blockchain, dall'altro.

Obiettivi specifici:
Il corso affronta quattro argomenti principali: 1) fondamenti delle blockchain e delle tecnologie distributed ledger; 2) programmazione dei contratti intelligenti; 3) sviluppo di un'applicazione blockchain-based full-stack; 4) valutazione e analisi di un'applicazione blockchain-based.

Conoscenza e comprensione:
Gli studenti apprenderanno le basi delle tecnologie blockchain e l'interazione delle tecniche sottostanti che portano all'immutabilità, persistenza e sicurezza delle piattaforme blockchain. Inoltre, impareranno a codificare smart contract e creare applicazioni decentralizzate (DApps) full-stack. Per progettare correttamente le DApps e i sistemi di token su cui si basano, gli studenti applicheranno i principi di modellazione ed esecuzione di processi. Sarà fornita anche una panoramica delle sfide di cybersecurity inerenti. Inoltre, i discenti guarderanno gli argomenti trattati da un punto di vista legislativo, al fine di considerare i vincoli normativi tra cui il rispetto della privacy degli utenti.

Applicazione di conoscenza e comprensione:
Al termine del corso, gli studenti avranno ottenuto una elevata comprensione dei pilastri fondamentali delle tecnologie per distributed ledger e delle blockchain. Avranno altresì la capacità di progettare e implementare sistemi basati su blockchain. Inoltre, produrranno report ad elevato livello informativo progettati per gli stakeholder delle applicazioni decentralizzate.

Autonomia di giudizio:
Gli studenti svilupperanno la capacità di valutare la qualità delle applicazioni decentralizzate e delle soluzioni basate su blockchain in generale dal punto di vista dell'affidabilità, della solidità comportamentale, del costo di esecuzione, dell'equilibrio del carico on-chain e off-chain, dell'applicabilità, della sicurezza informatica e della privacy.

Abilità comunicative:
Gli studenti impareranno a documentare le loro scelte progettuali, anche attraverso l'uso di diagrammi e reportistica. Avranno anche acquisito la capacità di preparare presentazioni su argomenti scientifici.

Capacità di apprendimento:
Le nozioni acquisite durante il corso forniranno agli studenti una solida base di conoscenza per poter ulteriormente approfondire gli aspetti più tecnici, e per mantenersi autonomamente informati sui continui sviluppi e aggiornamenti sulle blockchain e le distributed ledger technologies.

10616636 | MACHINE LEARNING SECURITY	2º	1º	6	ENG

Insegnamento	Anno	Semestre	CFU	Lingua
10600449 | ADVANCED INFORMATION SYSTEMS SECURITY AND BLOCKCHAIN	2º	2º	6	ENG

Obiettivi formativi

Lo scopo dell'insegnamento è quello di insegnare ad applicare tecniche di machine learning (incluso deep learning) in ambito di cybersecurity, e di capire le vulnerabilità che queste tecniche hanno in ambiti adversarial.
Obiettivi Specifici
Gli studenti impareranno formalmente e praticamente come funzionano diversi modelli di machine learning, le loro applicazioni a problemi di cybersecurity, e numerose vulnerabilità, attacchi e difese per proteggerli.
Conoscenza e Comprensione
- conoscenza e comprensione dei fondamenti matematici dietro le tecniche moderne di machine learning
- conoscenza e comprensione delle vulnerabilità dei modelli di machine learning ad attacchi adversarial
- conoscenza e comprensione di tecniche per proteggere i modelli da questi attacchi
- conoscenza e comprensione di varie applicazioni del machine learning ai problemi di cybersecurity
Applicazione di Conoscenza e Comprensione
- come selezionare le giuste tecniche di machine learning per un dato problema
- come implementare modelli di machine learning per risolvere dati problemi
- come analizzare i possibili rischi derivanti dalle applicazioni di machine learning a sistemi critici, come cybersecurity
Autonomia di Giudizio
Gli studenti saranno in grado di giudicare l’appropriatezza di una data applicazione di machine learning e valutarne possibili failure mode e vulnerabilità ad attacchi
Abilità Comunicative
Gli studenti saranno in grado di descrivere la sicurezza e l’appropriatezza di una data applicazione di machine learning e potranno valutare ed argomentare potenziali vulnerabilità e faliure modes.
Capacità di Apprendimento Successivo
Gli studenti saranno in grado di approfondire argomenti e modelli di machine learning più complessi e saranno equipaggiati con la conoscenza necessaria per studiare problemi di ricerca aperti nelle aree di cybersecurity e machine learning

Insegnamento	Anno	Semestre	CFU	Lingua

Obiettivi formativi

OBIETTIVI GENERALI

Il corso si propone di avvicinare lo studente a temi di sicurezza e privacy nei sistemi informativi avanzati. I recenti sviluppi delle Future Internet Technologies (ad esempio ICN), le architetture decentralizzate (ad esempio blockchain) e l'Internet of Things sollevano nuove e impegnative sfide di sicurezza e privacy. Il corso introdurrà soluzioni innovative presentate in letteratura per affrontare tali problematiche al fine di progettare e sviluppare componenti sicure e rispettose della privacy all'interno di un moderno ecosistema integrato di servizi basati sulle suddette tecnologie. Il corso affronterà argomenti relativi alla privacy e alla sicurezza in diversi domini, tra cui:

- Blockchain

- Internet of Things

- Future Internet Technologies

- Machine Learning

- Applicazioni Privacy-Preserving

OBIETTIVI SPECIFICI

Conoscenza e comprensione: Il corso stimola la curiosità degli studenti verso nuovi temi di sicurezza informatica. Lo studente apprende nuovi concetti che gli consentono di acquisire una conoscenza di base di innovativi sistemi informativi e della loro sicurezza.

Applicare la conoscenza e comprensione: Al termine del corso gli studenti dovrebbero essere in grado di analizzare recenti articoli scientifici relativi alla sicurezza, comprendere le informazioni principali, discuterle con i colleghi e riprodurne i risultati.

Capacità critiche e di giudizio: gli studenti acquisiscono la capacità di estrarre le principali informazioni da articoli scientifici e confrontarle con altre in letteratura. In questo modo lo studente sarà in grado di elaborare un giudizio critico sulla sicurezza di innovativi sistemi informativi allo stato dell'arte e di valutare cosa si può effettivamente ottenere e cosa è necessario per progredire ulteriormente nella ricerca.

Capacità di comunicazione: La discussione di un elaborato scientifico con la classe, valevole anche al fine dell'esame, richiede allo studente di approfondire uno degli argomenti affrontati durante le lezioni. Questo, stimola l'interazione durante la lezione e le capacità comunicative dello studente.

Capacità di apprendimento: Oltre alle classiche capacità di apprendimento fornite dallo studio teorico del materiale didattico, le modalità di svolgimento del corso, in particolare legate all’attività progettuale, stimola l'autoapprendimento degli studenti.

Obiettivi formativi

La laurea magistrale si propone di fornire conoscenze avanzate e di formare capacità professionali necessarie allo svolgimento di attività di ricerca, progettazione, realizzazione, verifica, coordinamento e gestione di sistemi informatici riferibili ai diversi ambiti di applicazione delle scienze e delle tecnologie informatiche nell'ambito della sicurezza e protezione dei sistemi, delle reti e delle infrastrutture informatiche e al trattamento sicuro e riservato dei dati. Il laureato magistrale in Sicurezza Informatica svolge attività di progettazione, sviluppo, realizzazione, verifica, manutenzione, controllo e gestione di infrastrutture e sistemi informatici sicuri e protetti. Obiettivo fondamentale della sua attività è il miglioramento costante di sistemi informatici sicuri e protetti, anche con riferimento alla gestione sicura dei dati sensibili, accompagnato dalla capacità di recepire e proporre negli ambiti applicativi in cui opera le innovazioni che continuamente caratterizzano la disciplina. Il corso di laurea magistrale si propone dunque di formare professionisti dotati di competenze scientifiche e tecnologiche di alto livello, di capacità metodologiche e operative e di visione aperta e critica delle problematiche connesse all'adozione e all'uso delle tecnologie informatiche. La laurea intende fornire a regime una preparazione di tipo multidisciplinare nel settore della cybersecurity a studenti provenienti da diverse estrazioni includendo economia, informatica, ingegneria dell'informazione, matematica, fisica e scienze statistiche. Obiettivi formativi specifici: • conoscere gli aspetti scientifici relativi alle fondamenta della progettazione, realizzazione, verifica e manutenzione di infrastrutture, sistemi informatici e dei relativi dati sicuri e protetti • conoscere le metodologie e gli strumenti tecnologici attraverso i quali si progettano, realizzano, verificano e mantengono infrastrutture, dati e sistemi informatici sicuri e protetti, con attenzione sia alle tecniche formali che sperimentali • conoscere i fondamenti del

informatica giuridica e del diritto commerciale elettronico • essere capaci di comunicare efficacemente, in forma scritta e orale, in almeno una lingua dell'Unione Europea, oltre l'italiano, anche con riferimento ai lessici disciplinari • possedere gli strumenti cognitivi di base per l'aggiornamento continuo delle proprie conoscenze • essere in grado di lavorare con ampia autonomia, anche assumendo responsabilità di progetti e strutture, ed evidenziando capacità relazionali e decisionali. I principali sbocchi occupazionali e professionali dei laureati magistrali di questa classe sono negli ambiti della sicurezza di infrastrutture e sistemi informatici e del trattamento di dati sensibili per imprese critiche, aziende di prodotti e servizi, enti della pubblica amministrazione e, più in generale, per qualunque organizzazione utilizzi sistemi informatici complessi. Il percorso formativo si articola nel modo seguente: • nel primo anno, i cui insegnamenti sono in gran parte obbligatori, viene fornita la preparazione di livello specialistico relativamente alle aree della crittografia, e delle reti di calcolatori, dei sistemi distribuiti, della statistica, dell'informatica giuridica e del diritto commerciale elettronico, del penetration testing e di altre metodologie etiche per testare la sicurezza dei sistemi informatici. • nel secondo anno si offre allo studente la possibilità di scegliere in quale direzione approfondire la propria preparazione, che può essere orientata verso tematiche relative alla cybersecurity in diversi contesti come, ad esempio, le infrastrutture critiche e i sistemi informatici, le applicazioni software e la loro progettazione sicura, la realizzazione di sistemi cloud, la gestione del rischio cyber in aziende e enti. Inoltre il secondo anno è prevista l'attività per la preparazione della tesi di laurea, che presenta i risultati di uno studio originale di natura applicativa, sperimentale o teorica. Per molti insegnamenti è prevista attività progettuale svolta in laboratorio, finalizzata allo sviluppo ed al test di soluzioni avanzate per problemi di complessità paragonabile a quella che si incontra nel mondo reale. Nell'ambito del corso di laurea magistrale è previsto che lo studente segua, oltre ai tradizionali insegnamenti, anche una delle attività formative complementari da 6 CFU proposte annualmente dal CAD. Esse mirano a creare competenze trasversali utili a completare il percorso formativo dello studente ed a favorire il suo inserimento nel mondo del lavoro. Il regolamento didattico del corso di laurea definirà, nel rispetto dei limiti normativi, la quota dell'impegno orario complessivo a disposizione dello studente per lo studio personale o per altre attività formative di tipo individuale.

Profilo professionale

Profilo

Information Officer

Funzioni

Information Officer. L'information officer è impegnato nella guida di analisi e re-engineering dei processi di business esistenti garantendo appropriate politiche di sicurezza, individuando e sviluppando la capacità di utilizzare nuovi strumenti, rimodellando le infrastrutture fisiche dell'impresa e l'accesso alla rete, e di identificare e sfruttare le risorse di conoscenza dell'impresa. Si occupa anche della gestione di progetti orientati alla sicurezza informatica all'interno dei sistemi informativi aziendali.

Competenze

L'Information Officer è dotato sia di competenze specifiche nel campo delle tecnologie e dei metodi per la sicurezza informatica sia di conoscenze interdisciplinari e di gestione, indispensabili per padroneggiare non solo gli aspetti più tecnici ma anche le esigenze derivanti dalla gestione dei sistemi informativi. Partendo da una formazione di tipo tecnico-scientifico, tali figure professionali approfondiscono tematiche trasversali che includono competenze di gestione di progetto, aspetti economici, competenze giuridiche, gestione dei rischi connessi col ciclo di vita di un progetto.

Sbocchi lavorativi

I principali sbocchi occupazionali e professionali dei laureati magistrali di questa classe sono negli ambiti della sicurezza di infrastrutture e sistemi informatici e del trattamento di dati sensibili per aziende di prodotti e servizi, enti della pubblica amministrazione e, più in generale, per qualunque organizzazione utilizzi sistemi informatici sicuri. Grandi, medie e piccole aziende, pubblica amministrazione, amministrazioni locali, enti di ricerca pubblici e privati, istituti di analisi economico-sociale.

Frequentare

Laurearsi

La prova finale consiste nella discussione di una tesi di laurea magistrale, costituita da un documento scritto in lingua inglese, che presenta i risultati di uno studio originale condotto su un problema di natura applicativa, sperimentale o di ricerca. La preparazione della tesi si svolge sotto la direzione di un relatore (che può essere un docente del corso di laurea, o di altri corsi di laurea italiani o stranieri o di un ente di ricerca italiano o straniero) e si svolge di norma nel secondo anno del corso, occupandone circa la metà del tempo complessivo. La prova finale potrà essere inerente a un'attività progettuale, di ricerca, metodologica o di tirocinio, presso una struttura industriale, istituzioni pubbliche di ricerca o presso i laboratori stessi dell'università. Il lavoro svolto dovrà dimostrare che lo studente ha raggiunto una padronanza delle metodologie di Cybersecurity e/o della loro applicazione in un settore specifico a un livello di competenza in linea con le esigenze imposte dai processi di innovazione tecnologica. La prova finale sarà impostata in maniera tale da costituire una credenziale importante per l'inserimento del laureato nel tessuto lavorativo.

Organizzazione

Presidente del Corso di studio - Presidente del Consiglio di area didattica

Daniele Venturi

Tutor del corso

DANIELE VENTURI
FRANCESCA CUOMO
GIUSEPPE ANTONIO DI LUNA
TOMMASO GASTALDI

Manager didattico

Rappresentanti degli studenti

Eleonora Fornaro
William Corrias

Docenti di riferimento

TOMMASO GASTALDI
SILVIA BONOMI
ANGELO SPOGNARDI
DANIELE CONO D'ELIA
FRANCESCA CUOMO
GIUSEPPE ANTONIO DI LUNA
LEONARDO QUERZONI
FABRIZIO D'AMORE
MARCO POLVERINI
FRANCESCO LIBERATI

Regolamento del corso

Il percorso formativo si articola nel modo seguente: • nel primo anno, i cui insegnamenti sono in gran parte obbligatori, viene fornita la preparazione di livello specialistico relativamente alle aree della crittografia, e delle reti di calcolatori, dei sistemi distribuiti, della statistica, dell’informatica giuridica e del diritto commerciale elettronico, del penetration testing e di altre metodologie etiche per testare la sicurezza dei sistemi informatici. • nel secondo anno si offre allo studente la possibilità di scegliere in quale direzione approfondire la propria preparazione, che può essere orientata verso tematiche relative alla cybersecurity nel contesto: di infrastrutture e sistemi anche cyber-physical, delle applicazioni software e della loro progettazione sicura, della programmazione, e della gestione del rischio . Nel secondo anno è prevista inoltre l'attività per la preparazione della tesi di laurea, che presenta i risultati di uno studio originale di natura applicativa, sperimentale o teorica. Per molti insegnamenti è prevista attività progettuale svolta in laboratorio, finalizzata allo sviluppo ed al testing di soluzioni avanzate per problemi di complessità paragonabile a quella che si incontra nel mondo reale. Nell’ambito del corso di laurea magistrale è previsto che lo studente segua, oltre ai tradizionali insegnamenti, anche una delle attività formative complementari da 6 CFU proposte annualmente dal CAD. Esse mirano a creare competenze trasversali utili a completare il percorso formativo dello studente ed a favorire il suo inserimento nel mondo del lavoro. Il regolamento didattico del corso di laurea definisce, nel rispetto dei limiti normativi, la quota dell'impegno orario complessivo a disposizione dello studente per lo studio personale o per altre attività formative di tipo individuale.

Assicurazione qualità

Consultazioni iniziali con le parti interessate

In data 2/11/2016 alle ore 17.00 presso la sede della Facoltà I3S di Via Ariosto 25, sono state incontrate imprese (Telecom Italia, Leonardo Company, Vitrociset, AIIC, ACEA SpA, SOGEI, Elettronica) ed enti pubblici (Polizia di Stato, AGID, ESA, Corte di Cassazione) in relazione alla proposta di laurea magistrale in Cybersecurity. Altre aziende quali IBM, CISCO, Epsadatacom, ed enti pubblici quali Cassa Risparmi e Depositi, MISE, Corte dei Conti e CERT Nazionale, pur non essendo potute intervenire hanno comunicato tramite email il loro pieno sostegno all'iniziativa e la disponibilità a seguire da vicino nel prossimo futuro lo sviluppo della laurea magistrale. Tutte le realtà dei servizi, dell'industria e delle professioni intervenute hanno sottolineato la difficoltà di reperire sul mercato del lavoro le figure professionali legate al mondo della sicurezza cibernetica. Tutte hanno lamentato una mancanza di personale qualificato in grado di definire e gestire processi di analisi e governo della sicurezza di sistemi ed informazioni in ambito aziendale, di attuare processi di gestione degli incidenti informatici, di sviluppare attraverso metodologie avanzate software sicuro e, infine, di inquadrare gli aspetti legati alla sicurezza di sistemi e informazioni all'interno delle politiche aziendali di gestione del rischio. La consultazione ha rivelato positivamente come l'approccio interdisciplinare della laurea sia quindi un aspetto fondamentale per la preparazione dei profili professionali richiesti dal mercato. Le aziende e gli enti intervenuti hanno inoltre rimarcato come le figure che verranno preparate attraverso questo corso di laurea magistrale si inquadrino perfettamente all'interno Quadro strategico nazionale per la sicurezza dello spazio cibernetico varato dalla Presidenza del Consiglio dei Ministri con decreto del 27 gennaio 2014. In particolare nell'indirizzo operativo 3 che prevede la creazione di una workforce di esperti di cybersecurity adeguata alle esigenze del nostro paese. Infine a livello Europeo, la direttiva NIS che diventerà operativa nei paesi membri nel 2018 prevede la costituzione di gruppi di esperti in cybersecurity all'interno di ogni infrastruttura sensibile di ogni stato membro in modo da aumentare la resilienza europea a attacchi cyber. Il 30 gennaio 2017, si è tenuto l'incontro conclusivo, a livello di Ateneo, della consultazione con le Parti Sociali. Durante tale incontro sono stati acquisiti i pareri delle organizzazioni consultate, come riportato nel verbale allegato. L'Ateneo prevede incontri con le Parti Sociali, con cadenza annuale.

Consultazioni successive con le parti interessate

In data 2/11/2016 alle ore 17.00 presso la sede della Facoltà I3S di Via Ariosto 25, sono state incontrate imprese (Telecom Italia, Leonardo Company, Vitrociset, AIIC, ACEA SpA, SOGEI, Elettronica) ed enti pubblici (Polizia di Stato, AGID, ESA, Corte di Cassazione) in relazione alla proposta di laurea magistrale in Cybersecurity. Altre aziende quali IBM, CISCO, Epsadatacom, ed enti pubblici quali Cassa Risparmi e Depositi, MISE, Corte dei Conti e CERT Nazionale, pur non essendo potute intervenire, hanno comunicato tramite email il loro pieno sostegno all'iniziativa e la disponibilità a seguire da vicino nel prossimo futuro lo sviluppo della laurea magistrale. Tutte le realtà dei servizi, dell'industria e delle professioni intervenute hanno sottolineato la difficoltà di reperire sul mercato del lavoro le figure professionali legate al mondo della sicurezza cibernetica. Tutte hanno lamentato una mancanza di personale qualificato in grado di definire e gestire processi di analisi e governo della sicurezza di sistemi ed informazioni in ambito aziendale, di attuare processi di gestione degli incidenti informatici, di sviluppare attraverso metodologie avanzate software sicuro e, infine, di inquadrare gli aspetti legati alla sicurezza di sistemi e informazioni all'interno delle politiche aziendali di gestione del rischio. La consultazione ha rivelato positivamente come l'approccio interdisciplinare della laurea sia quindi un aspetto fondamentale per la preparazione dei profili professionali richiesti dal mercato. Le aziende e gli enti intervenuti hanno inoltre rimarcato come le figure che verranno preparate attraverso questo corso di laurea magistrale si inquadrino perfettamente all'interno Quadro strategico nazionale per la sicurezza dello spazio cibernetico varato dalla Presidenza del Consiglio dei Ministri con decreto del 27 gennaio 2014. In particolare nell'indirizzo operativo 3 che prevede la creazione di una work force di esperti di cybersecurity adeguata alle esigenze del nostro paese. Infine a livello Europeo, la direttiva NIS che diventerà operativa nei paesi membri nel 2018 prevede la costituzione di gruppi di esperti in cybersecurity all'interno di ogni infrastruttura sensibile di ogni stato membro in modo da aumentare la resilienza europea a attacchi cyber. Il 30 gennaio 2017, si è tenuto l'incontro conclusivo, a livello di Ateneo, della consultazione con le Parti Sociali. Durante tale incontro sono stati acquisiti i pareri delle organizzazioni consultate. L'Ateneo prevede incontri con le Parti Sociali, con cadenza annuale. Nel mese di marzo 2018, sono state incontrate imprese ed enti pubblici per una valutazione sull’andamento del primo semestre di attivazione della laurea magistrale in Cybersecurity. Tutte hanno manifestato il loro pieno sostegno all'iniziativa e hanno confermato la difficoltà di reperire sul mercato del lavoro le figure professionali legate al mondo della

Cybersecurity.

Organizzazione e responsabilità della AQ del Cds

Il Sistema di Assicurazione Qualità (AQ) di Sapienza è descritto diffusamente nelle Pagine Web del Team Qualità consultabili all'indirizzo https://www.uniroma1.it/it/pagina/team-qualita. Nelle Pagine Web vengono descritti il percorso decennale sviluppato dall'Ateneo per la costruzione dell'Assicurazione Qualità Sapienza, il modello organizzativo adottato, gli attori dell'AQ (Team Qualità, Comitati di Monitoraggio, Commissioni Paritetiche Docenti-Studenti, Commissioni Qualità dei Corsi di Studio), i Gruppi di Lavoro attivi, le principali attività sviluppate, la documentazione predisposta per la gestione dei processi e delle attività di Assicurazione della Qualità nella Didattica, nella Ricerca e nella Terza Missione. Le Pagine Web rappresentano inoltre la piattaforma di comunicazione e di messa a disposizione dei dati di riferimento per le attività di Riesame, di stesura delle relazioni delle Commissioni Paritetiche Docenti-Studenti e dei Comitati di Monitoraggio e per la compilazione delle Schede SUA-Didattica e SUA-Ricerca. Ciascun Corso di Studio e ciascun Dipartimento ha poi facoltà di declinare il Modello di Assicurazione Qualità Sapienza definito nelle Pagine Web del Team Qualità nell'Assicurazione Qualità del CdS/Dipartimento mutuandolo ed adattandolo alle proprie specificità organizzative pur nel rispetto dei modelli e delle procedure definite dall'Anvur e dal Team Qualità. Le Pagine Web di CdS/Dipartimento rappresentano, unitamente alle Schede SUA-Didattica e SUA-Ricerca, gli strumenti di comunicazione delle modalità di attuazione del Sistema di Assicurazione Qualità a livello di CdS/Dipartimento.