

Università	Università di PISA
Facoltà	SCIENZE MATEMATICHE FISICHE e NATURALI
Classe	LM-66 Sicurezza informatica
Nome del corso	SICUREZZA INFORMATICA: INFRASTRUTTURE ED APPLICAZIONI adeguamento di SICUREZZA INFORMATICA: INFRASTRUTTURE ED APPLICAZIONI (codice 1011785)
Nome inglese del corso	Security of Information Systems: Infrastructure and Applications
Il corso è	di nuova istituzione
Data di approvazione del consiglio di facoltà	01/04/2009
Data di approvazione del senato accademico	02/04/2009
Data della relazione tecnica del nucleo di valutazione	09/01/2009
Data del parere favorevole del Comitato regionale di Coordinamento	22/01/2009
Data della consultazione con le organizzazioni rappresentative a livello locale della produzione, servizi, professioni	28/01/2009
Modalità di svolgimento	convenzionale
Indirizzo internet del corso di laurea	http://sec.di.unipi.it
Massimo numero di crediti riconoscibili (DM 16/3/2007 Art 4)	20
Corsi della medesima classe	

Sintesi della relazione tecnica del nucleo di valutazione

Il Corso di Laurea Magistrale in Sicurezza Informatica: Infrastrutture e Applicazioni appartiene alla classe LM-18, ha sede a La Spezia ed è di nuova istituzione; esso ha l'obiettivo di formare laureati che sappiano applicare le conoscenze informatiche ai sistemi informatici per il controllo, il governo e la gestione di infrastrutture critiche. Non vi sono curricula. Viene indicato come naturale prosecuzione del corso di laurea in Informatica Applicata, già attivato a La Spezia l'anno scorso. I requisiti curriculari di ammissione sono precisamente indicati come numero di crediti da acquisire in specifici settori disciplinari, mentre la verifica della preparazione personale sarà stabilita dal reg. did. del CdS.

Sono da valutare positivamente:

- ob. form. spec. coerenti con ob. apprend. (descr. Dublino)
- la presenza di un percorso di eccellenza;
- la percentuale di "docenti equivalenti", pari a 0,78;
- il rispetto dei requisiti minimi di cui all'art 6 DM. 544/2007;
- la sostenibilità del complesso dei CdS proposti dalla Facoltà in termini di docenza;
- la coerenza dell'attività di ricerca svolta dai docenti del CdS con gli obiettivi formativi;
- la compatibilità dell'offerta formativa con le strutture.

Non sono indicate le modalità di recupero delle lacune nella preparazione.

Il NVA esprime parere favorevole alla istituzione del CdLM in Informatica: infrastrutture ed applicazioni, per le motivazioni sopra esposte.

Sintesi della consultazione con le organizzazioni rappresentative a livello locale della produzione, servizi, professioni

L'Università di Pisa è attualmente impegnata da una profonda evoluzione, innestata dalla pubblicazione del D.M. 270/04, incentrata su innovativi processi di autonomia, di responsabilità e di qualità. L'attuazione di tali processi, però, dipende anche dalla possibilità di realizzare una più efficace integrazione tra università e apparato produttivo. L'autonomia didattica si sta indirizzando verso alcuni obiettivi di sistema, come il ridurre e razionalizzare il numero dei corsi di laurea e delle prove d'esame, migliorare la qualità e la trasparenza dell'offerta e il rapportarsi tra progettazione e analisi della domanda di conoscenze e competenze espressa dai principali attori del mercato del lavoro, come elemento fondamentale per la qualità e l'efficacia delle attività cui l'università è chiamata.

Si è chiesto ai consessi l'espressione di un parere circa l'ordinamento didattico del corso in Sicurezza informatica: infrastrutture ed applicazioni.

Il fatto che l'Università di Pisa abbia privilegiato nel triennio la formazione di base spostando al secondo livello delle lauree magistrali numerosi indirizzi specialistici che potranno coprire alcune esigenze di conseguimento di professionalità specifiche per determinati settori, è stato giudicato positivamente sottolineando anche che, oltre all'attenzione posta alla formazione di base, positivi sono sia la flessibilità curricolare che l'autonomia e la specificità della sede universitaria, che mostra in questo contesto tutte le eccellenze di cui è depositaria.

Sintesi del parere del comitato regionale di coordinamento

Il Comitato regionale di coordinamento delle Università toscane, viste le proposte dell'Università di Pisa, valutate le motivazioni addotte dal proponente esprime parere favorevole per l'istituzione del corso di studio.

Il rettore dichiara che nella stesura dei regolamenti didattici dei corsi di studio il presente corso ed i suoi eventuali curricula differiranno di almeno 30 crediti dagli altri corsi e curricula appartenenti alla medesima classe, ai sensi del DM 16/3/2007, art. 1 §2.

Obiettivi formativi qualificanti della classe

I laureati magistrali nei corsi di laurea della classe devono:

- conoscere gli aspetti scientifici relativi alle fondamenta della progettazione, realizzazione, verifica e manutenzione di infrastrutture e sistemi informatici sicuri e protetti
- conoscere le metodologie e gli strumenti tecnologici attraverso i quali si progettano, realizzano, verificano e mantengono infrastrutture e sistemi informatici sicuri e protetti, con attenzione sia alle tecniche formali che sperimentali
- conoscere gli aspetti relativi alla organizzazione del lavoro ed alle problematiche di carattere psicologico e sociale come elementi critici rispetto alla sicurezza delle infrastrutture e dei sistemi informatici ed alla protezione dei dati informatici, nonché gli aspetti giuridici relativi al trattamento sicuro e riservato dei dati informatici e quelli bio-sanitari e bio-etici relativi alle tecniche biometriche ed al trattamento, conservazione e trasmissione dei dati sensibili riguardanti la salute
- 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, aziende di servizi, enti della pubblica amministrazione e, più in generale, per qualunque organizzazione utilizzi sistemi informatici complessi.

Ai fini indicati, i curricula dei corsi di laurea magistrale della classe:

- prevedono lezioni ed esercitazioni di laboratorio oltre ad attività progettuali autonome e attività individuali in laboratorio per non meno di 10 crediti;
- prevedono, in relazione a obiettivi specifici, attività esterne come tirocini formativi presso aziende, strutture della pubblica amministrazione e laboratori, oltre a soggiorni di studio presso altre università italiane ed europee, anche nel quadro di accordi internazionali.

In considerazione della valenza sia scientifica che professionalizzante di questo percorso formativo, l'ammissione ai corsi di laurea magistrale della classe richiede il possesso di requisiti curriculari che prevedano, comunque, un'adeguata padronanza di metodi e contenuti scientifici propedeutici a quelli di almeno uno degli ambiti disciplinari caratterizzanti l'ordinamento della presente classe di laurea magistrale.

Obiettivi formativi specifici del corso e descrizione del percorso formativo

Il corso di laurea "Sicurezza informatica: infrastrutture ed applicazioni" ha come obiettivo quello di formare laureati che sappiano applicare le conoscenze e competenze dei laureati della classe a tutti i sistemi informatici ed in particolare quelli per il controllo, il governo e la gestione di infrastrutture critiche, ad esempio quelle per la distribuzione della energia elettrica o di beni materiali. Questa è la ragione della particolare attenzione prestata a temi quali le infrastrutture logistiche, la sicurezza fisica di sistemi di elaborazione e trasmissione delle informazioni, i componenti di tipo Radio Frequency Identification (RFID) per l'identificazione ed il monitoraggio attivo e passivo della sicurezza e dell'integrità di merci e container. La specificità del corso di laurea è fortemente correlata alle specificità del territorio spezzino che ha un forte interesse alla sicurezza ed alla logistica così come evidenziato dalle attività del nascente Distretto Ligure delle Tecnologie Marine che avrà un ruolo privilegiato per la collaborazione mediante tesi ed attività di ricerca sulle problematiche su cui il corso di studi è focalizzato.

Risultati di apprendimento attesi, espressi tramite i Descrittori europei del titolo di studio

Conoscenza e capacità di comprensione (knowledge and understanding)

Il laureato magistrale in Sicurezza Informatica possiede le conoscenze scientifiche e la capacità di comprensione che permettono di affrontare e di risolvere problemi di sicurezza tramite tecnologie informatiche innovative. Le conoscenze acquisite con la laurea triennale vengono raffinate e focalizzate sulla comprensione dei problemi di sicurezza posti dalle infrastrutture informatiche viste sia in isolamento sia come elementi di controllo e gestione di sistemi informatici più complessi, in particolare quelle collegate ai trasporti materiali ed immateriali. La capacità di analizzare tali sistemi e di integrare in essi componenti che ne aumentino la sicurezza, nei suoi aspetti di integrità, confidenzialità e disponibilità, permette anche al laureato di definire, implementare e valutare nuovi componenti interagendo e partecipando con gruppi di ricerca che si occupino dei temi considerati. Proprio per garantire una conoscenza approfondita degli aspetti di sicurezza parte degli insegnamenti approfondisce gli aspetti metodologici della sicurezza e degli strumenti informatici per la sicurezza. I laureati devono conoscere i vari standard internazionali che regolano le varie attività di sicurezza ed intervenire attivamente nella loro definizione.

Capacità di applicare conoscenza e comprensione (applying knowledge and understanding)

Il laureato magistrale in Sicurezza Informatica è in grado di applicare le sue conoscenze e capacità di comprensione in modo da dimostrare un approccio professionale al lavoro. Possiede le competenze adeguate e le conoscenze tecnico-scientifiche necessarie per gestire il rischio dei sistemi informativi. La gestione del rischio è una attività altamente complessa che richiede un insieme di capacità correlate per realizzare i seguenti passi

1. analizzare un sistema ed individuarne le vulnerabilità
2. individuare gli attacchi che tali vulnerabilità permettono

3. individuare gli attori (minacce) in grado di attaccare il sistema e quali obiettivi tali minacce si prefiggono
4. individuare gli attacchi che tali minacce possono realizzare
5. individuare gli obiettivi che le minacce possono raggiungere ed i danni per l'utilizzatore del sistema
6. individuare quali contromisure possono essere applicate per ridurre o minimizzare il danno.

Altra competenza fondamentale è quella di comunicare il risultato delle loro analisi in tutti quei casi in cui gli utilizzatori e gli utenti del sistema non possiedono le competenze tecnologiche necessarie per la comprensione delle analisi.

Ciò che caratterizza il laureato è la capacità di condurre tutte le varie analisi in modo formale ed utilizzando strumenti logico-matematici ed informatici. Il laureato deve altresì essere in grado di definire chiaramente i margini di incertezza della propria analisi in modo da permettere agli utilizzatori di compiere scelte informate e coscienti. L'impostazione degli insegnamenti del percorso formativo prevede che la formazione teorica sia accompagnata da esempi, applicazioni, lavori individuali e di gruppo e verifiche che sollecitino la partecipazione attiva, l'attitudine propositiva, la capacità di elaborazione autonoma e di comunicazione dei risultati del lavoro svolto. Sono previste due tipologie di valutazione: valutazione finale e valutazioni intermedie.

La parte di approfondimento ed elaborazione delle conoscenze demandata allo studio personale dello studente assume a questo proposito una rilevanza notevole, è infatti tramite una congrua rielaborazione personale delle informazioni introdotte durante le ore di lezione che lo studente misura concretamente quale sia il livello di padronanza delle conoscenze. Accanto allo studio personale assumono notevole importanza anche le attività di laboratorio eseguite in gruppo e le esercitazioni svolte in aula.

Autonomia di giudizio (making judgements)

I laureati devono essere in grado di valutare in modo autonomo utilizzando strumenti matematici ed informatici i rischi conseguenti all'adozione o alla modifica di sistemi informativi per il controllo e la gestione di sistemi complessi, in primis una infrastruttura informatica o logistica complessa. Devono anche essere in grado di decidere quali strumenti organizzativi, gestionali ed informatici possano essere utilizzati per ridurre il rischio ad un livello accettabile per il proprietario e per gli utilizzatori di tali sistemi. Devono inoltre valutare l'adeguatezza del lavoro svolto rispetto al contesto normativo.

La prima parte del percorso formativo della laurea magistrale si pone come obiettivo quello fare crescere la capacità di astrazione degli studenti analizzando la sicurezza di un sistema informatico nel contesto aziendale a diversi livelli di astrazione. Questa capacità di considerare la sicurezza usando tecniche e linguaggi differenti è l'aspetto che meglio caratterizza il laureato magistrale e che gli permette di comprendere e dominare la complessità dei settori dell'innovazione tecnologica, aziendale ed anche normativa. Successivamente lo studente può scegliere tra diverse attività formative che approfondiscono tematiche differenti e riflettono alcune tra le linee di ricerca innovative del settore della sicurezza informatica.

Inoltre, gli insegnamenti di carattere sperimentale introdotte nel piano di studio enfatizzano, attraverso esercitazioni svolte in laboratorio, sia individuali che di gruppo, la capacità di selezionare, elaborare ed interpretare problemi complessi nel settore della sicurezza. Il piano di studi comprende attività di esercitazione autonoma e di gruppo affinché lo studente sia in grado di valutare autonomamente i risultati ottenuti da questo tipo di attività didattica. Tra le finalità di queste attività ci sono lo sviluppo della capacità di lavorare in gruppo, la competenza di selezionare le informazioni rilevanti per l'analisi e la risoluzione di un problema di sicurezza posto da un sistema informatico e lo sviluppo delle capacità di esprimere giudizi.

Abilità comunicative (communication skills)

I laureati devono saper comunicare i rischi posti dall'adozione di sistemi informativi in modo da permettere a decisori che in generale non possiedono le competenze scientifiche e tecnologiche per apprezzare e valutare tali rischi di compiere delle scelte informate per quanto riguarda l'adozione di sistemi informativi complessi. Devono anche saper comunicare in forma scritta e orale i rischi agli utenti finali di tali sistemi per evitare che comportamenti non corretti degli utenti aumentino tali rischi.

Il laureato magistrale saranno in grado di comunicare con altri specialisti tecnico scientifici per interagire e cooperare con loro. Inoltre saranno in grado di documentare le analisi sulla sicurezza e le soluzioni proposte ai vari livelli di costruzione ed implementazione dei sistemi informatici di interesse producendo relazioni scritte utilizzando un linguaggio tecnico scientifico appropriato.

Nel percorso formativo, alcuni degli insegnamenti prevedono lo svolgimento, da parte degli studenti, di attività di progetto a cui deve seguire una discussione per favorirne il coinvolgimento e prepararli al confronto pubblico con gli interlocutori. La valutazione finale degli insegnamenti (esami di profitto) è un ulteriore strumento di elaborazione e comunicazione del lavoro svolto: la valutazione finale dell'insegnamento è composto da una prova scritta e una prova orale. La prova finale offre inoltre allo studente un'ulteriore opportunità di approfondimento e di verifica delle capacità di analisi, elaborazione e comunicazione del lavoro svolto. Essa prevede infatti, di norma, la discussione, innanzi ad una commissione, di un elaborato, con contenuti di originalità preparata dallo studente. La tesi deve essere relativa ad un argomento o progetto a carattere innovativo, svolta in autonomia dallo studente. La tesi dovrà documentare i risultati innovativi ottenuti nonché i collegamenti del lavoro svolto con lo stato delle conoscenze nel settore della sicurezza informatica. In tutti i casi i laureati magistrali dovranno poter utilizzare sia la lingua italiana che quella inglese.

Capacità di apprendimento (learning skills)

I laureati devono possedere competenze matematiche ed informatiche che permettano loro un aggiornamento costante sulle vulnerabilità dei sistemi informativi e sulle contromisure che permettano di limitare o ridurre il rischio collegato a tali vulnerabilità. In particolare, le competenze matematiche devono permettere loro di conoscere e sapere applicare nuove strategie per l'encryption o la compressione dei dati. Per quanto riguarda le competenze informatiche, il laureato deve saper applicare le metodologie per l'analisi del rischio ai sistemi prodotti dalla evoluzione delle tecnologie informatiche.

Inoltre il laureato magistrale in Sicurezza Informatica sarà dotato di una preparazione culturale, scientifica e metodologica di base che gli permetterà di accedere ai livelli di studio universitario successivi al magistrale, quali il Dottorato di Ricerca in Informatica. La suddivisione delle ore di lavoro complessive previste per lo studente dà un forte rilievo alle ore di lavoro personale proprio per offrire allo studente la possibilità di verificare e migliorare la propria capacità di apprendimento. Analogo obiettivo viene perseguito con il rigore metodologico dell'impostazione degli insegnamenti di base, che deve portare lo studente a sviluppare l'attitudine a un ragionamento orientato alla risoluzione di problemi (problem solving) con solide basi scientifiche e metodologiche che, sulla base di precise ipotesi, porti alla conseguente risoluzione di un problema ed alla dimostrazione della correttezza ed adeguatezza della soluzione prodotta. Altri strumenti utili al conseguimento di questa abilità sono i progetti di laboratorio, e la prova finale.

Conoscenze richieste per l'accesso

I requisiti curriculari per l'ammissione al corso di studi sono definiti nel regolamento didattico del corso di studi medesimo in termini di numero di CFU conseguiti in specifici settori scientifico-disciplinari. Il regolamento didattico del corso di studi definisce altresì le modalità di verifica della personale preparazione dello studente.

I principi a cui si ispirerà il regolamento sono i seguenti:

Ammissione per i laureati triennali delle classi

- ° Scienze matematiche: classe 32, classe L-35
- ° Scienze e tecnologie fisiche: classe 25, classe L-30
- ° Scienze e tecnologie informatiche: classe 26, classe L-31
- ° Ingegneria dell'informazione: classe 9, classe L-8

Potranno essere comunque ammessi laureati triennali in altre classi che abbiano acquisito i seguenti crediti nei seguenti settori

1. Conoscenze informatiche di base: 24 CFU
2. Conoscenze matematiche di base: 24 CFU
3. Architetture, Sistemi operativi: 12 CFU
4. Reti e programmazione di rete: 18 CFU
5. Metodologie di programmazione ed ingegneria del software: 24 CFU

Eventuali lacune nelle conoscenze in ingresso dovranno essere colmate secondo le modalità previste nel regolamento didattico di corso di studio

Caratteristiche della prova finale

La prova finale prevede una parte teorica ed una sperimentale che si svolge sotto la supervisione di un docente del corso. Parte della attività può anche essere svolta in una azienda interessata alle tematiche della sicurezza. Tale azienda può essere una utilizzatrice degli sistemi informativi per i propri processi aziendali oppure può essere interessata allo sviluppo di nuovi strumenti informatici per aumentare la sicurezza dei sistemi esistenti. I laboratori utilizzati per la parte sperimentale possono essere quelli del corso di studi, quelli della ditta coinvolta nella prova oppure quelli del distretto tecnologico di La Spezia. Parte dei crediti previsti per la prova finale è dedicata alla stesura della relazione finale.

Sbocchi occupazionali e professionali previsti per i laureati

1. industrie informatiche che sviluppano sistemi
 - a. con elevate caratteristiche di sicurezza
 - b. per il settore della difesa
 - c. applicazioni biomedicali
 - d. applicazioni per il governo elettronico
2. enti pubblici ed industrie operanti nei settori
 - a. della difesa e della salute
 - b. sicurezza ambientale ed anti intrusione
 - c. della logistica e dei trasporti
3. enti pubblici e privati operanti nel campo della certificazione di processo e di sistemi software

Il corso prepara alle professioni di

- Analisti e progettisti di software applicativi e di sistema
- Analisti di sistema
- Specialisti in sicurezza informatica
- Specialisti in reti e comunicazioni informatiche
- Ricercatori e tecnici laureati nelle scienze matematiche e dell'informazione

Attività formative caratterizzanti

ambito disciplinare	settore	CFU
Ambito Scientifico	INF/01 Informatica ING-INF/05 Sistemi di elaborazione delle informazioni MAT/06 Probabilità e statistica matematica MAT/09 Ricerca operativa	36 - 36
Ambito Tecnologico	INF/01 Informatica ING-INF/05 Sistemi di elaborazione delle informazioni	18 - 30
Ambito Giuridico, Sociale ed Economico	IUS/14 Diritto dell'unione europea IUS/20 Filosofia del diritto SECS-P/08 Economia e gestione delle imprese SECS-P/10 Organizzazione aziendale SECS-S/01 Statistica	12 - 12

Totale crediti riservati alle attività caratterizzanti (da DM min 48)

66 - 78

Attività formative affini ed integrative

settore	CFU
CHIM/12 Chimica dell'ambiente e dei beni culturali ICAR/04 Strade, ferrovie e aeroporti INF/01 Informatica ING-IND/35 Ingegneria economico-gestionale ING-INF/03 Telecomunicazioni ING-INF/05 Sistemi di elaborazione delle informazioni IUS/14 Diritto dell'unione europea IUS/20 Filosofia del diritto MAT/05 Analisi matematica MAT/06 Probabilità e statistica matematica MAT/09 Ricerca operativa SECS-P/06 Economia applicata SECS-P/08 Economia e gestione delle imprese SECS-P/10 Organizzazione aziendale SECS-S/01 Statistica SECS-S/06 Metodi matematici dell'economia e delle scienze attuariali e finanziarie	12 - 24

Motivazioni dell'inserimento nelle attività affini di settori previsti dalla classe (INF/01, ING-INF/03, ING-INF/05, IUS/14, IUS/20, MAT/05, MAT/06, MAT/09, SECS-P/08, SECS-P/10, SECS-S/01)

In generale, vista la possibilità di accedere al corso di laurea da classi di lauree triennali diverse, si è scelto di allocare i crediti negli stessi settori di quelli caratterizzanti per potenziare la preparazione di base dei laureati triennali ammessi al corso nei settori non coperti dalla laurea posseduta.

Questa è l'unica strategia che permette di erogare un numero di crediti formativi in grado di fornire agli studenti le competenze e le conoscenze richieste dagli obiettivi formativi, indipendentemente dalla laurea triennale posseduta. In particolare i settori INF/01, ING-INF/03, ING-INF/05 permettono di potenziare la formazione nel settore dell'informatica, delle reti e delle telecomunicazioni.

I settori IUS/14 e IUS/20 permettono di potenziare la formazione nei settori del diritto nazionale ed europeo, per consentire al laureato di valutare il rispetto della normativa nazionale ed europea.

I settori MAT/05, MAT/06 e MAT/09 permettono di rafforzare la formazione nei settori della ricerca operativa, dell'analisi e della statistica fornendo le conoscenze necessarie per l'applicazione di modelli matematici e statistici all'analisi del rischio.

I settori SECS-P/08, SECS-P/10, SECS-S/01 consentono di rafforzare la formazione nei settori economico-aziendali, permettendo ai laureati di comprendere i problemi di carattere economico ed aziendale e individuare soluzioni ai problemi di sicurezza coerenti con il contesto e gli obiettivi aziendali.

Altre attività formative (D.M. 270 art.10 §5)

ambito disciplinare		CFU
A scelta dello studente (art.10, comma 5, lettera a)		12
Per la prova finale (art.10, comma 5, lettera c)		17
Ulteriori attività formative (art.10, comma 5, lettera d)	Ulteriori conoscenze linguistiche	
	Abilità informatiche e telematiche	
	Tirocini formativi e di orientamento	
	Altre conoscenze utili per l'inserimento nel mondo del lavoro	1

Totale crediti riservati alle altre attività formative**30****CFU totali per il conseguimento del titolo (range 108 - 132)****120**