ISTITUTO DI SCIENZE FORENSI
CORPORATE UNIVERSITY

Regolamento dell'

Executive Master in Digital Forensics & Cyber Security 8° Ed.

con i docenti di

riconosciuto da

Associazione Nazionale Criminologi e Criminalisti
Associazione Professionale nazionale censita nell'elenco del
Ministero dello Sviluppo Economico ai sensi della legge 14 gennaio 2013, n. 4.
La maggiore Associazione Professionale di categoria dei Criminologi e dei Criminalisti Professionisti.
www.ancrim.it

Posti disponibili: 15 (quindici)
Scadenza iscrizioni: 29 novembre 2024

Art. 1. Executive Master in Digital Forensics & Cyber Security

L'Istituto di Scienze Forensi, nella persona del Direttore Generale, ha istituito il corso di alta formazione denominato "Executive Master in Digital Forensics & Cyber Security" per la preparazione della figura professionale dell'esperto in investigazioni digitali e sicurezza informatica.
Il presente Regolamento sarà valido per l'anno accademico 2024/2025. Eventuali modifiche e/o integrazioni al suo contenuto, saranno rese note agli interessati a mezzo posta elettronica.

Art. 2. Natura del percorso formativo

Gli Executive Master (master brevi) offerti dall'Istituto di Scienze Forensi Corporate University sono corsi di alta formazione rivolti ai laureati e ai diplomati già inseriti nel mondo del lavoro, i quali desiderano perfezionarsi o specializzarsi in un determinato ambito tecnico e/o scientifico. Possono accedere ai percorsi formativi in argomento anche soggetti ancora non collocati professionalmente che intendono ampliare, completare e/o integrare le proprie conoscenze al fine di renderle adatte alle proprie aspirazioni professionali e prontamente spendibili nel mondo del lavoro.

Art. 3. Obiettivi formativi

La Digital Forensics si occupa dell'identificazione, dell'acquisizione, dell'analisi e della documentazione dei reperti informatici al fine di ricavare elementi probatori, cioè le "digital evidences", in procedimenti civili e penali. La "digital evidence" può essere definita come "qualsiasi informazione con valore probatorio che sia memorizzata o trasmessa in forma digitale e che può essere estratta da dispositivi digitali quali personal computer, notebook, hard disk, USB drive, dispositivi di memoria SSD, tablet, smartphone, SIM card ecc.". Pertanto, la Digital Forensics assume un ruolo fondamentale nel contesto giudiziario, dove è richiesto acquisire e analizzare elementi di prova, nonché in campo civile, commerciale, giuslavoristico e fiscale per finalità di sicurezza, difesa o indagine di stampo stragiudiziale.
L'esigenza di un esperto con adeguata conoscenza delle metodologie per l'acquisizione, il trattamento e la gestione delle fonti di prova informatiche, che sia altresì in grado di adottare idonee misure per la tutela dei dati digitali, è sempre più sentita a qualsiasi livello e in qualsiasi contesto, da quello squisitamente giudiziario a quello aziendale. Del resto, le statistiche confermano che la criminalità informatica è in costante ascesa e i danni prodotti dal fenomeno su scala mondiale ammontano a centinaia di miliardi di euro ogni anno.
L'Executive Master in Digital forensics fornisce competenze di alto profilo finalizzate all'assunzione di incarichi di indagine, sicurezza e difesa in relazione alle attività illecite legate al mondo digitale.

Art. 4. Sbocchi professionali

L'Executive Master in Digital Forensics & Cyber Security intende formare esperti in grado di:

- gestire le fonti normative e le interpretazioni giurisprudenziali inerenti le nuove tecnologie;
- esprimere un livello di competenza tecnica e giuridica altamente qualificata, al fine di analizzare sistemi digitali e garantire procedure conformi alle normative nazionali ed europee nonché alle "best practices" internazionali.

Il percorso formativo prepara tecnici che potranno operare nei seguenti settori:

- Investigazioni private civili e penali;
- Consulenza tecnica giudiziaria e stragiudiziale;
- Attività ausiliarie di polizia giudiziaria (art. 348, c. 4, c.p.p.);
- Servizi di prevenzione, sicurezza e difesa delle organizzazioni pubbliche e private.

Art. 5. Destinatari, titoli di accesso e numero massimo di studenti

L'Executive Master in Digital Forensics & Cyber Security è rivolto a soggetti in possesso di diploma di

Data _____ Firma leggibile dell'aspirante studente_____

maturità o laurea come meglio sotto specificato:

- Diploma o laurea in Informatica
- Diploma o laurea in Scienze chimiche, fisiche, matematiche e assimilate
- Laurea in Ingegneria o Architettura
- Diploma o laurea in Scienze e tecnologie
- Laurea in Scienze giuridiche
- Diploma o laurea in Scienze economiche e/o aziendali

Potranno altresì essere ammessi sia diplomati (maturità) che laureati che abbiano acquisito conoscenze e maturato competenze di buon livello in ambito informatico e che siano in possesso dei prerequisiti fissati nell'articolo seguente.
Il numero massimo di studenti ammessi all'Executive Master è pari a 15 unità.

Art. 6. Prerequisiti di accesso (conoscenze e competenze di base per partecipare)

- Conoscenze e qualità di base: conoscenza dei concetti fondamentali dei file system (FAT, FAT32, NTFS, EXT3), dei sistemi operativi Windows, OSX e Linux e fondamenti di networking. Buone capacità di intervista, ricerca, comunicazione e problem solving. Conoscenza delle tecniche di base per rimuovere e installare componenti hardware in un PC.
- Elaborazione delle informazioni: capacità di usare strategie di ricerca avanzata (ad esempio utilizzando operatori di ricerca) per trovare informazioni affidabili su Internet. Capacità di valutazione della validità e della credibilità delle informazioni utilizzando una serie di idonei criteri. Conoscenza delle nuove tecniche e tecnologie di ricerca di informazioni, archiviazione e recupero.
- Creazione di contenuti: capacità di produrre o modificare contenuti multimediali in diversi formati, utilizzando una varietà di piattaforme digitali, strumenti e ambienti. Capacità di progettare, creare e modificare i database con uno strumento informatico.
- Comunicazione: capacità di usare una vasta gamma di strumenti di comunicazione (posta elettronica, chat, SMS, messaggistica istantanea, blog, micro-blog, reti sociali ecc.) per la comunicazione on-line. Capacità di creare e gestire i contenuti con strumenti di collaborazione (ad esempio calendari elettronici, i sistemi di gestione del progetto, di correzione in linea, fogli di calcolo on-line).
- Risoluzione dei problemi: capacità di risolvere i problemi che sorgono utilizzando la tecnologia digitale. Capacità di scegliere il corretto strumento (dispositivo, applicazione, software) o idonei servizi per risolvere i problemi non tecnici. Conoscenza di nuovi sviluppi tecnologici. Comprensione del funzionamento di nuovi strumenti di lavoro. Attitudine ad aggiornare spesso le proprie competenze digitali.
- Sicurezza: attitudine a controllare frequentemente la configurazione e i sistemi di sicurezza dei dispositivi e/o delle applicazioni usate. Capacità di risolvere i problemi di infezione da virus degli strumenti utilizzati. Capacità di configurare o modificare le impostazioni del firewall e di sicurezza dei dispositivi digitali. Capacità di crittografare le e-mail o i file e di applicare filtri per le e-mail (spam).
- Lingua inglese: livello minimo B1 (Quadro comune europeo di riferimento per la conoscenza delle lingue).

Art. 7. Dotazioni personali dello studente

Lo studente, per la parte di lezioni a distanza (videoconferenza), dovrà avere a disposizione un pc collegato a internet per accedere alla piattaforma Adobe Connect© dell'Istituto e seguire le videolezioni in diretta. Per le lezioni in presenza, invece, saranno disponibili i pc dell'aula informatica dell'Istituto.
Specifiche tecniche richieste per le videoconferenze:

Data _____ Firma leggibile dell'aspirante studente_____

Windows

- 1.4GHz Intel® Pentium® 4 o processore superiore o equivalente per Microsoft® Windows® XP, Windows 7 o Windows 8
- 2GHz Pentium 4 o processore equivalente per Windows Vista®, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10 o Windows Professional
- 1GB di RAM per Windows XP, Windows 7 or Windows 8; 2GB di RAM per Windows Vista
- Microsoft Internet Explorer 7, 8, 9, 10; Mozilla Firefox; Google Chrome
- Adobe® Flash® Player 10.3 Mac OS

Mac OS

- 1.83GHz Intel Core™ Duo o processore superiore
- 1GB di RAM
- Mac OS X, 10.5, 10.6, 10.7.4, 10.8
- Mozilla Firefox; Apple Safari; Google Chrome
- Adobe Flash Player 10.3 2

Requisiti aggiuntivi

- Connessione ADSL minimo 7Mbps
- Webcam, cuffie di buona qualità con microfono incorporato (sconsigliato il microfono integrato nel notebook)

Art. 8. Modalità di iscrizione

Per iscriversi all'Executive Master in Digital Forensics & Cyber Security è necessario effettuare il pagamento della prima rata della retta (o dell'intero importo se lo studente opta per il versamento in un'unica soluzione), compilare la domanda di ammissione, i moduli contrattuali (condizioni generali di contratto, contratto dei servizi erogati, autorizzazione al trattamento dei dati personali ecc.), procurarsi i documenti da allegare alla domanda di ammissione e spedirli con raccomandata a/r oppure consegnarli personalmente alla Segreteria Studenti dell'Istituto. Entro dieci giorni dall'inizio delle lezioni, lo studente riceverà via e-mail il numero di matricola e le credenziali per l'accesso all'applicazione web didattica.

Art. 9. Ente erogatore dell'Executive Master

L'Executive Master è erogato dall'Istituto di Scienze Forensi (codice fiscale e partita Iva IT09467620960) attraverso la propria Corporate University.
L'Istituto di Scienze Forensi è un'azienda certificata ISO 9001:2015 (Progettazione ed erogazione di servizi di formazione e consulenza tecnico scientifico forensi).
Sede delle lezioni e dei laboratori: Istituto di Scienze Forensi, via Leonardo da Vinci n. 5, Corsico (Milano). Sul sito internet www.scienzeforensi.net sono riportate tutte le indicazioni inerenti gli hotel convenzionati e le modalità per raggiungere questi ultimi e la sede dell'Istituto.

Art. 10. Compatibilità con la frequenza di corsi presso università pubbliche o private

L'Executive Master di cui al presente Regolamento è compatibile con l'immatricolazione e la frequenza di corsi di laurea, master ecc. presso università statali e private, salvo disposizioni dei regolamenti delle medesime università in cui si vietano attività formative svolte anche presso enti diversi da università.

Art. 11. Anno accademico, durata dell'Executive Master

L'anno accademico inizia il 1° ottobre e termina il 30 settembre dell'anno successivo. Per l'edizione dell'Executive Master in Digital Forensics & Cyber Security di cui al presente Regolamento, le lezioni (sia e-learning che in presenza), nonché le sessioni d'esame, si svolgeranno nell'anno accademico 2024/2025 a

Data _____ Firma leggibile dell'aspirante studente_____

partire dal mese di **gennaio 2024**.
Lo studente che non avrà frequentato almeno l'80% delle lezioni a distanza (videoconferenza) o delle lezioni frontali di ciascun insegnamento, ovvero che non avrà superato uno o più esami nelle sessioni previste, non potrà conseguire l'Attestato dell'Executive Master e la certificazione degli studi. In tal caso, dovrà iscriversi all'edizione successiva, qualora venisse attivata, versando una somma corrispondente al numero di crediti formativi ancora da conseguire in relazione al valore della retta ordinaria.

Art. 12. Crediti Formativi ISF

Ogni Credito Formativo corrisponde a 25 ore di attività secondo gli standard delle normative europee. Le ore di attività riguardano le lezioni a distanza (videoconferenza), lo studio e la ricerca individuale, la partecipazione alle lezioni in presenza, il tempo dedicato all'interazione con i docenti e i colleghi di corso, nonché eventuali attività "extra" organizzate dall'Istituto di Scienze Forensi Corporate University.

Art. 13. Modalità di erogazione, ore di lavoro ed esami

L'Executive Master è organizzato in attività didattiche di studio a distanza (lezioni in videoconferenza in diretta), interazioni con i docenti e i colleghi, lezioni frontali e laboratori presenziali che si svolgeranno secondo il **calendario che verrà pubblicato entro il giorno venerdì 30 agosto 2024 (salvo modifiche non dipendenti dalla volontà dell'Istituto)**.

Art. 13.1. Suddivisione ore di lavoro (totale 750 ore)

- Lezioni in videoconferenza: 50
- Lezioni in presenza: 54 (teoria 10 - laboratorio 44)
- Studio individuale: 360
- Attività di ricerca individuale: 256
- Interazione con i docenti e i colleghi: 30
- Preparazione dell'elaborato finale: (non è prevista una tesi)

Art. 13.2. Modalità di verifica (esami)

Verifiche degli insegnamenti teorici
- Sessioni d'esame: test somministrato al termine di ogni modulo
- Percentuale della valutazione complessiva: 25%

Verifiche degli insegnamenti con laboratorio
- Sessioni d'esame: verifica somministrata al termine di ogni sessione di laboratorio
- Percentuale della valutazione complessiva: 25%

Verifica finale degli insegnamenti con laboratorio
- Sessioni d'esame finale: 50% della valutazione complessiva.

Art. 14. Attivazione del servizio e utilizzo applicazione Web Storage e WebMail

Allo studente, entro cinque giorni lavorativi dal perfezionamento dell'iscrizione, ovvero dalla data del buon fine del pagamento della retta (1° rata o saldo), saranno assegnati un account e una password (provvisoria) per l'accesso al proprio desktop Aruba su dominio studenti.unisf.eu che gli consentirà di gestire le proprie e-mail, usufruire del materiale didattico (potendolo anche scaricare), organizzare cartelle e rubriche, archiviare messaggi, impostare un calendario ecc. Lo studente, tramite il proprio account, interagirà con la Segreteria Studenti, i docenti e i colleghi del corso. Tramite e-mail, i docenti designati saranno a disposizione dello studente al fine di fornire sintetici chiarimenti ma non per le spiegazioni degli argomenti che, invece, verranno rese esclusivamente nel corso delle lezioni a distanza o in presenza. Il materiale didattico sarà caricato entro due giorni dall'inizio delle attività a distanza. L'account e la password per

Data _____ Firma leggibile dell'aspirante studente_____

l'applicazione Adobe Connect©, che servirà per seguire le lezioni in videoconferenza, saranno forniti all'inizio delle attività didattiche in videoconferenza.

Art. 15. Sede delle lezioni in presenza

Le lezioni in presenza si svolgeranno presso l'Istituto di Scienze Forensi Corporate University, via Leonardo da Vinci n. 5, Corsico (Milano). La sede fisica delle lezioni in presenza potrebbe essere modificata per ragioni logistiche o didattiche non prevedibili, fatta salva la circostanza che, l'eventuale altra sede, sarà comunque in Milano o provincia di Milano.

Art. 16. Consenso pubblicazione foto e video (ex D.lgs. 196/2003 - GDPR 679/16)

Accettando il presente Regolamento, lo studente fornisce il proprio consenso alla pubblicazione sui mezzi di comunicazione dell'Istituto di Scienze Forensi Corporate University, di fotografie e video che lo riprendono nel corso di attività didattiche o extra didattiche insieme ai colleghi di corso.

Art. 17. Direzione del corso

Direttore Scientifico: dr. Ing. Nicola Chemello
Coordinatore: Dr. Francesco Costanzo

Art. 18. Segreteria

Segreteria Studenti Istituto di Scienze Forensi Corporate University
Via Leonardo da Vinci n. 5 - 20094 Corsico (Milano)
Orari di apertura: dal lunedì al venerdì, h. 9,30-13 / 14-16
E-mail: segreteria@unisf.eu
Tel. 02.3672.8310

Data _____ Firma leggibile dell'aspirante studente_____

Art. 19. Piano degli Studi e docenti

Insegnamenti	Crediti	Ore frontali	Ore online
1° fase			
Introduzione alla Computer forensics	5	4	10
Le fasi della produzione della digital evidence			
Principi generali			
Introduzione ai sistemi operativi			
Triage nei casi di ispezione informatica			
Best practice per le acquisizioni informatiche			
La gestione del reperto e la catena di custodia			
Tipologie di acquisizione dei supporti di memorizzazione di massa e volatili			
Esplorazione dei tools open source e tools commerciali per l'acquisizione e l'analisi di supporti di memorizzazione di massa			
Legge 18 marzo 2008, n. 48 del 2008 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica"			
Laboratorio e case study - cosa non fare		12	
2° fase			
Gestione delle immagini forensi	10	2	12
Principali files system (FAT32, NTFS, HFS+, EXTi)			
Data recovery e file carving			
Creazione di una timeline			
Password cracking			
Windows Forensics			
OSX Forensics			
Analisi dei principali Artifacts			
Searching e Indexing			
Hashing e ricerche tramite hash			
Tecniche di ricerca degli elementi di interesse			
Laboratorio e case study - cosa non fare		14	
Audio e video forensics	15	4	28
Acquisizione ed analisi dei tabulati telefonici			
Analisi celle telefoniche			
Mobile forensics			
Best practice per il settore mobile			
Riepilogo su metodologie e strumenti di acquisizione			
Tecniche di Anti-Forensics			
Tool per analisi forensi			
Laboratorio e case study - cosa non fare		18	
Totale Crediti Formativi ISF	**30**	**54**	**50**

Data _____ Firma leggibile dell'aspirante studente_____

Docenza affidata agli Esperti di:
Insegnamento:

SECURCUBE S.R.L.		Computer & Mobile forensics, Cell Site Analysis
AMPED S.R.L.		Video forensics
Marco Perino	Docente UniSF	Audio forensics

Art. 20.1. Insegnamenti e manuali (non compresi nel costo della retta)

Quelli che seguono sono i manuali / libri / risorse web ecc. di riferimento relativi agli insegnamenti dell'Executive Master

Insegnamento	**Manuale**
Audio Forensics	**Forensic Speaker Identification**, Phil Rose, CRC Press, 2003; **Digital multimedia audio forensics: past, present and future**, Zakariah - Khurram Khan - Malik, Springer Link, 2018; **SWGDE Best Practices for Forensic Audio v1-0 / v2-0 / v2-1**, https://www.swgde.org/documents/viewArchivedDocuments
Video Forensics	Link a web: https://github.com/ampedsoftware/digital_video_introduction
Computer Forensics	**EnCase Computer Forensics – The Official EnCE: EnCase Certified Examiner Study Guide, 3rd Edition**, Bunting, Wiley, 2012
Mobile Forensics	**Practical Mobile Forensics - 3rd Edition: A hands-on guide to mastering mobile forensicsfor the iOS, Android and the Windows Phone Platforms**, Tamma - Skulkin - Mahalik - Bommisetty, Packt, 2018

Art. 21. Norme di comportamento all'interno e all'esterno del contesto dell'Istituto

Con l'accettazione del presente Regolamento, lo studente si impegna solennemente ad osservare quanto segue:

1. indossare e mantenere ben visibile il badge di riconoscimento all'interno dell'Istituto, non indossare copricapi durante le lezioni e ricordare il proprio numero di matricola a memoria;
2. avere un atteggiamento non offensivo e rispettoso degli altri e dell'ambiente;
3. evitare atteggiamenti che sviliscano il decoro e la professionalità dell'Istituto sia all'interno che all'esterno di esso;
4. evitare atteggiamenti che precludano il regolare svolgimento delle attività a discapito degli altri studenti e dell'Istituto;
5. Seguire scrupolosamente le disposizioni fornite da docenti e assistenti, dai responsabili dei vari uffici o dai loro delegati;
6. rispettare i colleghi e i docenti;

Data _____ Firma leggibile dell'aspirante studente_____

7. non contestare i docenti, i dirigenti e i loro delegati. Qualsiasi rimostranza in ordine a dissidi con docenti, i dirigenti e loro delegati ovvero con i colleghi, deve essere manifestata alla Direzione dell'Istituto;
8. porre la massima attenzione alla pulizia dei luoghi in cui si svolgono le attività, ivi compresi i servizi igienici, riordinare sedie, mobili, strumenti ecc. al termine delle lezioni;
9. essere puntuale negli impegni assunti (es. orario di inizio delle attività didattiche);
10. mantenere il massimo riserbo sul materiale didattico, sulla tipologia di strumenti o altro materiale presenti presso i laboratori, sulle conoscenze e competenze acquisite nonché su eventuali attività di ricerca o consulenza svolte con i criminalisti professionisti;
11. non divulgare a terzi il materiale didattico e non utilizzarlo per proprie attività esterne all'Istituto;
12. non fornire a terzi, nemmeno ai familiari, la propria password personale;
13. informare tempestivamente la Direzione circa fatti contrari al Regolamento dei quali si è venuti a conoscenza;
14. segnalare immediatamente alla Direzione eventuali anomalie della struttura e degli impianti in cui si tengono le attività didattiche ed "extra", sia all'interno che all'esterno;
15. non lasciare le cose proprie o di proprietà dell'Istituto incustodite. Per le cose personali sottratte e/o smarrite, l'Istituto non ne risponde in alcun caso;
16. essere preciso/a e puntuale nell'assolvimento del pagamento delle rette e degli altri contributi dovuti.

Il mancato rispetto delle norme di cui sopra, sarà soggetto a richiami scritti nei confronti dell'inadempiente. Alla terza infrazione, la Direzione dell'Istituto potrà procedere con l'espulsione dello studente. Al verificarsi della predetta circostanza, la retta sarà comunque dovuta per l'intero corso di studi. Inoltre, qualora dal comportamento (azione od omissione) ne derivasse un serio danno materiale o immateriale all'Istituto, nonché ai colleghi o al personale docente e non docente, l'Istituto avrà facoltà di esperire tutte le azioni legali più opportune.

Art. 22. Impegni assunti dall'Istituto

L'Istituto di Scienze Forensi Corporate University si impegna ad erogare i seguenti servizi allo studente:

1. tutte le attività amministrative, didattiche ed extra didattiche in modo puntuale ed esatto, fatti salvi casi di forza maggiore non prevedibili;
2. contenuti didattici aggiornati e rispondenti alle esigenze del mercato del lavoro;
3. opportune azioni di coesione del gruppo ai fini del raggiungimento degli scopi del corso;
4. attività informative e formative "extra" in modo gratuito ovvero a costi di assoluto favore (restano escluse spese di viaggio, vitto e alloggio).

Art. 23. Attestazioni finali

Alla positiva conclusione dell'Executive Master, saranno rilasciati i seguenti certificati:

- Attestato di Executive Master in Digital forensics & Cyber Security;
- Certificazione degli Studi riportante il programma svolto;
- Il percorso di studi è valido altresì quale percorso formativo e tirocinio professionale (in termini di ore) ai fini dell'iscrizione nella Sezione Criminalisti - Informatici forensi dell'Associazione Nazionale Criminologi e Criminalisti (ass. prof. Iscr. Elenco Ministero dello Sviluppo Economico ai sensi della legge 14 gennaio 2013, n. 4).

Data _____ Firma leggibile dell'aspirante studente_____

Art. 24. Retta di partecipazione

L'importo della retta è indicato nella modulistica di iscrizione.
La retta sarà dovuta per l'intero periodo del corso, anche nel caso in cui lo studente avesse rinunciato alla frequenza dello stesso.
Nella retta è incluso il materiale didattico predisposto dai docenti (slide e/o dispense) ma non i manuali relativi agli insegnamenti (cfr. Piano degli Studi).

Art. 25.1. Rimborsi

Le rette versate non saranno in alcun modo rimborsabili se non per i casi previsti dai contratti sottoscritti o dalla legge.

Art. 25.2. Inadempimento

Il mancato versamento della retta, anche di una sola rata di essa, comporterà l'esclusione da qualsiasi attività didattica e la sospensione di tutti i servizi ad essa connessi.
In caso di rateizzazione della retta, l'inadempimento, anche per un solo ritardato pagamento, comporterà la perdita dei benefici accordati.
Le rette non corrisposte entro le date previste saranno da corrispondere in qualsiasi caso. I ritardi nei pagamenti saranno produttivi di interessi di mora pari al tasso legale.

Corsico (Milano), 18 luglio 2024

Istituto di Scienze Forensi
Il Direttore Generale
Prof. MASSIMO BLANCO

Data _____ Firma leggibile dell'aspirante studente_____