

Università degli Studi di Roma “Tor Vergata”

Dipartimento di Ingegneria Elettronica

*

Corso di formazione in "Security Manager"

*

Realizzato in convenzione con OSDIFE – Osservatorio
Sicurezza e Difesa CBRNe

*

Anno Accademico 2017-2018

Università degli Studi di Roma “Tor Vergata”

Dipartimento di Ingegneria Elettronica

Corso di formazione in "Security Manager"

Realizzato in convenzione con OSDIFE – Osservatorio Sicurezza e Difesa CBRNe

Anno Accademico 2017-2018

Edizione I

Istituzione

E' attivato nell'Anno Accademico 2017-2018 dall'Università degli Studi di Roma "Tor Vergata", Dipartimento di Ingegneria Elettronica, il corso di Formazione in "Security Manager"

Finalità

Obiettivo del Corso di formazione è quello di formare una figura professionale capace di agire trasversalmente nelle sue attività; tale figura pertanto dovrà rappresentare un esperto in materia di sicurezza pubblica e privata, avere un approccio consapevole alla business continuity ed ai processi aziendali ma soprattutto essere in grado di rispondere alle esigenze di security in modo puntuale e concreto, al fine di accrescere la resilienza della struttura a lui affidata.

Nel rispetto di quanto previsto dal D.M. 1 dicembre 2010 n.269 (recante la disciplina delle caratteristiche minime del progetto organizzativo e dei requisiti minimi di qualità degli istituti e dei servizi di cui agli articoli 256-bis e 257-bis del Regolamento di esecuzione del Testo unico delle leggi di pubblica sicurezza, nonché dei requisiti professionali e di capacità tecnica richiesti per la direzione dei medesimi istituti e per lo svolgimento di incarichi organizzativi nell'ambito degli stessi istituti), durante il percorso formativo verranno analizzati tutti i sottosistemi che concorrono a rendere il sistema aziendale efficiente ed efficace tanto in ordinario quanto nella gestione di eventi di straordinario accadimento e che possono minacciare la sicurezza di operatori, dipendenti, ambiente, cittadini e sistema Paese. Saranno oggetto del percorso formativo tutti gli aspetti di security espressione dei doveri del datore di lavoro nei riguardi dei lavoratori (2087 c.c. w D.lgs 81/08) e della garanzia degli stessi di protestare verso terzi, generalmente riconosciuti in capo all'impresa.

A tal proposito quindi, a latere degli scenari di rischio cui può essere associato un rischio fisico e materiale, verranno analizzate le minacce intangibili che possono colpire il patrimonio conoscitivo dell'azienda, i flussi informativi, la protezione e gestione di dati sensibili nonché la comunicazione e l'informazione. Nell'individuazione dei processi di gestione e mitigazione del rischio di security verranno altresì definiti i limiti normativi entro i quali un Security Manager ha la facoltà e la possibilità di agire per garantire la difesa e sicurezza della propria struttura.

Il Risk Management, la valutazione delle vulnerabilità e la definizione delle misure di mitigazione del rischio verranno quindi affrontate tanto da un punto di vista strategico e tattico per la definizione di una politica di security interna quanto da un punto di vista tecnico-operativo, grazie all'individuazione delle tecnologie e strumentazioni oggi esistenti che possono essere un valido supporto al Security Manager per la protezione fisica e materiale dell'azienda.

Al termine del Corso verrà rilasciata apposita certificazione attestante l'ottenimento delle competenze di Security Manager in conformità alla norma UNI 10459:2015 - Funzioni e Profilo del

Professionista della Security Aziendale, in ottemperanza a quanto previsto dal citato Decreto 1° dicembre 2010, n. 269.

Requisiti di ammissione e iscrizione al Corso

Requisito minimo per l'ammissione al Corso è il possesso di un diploma di scuola media superiore o di una laurea triennale e/o specialistica.

Il titolo di accesso deve essere posseduto al momento dell'immatricolazione, prima dell'avvio delle attività formative.

Quota d'iscrizione

La partecipazione è subordinata al versamento di una quota di iscrizione, il cui importo totale è fissato in € 1.500,00 (Euro millecinquecento,00), da corrispondersi in 4 rate di pari ammontare.

Durata

Il Corso ha durata di quattro mesi, per un impegno complessivo di 340 ore, corrispondenti a 20 crediti formativi universitari (CFU), suddivisi tra impegno didattico con docente ed esercitazioni (120 ore), impegno individuale (140 ore), elaborato finale (70 ore) e valutazione finale (10 ore).

È prevista una suddivisione del percorso formativo in 23 moduli per un totale di 12 CFU. A conclusione del Corso i partecipanti dovranno presentare un elaborato individuale al quale, se approvato, verranno riconosciuti 2 CFU.

Per il conseguimento del titolo sarà infine necessario sostenere la prova di valutazione finale che riconoscerà l'acquisizione di un ulteriore CFU.

Articolazione e programma

Il Corso si articola nei seguenti 23 moduli

Insegnamento	Ore	CFU	Acronimo
UNI 10459 – Il Professionista della Security e la Figura del Security Manager	5	0,5	IUS/01 - IUS/03
Attività del Security Manager ed ambiti di applicazione del D.Lgs. 231/01	5	0,5	IUS/01 - IUS/03
Decreto Legislativo 30 giugno 2003, n. 196 - "Codice in materia di protezione dei dati personali"	5	0,5	IUS/01 - IUS/03
Tecniche di identificazione delle sorgenti informative, integrazione delle informazioni, categorizzazione ed analisi dell'informazione	5	0,5	ING-INF/05
Processi di investigazione <ul style="list-style-type: none">• OSINT• TechInt• MasInt/ImInt• CBRNe Intelligence• Due Diligence	10	1	ING-IND/011
La Vigilanza privata e le investigazioni private <ul style="list-style-type: none">• Progettazione e organizzazione	10	1	ING-IND/03

<ul style="list-style-type: none"> • Centrali operative • Sistemi TLC • Mezzi Tecnici 			
Gestione e tutela delle informazioni classificate	5	0,5	ING-INF/05
Nuovi Scenari per la Security	5	0,5	ING-IND/011
Partenariato pubblico/privato e la sicurezza sussidiaria nella gestione della security	5	0,5	ING-IND/35
Problematiche di security delle infrastrutture critiche e relativa legislazione	5	0,5	ING-IND/011
La sicurezza Passiva	5	0,5	ING-IND/011
Sicurezza Perimetrale delle Reti ed Elementi di Crittografia – end to end	5	0,5	ING-IND/01
Materiali e Tecnologie esplosive Dual Use			
Ordigni esplosivi improvvisati	5	0,5	ING-IND/011
La valutazione dei rischi (ISO 31000) <ul style="list-style-type: none"> • Metodologia di identificazione dei pericoli, di quantificazione e valutazione dei rischi di origine criminosa, di definizione dei criteri di accettabilità. Di identificazione delle misure di mitigazione • Procedure, linee guida norme tecniche per la gestione del rischio nel proprio ambito operativo • Metodologie per la valutazione del grado di security nel territorio e nelle comunità ospitanti • Identificazione del rischio prevalente nell'area • Strumenti per valutare l'impatto delle attività di security sul contesto sociale ed economico di riferimento 	10	1	ING-IND/011
Elementi di coordinamento della continuità operativa ("business continuità" e "disaster recovery")	5	0,5	ING-IND/011
Elementi di coordinamento della gestione della crisi (crisis management")	5	0,5	ING-IND/011
Modalità di predisposizione di piani di security	5	0,5	ING-IND/011
Sistemi e tecniche di monitoraggio e "reporting"	5	0,5	ING-IND/011
Tecniche e strumenti di comunicazione (relazione con istituzioni, autorità, forze dell'Ordine, enti locali e stampa)	5	0,5	ING-IND/05
Modalità e gestione dei contratti di security	5	0,5	ING-IND/011
Competenze interdisciplinari <ul style="list-style-type: none"> • Team Working • Gestione finanziaria della security • Program management • Gestione dei conflitti e negoziazione • Relazioni sindacali 	5	0,5	ING-IND/011
TOTALE INSEGNAMENTI FRONTALI	120	12	
Elaborato individuale	70	7	
Valutazione finale	10	1	
TOTALE	200	20	

Calendario delle lezioni

Insegnamento	Data	Docente
UNI 10459 – Il Professionista della Security e la Figura del Security Manager	14/09/2018	Dr. Francesco Di Maio
Attività del Security Manager ed ambiti di applicazione del D.Lgs. 231/01	14/09/2018	Dr. Francesco Di Maio
Decreto Legislativo 30 giugno 2003, n. 196 - "Codice in materia di protezione dei dati personali"	15/09/2018	Dr. Francesco Di Maio
Tecniche di identificazione delle sorgenti informative, integrazione delle informazioni, categorizzazione ed analisi dell'informazione	15/09/2017	Prof. Roberto Mugavero
Processi di investigazione <ul style="list-style-type: none"> • OSINT • TechInt • MasInt/ImInt • CBRNe Intelligence • Due Diligence 	21/09/2018	Prof. Roberto Mugavero
La Vigilanza privata e le investigazioni private <ul style="list-style-type: none"> • Progettazione e organizzazione • Centrali operative • Sistemi TLC • Mezzi Tecnici 	22/09/2018	Prof. Roberto Mugavero
Gestione e tutela delle informazioni classificate	05/10/2018	Dott. Giovanni Villarosa
Nuovi Scenari per la Security	28/09/2018	Prof. Roberto Mugavero
Partenariato pubblico/privato e la sicurezza sussidiaria nella gestione della security	28/09/2018	Prof. Roberto Mugavero
Problematiche di security delle infrastrutture critiche e relativa legislazione	29/09/2018	Ing. Luisa Franchina
La sicurezza Passiva	29/09/2018	Dr. Giovanni Villarosa
Sicurezza Perimetrale delle Reti ed Elementi di Crittografia – end to end	12/10/2018	Ing. Marco Bonola
Materiali e Tecnologie esplosive Dual Use	12/10/2018	Dr. Stefano Scaini
Ordigni esplosivi improvvisati	13/10/2018	Dr. Stefano Scaini
La valutazione dei rischi (ISO 31000) <ul style="list-style-type: none"> • Metodologia di identificazione dei pericoli, di quantificazione e valutazione dei rischi di origine criminosa, di definizione dei criteri di accettabilità. Di identificazione delle misure di mitigazione • Procedure, linee guida norme tecniche per la gestione del rischio nel proprio ambito operativo • Metodologie per la valutazione del grado di security nel territorio e nelle comunità ospitanti • Identificazione del rischio prevalente nell'area 	13/10/2018	Prof. Massimiliano Caramia

<ul style="list-style-type: none"> • Strumenti per valutare l'impatto delle attività di security sul contesto sociale ed economico di riferimento 		
Elementi di coordinamento della continuità operativa ("business continuity" e "disaster recovery")	19/10/2018	Dr. Francesco Di Maio
Elementi di coordinamento della gestione della crisi (crisis management")	19/10/2018	Dr. Francesco Di Maio
Modalità di predisposizione di piani di security	20/10/2018	Dr. Francesco Di Maio
Sistemi e tecniche di monitoraggio e "reporting"	20/10/2018	Dr. Francesco Di Maio
Tecniche e strumenti di comunicazione (relazione con istituzioni, autorità, forze dell'Ordine, enti locali e stampa)	26/10/2018	Dr. Giulia Aubry
Modalità e gestione dei contratti di security	26/10/2018	Dr. Francesco Di Maio
Competenze interdisciplinari <ul style="list-style-type: none"> • Team Working • Gestione finanziaria della security • Program management • Gestione dei conflitti e negoziazione • Relazioni sindacali 	27/10/2018	Dr. Francesco Di Maio
TOTALE INSEGNAMENTI FRONTALI	120	12
Elaborato individuale	70	7
Valutazione finale	10	1
TOTALE	200	20

Valutazioni

L'iscritto dovrà sostenere delle prove intermedie di verifica del profitto. Al termine del corso, l'iscritto dovrà sostenere una prova orale. La Commissione esaminatrice è nominata dal Direttore del Corso ed è composta da 3 membri del corpo docente. La valutazione finale è espressa in trentesimi, tiene conto dei punteggi acquisiti nella precedente verifica a quiz e delle presenze effettive alle lezioni.

Corpo Docente

Il Corpo Docente è composto da Docenti dell'Università degli Studi di Roma "Tor Vergata" o di altri atenei italiani o esteri o di altri organismi nazionali e internazionali e da esperti designati dal Direttore del Corso.

Sede Amministrativa

La sede amministrativa del Corso è presso il Dipartimento di Ingegneria Elettronica dell'Università degli Studi di Roma "Tor Vergata".

Sede delle attività didattiche

La sede delle attività didattiche frontali del Corso è presso le strutture didattiche del Dipartimento di Ingegneria Elettronica dell'Università degli Studi di Roma "Tor Vergata".

Obbligo di frequenza

La frequenza al Corso è obbligatoria e deve essere attestata con le firme degli iscritti. Una frequenza inferiore al 70% (o 80%) delle ore previste comporterà l'esclusione dal Corso e la perdita della quota di iscrizione.

Attestato

Al termine del Corso, a coloro che avranno superato l'esame finale, verrà rilasciato un Attestato di frequenza o formazione e qualificazione professionale secondo le vigenti norme di legge.

Quote e modalità di iscrizione

Per i più meritevoli o per coloro che versino in situazioni di disagio economico, il Consiglio del Corso può deliberare l'attivazione di Borse di Studio e/o l'esenzione totale o parziale dal pagamento del contributo di iscrizione al Corso.

Per coloro che risultino, come attestato da idonea documentazione, essere in situazione di handicap con una invalidità riconosciuta pari o superiore al 66% è previsto l'esonero dal contributo di iscrizione ed il pagamento di soli € 100,00 (Euro cento,00) per l'intero Corso.

Nel caso di esonero parziale dal contributo di iscrizione, o di borse di studio, il 20% dell'intero contributo di iscrizione deve essere comunque versato a favore del bilancio dell'Ateneo per la copertura delle spese generali.

È prevista la possibilità di partecipare a singoli moduli didattici. Per l'iscrizione ai singoli moduli è richiesto lo stesso titolo di studio previsto per l'iscrizione al Corso. Gli oneri di contribuzione per l'iscrizione al singolo modulo sono proporzionali al numero di crediti formativi, dove il costo del singolo credito formativo è fissato a € 150,00 (Euro centocinquanta,00).

In caso di superamento delle prove previste al termine di ciascun modulo, potranno essere riconosciuti i crediti formativi relativi al modulo acquisito e verrà rilasciato un attestato di frequenza con l'indicazione dei crediti formativi maturati.

Contatti e informazioni

Per la segreteria amministrativa contattare:

Simona Ranieri

ranieri@ing.uniroma2.it

Tel. 06 7259 7574

Dipartimento di Ingegneria Elettronica