SEDE DELLA DIDATTICA
E PERIODO DI SVOLGIMENTO

Le lezioni avranno inizio il **14 Ottobre 2011** e si terranno nelle giornate di venerdì (09:00-13:00; 14:00—18:00) e sabato (09:00-13:00).

Le sedi della didattica saranno la facoltà di Giurisprudenza della Università di Roma Tor Vergta o presso le sale formazione in strutture convenzionate al Centro di Roma.

COSTI E MODALITA' DI ISCRIZIONE

Titolo di accesso: Possono presentare domanda di ammissione al corso tutte le persone interessate in possesso di Laurea triennale o specialistica, qualunque sia la disciplina.

La quota di iscrizione, pari ad € 3.800, è pagabile in due rate: la prima di € 2014,62 comprensiva di imposta di bollo entro il 04/10/2011, e la seconda di € 1.800,00 entro il 30.11.2011). Si valuteranno richieste di iscrizione ai singoli moduli.

Sono previste agevolazioni:

Per neolaureati (2010/2011) meritevoli in cerca di prima occupazione: fino al 40% di riduzione della quota di iscrizione;

Per gruppi provenienti da uno stesso Ente, e per dipendenti o associati delle aziende convenzionate: fino al 25% di riduzione della quota di iscrizione.

La preiscrizione avviene attraverso l'invio alla segreteria organizzativa del modulo di preiscrizione compilato, che può essere scaricato sul sito **www.cispa.uniroma2.it** o richiesto alla segreteria organizzativa a

simonetta.bianchini@uniroma2.it .

A seguito della ricezione del modulo verrete contattati per un colloquio orientativo.

Le Preiscrizioni si chiuderanno il 20 Settembre 2011. Seguiranno la valutazione delle domande e l'ammissione. E' previsto un limite di 20 ammessi per Aula; qualora le persone ammesse siano in numero superiore il Consiglio del corso valuterà la possibilità di creazione di ulteriori Aule didattiche fino ad un massimo di 4.

Gli ammessi saranno abilitati alla procedura di immatricolazione sul sito di Ateneo e potranno procedere al pagamento della prima rata entro il 30/09/2011 e completare la procedura ed inviare i documenti richiesti dal bando entro il 04/10/2011.

IN COLLABORAZIONE CON

CENTRO STUDI SERMAS
Security Research and Management School

secur index

CON IL PATROCINIO DI

aias dal 1975 network aias

CONFESERCENTI

aipsa
Associazione Italiana Professionisti Security Aziendale

PRIMAe
privacy management e... dintorni

A.I.PRO.S.

essecome
security&safety

vigilanza
e dintorni

RESPONSABILE SCIENTIFICO

Prof. Luciano Hinna

RESPONSABILE TECNICO—DIDATTICO

Avv. Antonio Serra

antonio.serra@avvocatoserra.it

COORDINAMENTO ESECUTIVO

Dott. Francesco Farina:

francesco.farina@uniroma2.it

SEGRETERIA ORGANIZZATIVA

Simonetta Bianchini:

simonetta.bianchini@uniroma2.it

tel. 0672593876, fax 0672592026

www.cispa.uniroma2.it

CISPA Innovazione per la Pubblica Amministrazione

"Centro Interdipartimentale di Studi sulla Pubblica Amministrazione"
DIPARTIMENTO DI DIRITTO PUBBLICO

Corso di Perfezionamento
in
SECURITY MANAGER

conforme alla norma UNI 10459 del marzo 1995

"funzioni e profilo del professionista della security aziendale"

corso in fase di qualifica da parte del CEPAS

Facoltà di Giurisprudenza
Università degli Studi di Roma
Tor Vergata

CISPA Innovazione per la Pubblica Amministrazione

CORSO DI PERFEZIONAMENTO IN "SECURITY MANAGER"

FINALITA' DEL CORSO

I macrosistemi aziendali si configurano oggi con un patrimonio intangibile di informazioni, dati, conoscenze, processi e sistemi, che è necessario presidiare attentamente con nuove sensibilità e dinamiche operative.

Questi nuovi scenari tecnici, economici e di mercato, che configurano un mondo in crescita esponenziale, condizionato dagli incessanti sviluppi tecnologici e dalla globalizzazione, sempre più interconnesso e interdipendente, influenzano fortemente la professione del *Security Manager* e richiedono un modo nuovo di presidiare rischi e minacce a 360 gradi. Ai rischi tradizionali di sicurezza fisica e logica si intrecciano nuove e forti esigenze di sicurezza, *privacy* e *governance* che modificano il perimetro delle attività della *security* ed ampliano significativamente le responsabilità del *security manager*.

In questo contesto è necessario che il *security manager* abbia una buona conoscenza del business e rappresenti una funzione che è parte integrante di tutto il sistema, che opera in modo trasversale nei processi aziendali e che è percepita come funzione di supporto.

A partire da queste considerazioni nasce l'idea di creare un corso di perfezionamento universitario in grado di affrontare le problematiche della sicurezza secondo una molteplicità di dimensioni, una pluralità di discipline, e, conseguentemente, avvalendosi di specifiche competenze declinate nei diversi campi della scienza e della ricerca.

Tali strumenti devono necessariamente essere in linea con i progressi in ambito tecnologico, ingegneristico ed avvalersi di persone con competenze culturali e umanistiche ma anche più prettamente inerenti la sicurezza, oltre a supportare la previsione e il contrasto di accadimenti (anche catastrofici, o dovuti a eventi naturali o accidentali).

ARTICOLAZIONE DEL CORSO

Il Corso si sviluppa con un impegno didattico di 375 ore, di cui 132 di didattica frontale in aula, equamente suddivise tra teoria ed esercitazioni e suddivise in 5 moduli, per un totale di **15 crediti formativi (CFU).**

Al termine del percorso didattico i partecipanti dovranno affrontare uno stage della durata di 130 ore, da svolgersi presso organizzazioni esterne convenzionate, con lavoro finalizzato alla comprensione ed applicabilità in contesti operativi complessi.

IL PROGRAMMA FORMATIVO

Il programma del corso, è finalizzato a trasferire conoscenze e competenze ai futuri "security manager",

il Risk Management: Introduzione all'analisi dei rischi; ; Gli scenari di rischio; Introduzione alle strategie di gestione e controllo dei rischi; Identificazione e valutazione dei rischi; Rischio di compliance; Strategie di gestione dei rischi e strumenti di controllo; Enterrprise risk management; il Crisis management

Lo Scenario di Riferimento, la valutazione e la presa in carico dei rischi: evoluzione dei rischi: dal rischio fisico al rischio strategico; riferimenti legislativi della security; la strutturazione della funzione di security e le sue interrelazioni interne ed esterne; la collocazione organizzativa, la missione ed il ruolo della funzione de security;

l'intelligence preliminare: analisi del territorio, analisi di azienda, analisi del contesto competitivo, analisi dei fenomeni; l'analisi dei rischi: individuazione e valutazione;l'analisi della vulnerabilità; le tipologie di rischi in un approccio integrato di tutela aziendale: ambiente, safety security; l'assunzione ed il trasferimento del rischio;valutazione dei rischi alla politica d'intervento: analisi costi/benefici; il processo decisionale per la scelta delle opzioni de security; le tecnologie a supporto dell'Homeland security.

Governo della Security: La risposta organizzativa ai rischi di security: l'mpresa e la Qualità; le certificazioni dei Sistemi e delle Professionalità; le interrelazioni tra Security e Qualità: esame degli elementi d'analogia e di differenza; le norme ISO 9000 e la loro evoluzione: le prospettive per la certificazione della Security; dalle scelte strategiche alla pianificazione aziendale della Security; il modello di pianificazione: esempi specifici; Il sistema di gestione della Security aziendale secondo UNI EN ISO 9004; la Security nei contratti esterni - la Security e la normativa del lavoro; la formalizzazione e la diffusione delle procedure di Security; la Security e la sicurezza privata: la selezione, l'utilizzo e la gestione dei servizi dis sorveglianza; l'organizzazione della sicurezza pubblica e privata; la sicurezza come sistema integrato: definizione di una Security policy; la sicurezza del "top management"; La tutela delle informazioni aziendali - la sicurezza del patrimonio informativo.

Sicurezza delle informazioni e diritto della sicurezza: sicurezza dei sistemi d'elaborazione isolati: tipologie di attacco, tecniche di difesa HW e SW; la sicurezza dei sistemi di telecomunicazioni; la tutela delle informazioni; la tutela dei dati personali in applicazione del Dlgs 196/03 sulla "privacy"; la sicurezza delle basi di dati: autorizzazioni, piani di backup e procedure di disaster recovery, meccanismi di tracing e di auditing; la sicurezza dei sistemi distribuiti: controllo dell'accesso, tecniche di tracing e di auditing, firewall per l'interconnessione con la rete Internet, ecc..;

Elementi di Organizzazione aziendale e risposte operative ai rischi di Security: l'attuazione del sistema di gestione sella Security; contenuti/raccomandazioni/ responsabilità nella realizzazione delle azioni/ pianificazione/revisione e aggiornamento periodico; la valutazione costi/benefici e la valutazione della performance del servizio di Security; il budget della Security: costi operativi di loss prevention/costi di loss mitigation; convalida delle procedure operative; il "crisis managementt" esperienze ed esercitazioni; l'auditing: uno strumento di garanzia per la gestione della Security/il Security auditing e la norma UNI EN ISO 19011; l'intelligence aziendale e la Business Security; le relazioni istituzionali; le prospettive verso la sicurezza del sistema paese.

LA VALUTAZIONE DEL PROFITTO

L'articolazione del corso prevederà prove intermedie di verifica del profitto alla fine di ciascun modulo ed una prova di valutazione finale delle conoscenze acquisite.

L'ammissione alla prova finale è subordinata allo svolgimento di tutte le prove intermedie di verifica, e vi saranno ammessi solo i partecipanti, in possesso di tutti i requisiti di accesso al corso, che in caso di esito positivo, conseguiranno il perfezionamento.

I DOCENTI

L.Accardi; G.Andrei; C.Bellinzona; G.Bianchi; S.Cipriano; G.Cipolletta; G.Detoni; F.DelConte; R. De Sortis; C.Franchini; A.Gentili; L.Hinna; F.Monteduro; A.Fazzari; A.Limone; A.Manfredini; M.Marrocco; L.Norsa; B.Pellero; A.Salice; F.Sansone; A.Serra; E.Tricarico;