PROGRAMMA DEL CORSO DI INNOVATION & CYBERSECURITY MANAGEMENT PER LA PA

SETTORE SCIENTIFICO

SECS-P/08 (ECON-07/A)

CFU

6

OBIETTIVI FORMATIVI

Nella cornice di un più ampio e globalizzato macroambiente di carattere economico, politico-istituzionale, tecnologico e sociodemografico, l'insegnamento si propone di affrontare il tema della Innovation & Cybersecurity Management Per La Public Administration.

Il corso analizza i fondamenti teorici, le metodologie e le modalità di applicazione della gestione dell'innovazione e sicurezza informatica per l'amministrazione pubblica nonché dei flussi strategici. Tale obiettivo è raggiunto tramite un'attenta analisi delle tematiche relative la digitalizzazione, l'innovazione e sicurezza della P.A.

Gli argomenti del corso saranno trattati facendo ampio riferimento ai contributi più rilevanti della dottrina scientifica di settore nazionale ed internazionale e tenendo conto, al tempo stesso, delle best practice consolidate. Coerentemente con la declaratoria ministeriale relativa al Settore Scientifico Disciplinare, il corso si propone di perseguire i seguenti obiettivi formativi:

1. Inquadrare il tema della innovation and cybersecurity management per la public administration dal punto di vista teorico, alla luce dei più importanti contributi scientifici.

2. Descrivere i principali approcci di integrazione nelle decisioni strategiche alla base della innovazione e sicurezza della p.a

3. Comprendere L'organizzazione Aziendale Del Cybersecurity Management Della P.A.

4. Conoscere lo stato dell'arte in tema di innovazione e gestione della sicurezza informativa per la pubblica amministrazione

RISULTATI DI APPRENDIMENTO ATTESI

- Conoscenza e capacità di comprensione

Completato il corso, gli studenti saranno in grado di conoscere e comprendere problemi aziendali di ampia natura. Le conoscenze saranno trasferite agli studenti adottando un'articolata prospettiva di analisi, finalizzata a:

comprendere i fondamenti teorici ed i campi applicativi della innovazione e gestione della Cybersecurity per la Pubblica Amministrazione (Ob.1);

conoscere i concetti base della gestione strategica della sicurezza informatica per la Pubblica Amministrazione (Ob.2);

comprendere e valutare lo stato dell'arte in tema di innovazione e gestione della sicurezza informativa per la pubblica amministrazione (Ob.3);

conoscere la digitalizzazione, l'Innovazione e la Sicurezza nella PA per garantire la sicurezza dei dati pubblici e dei servizi digitali (ob. 4);

comprendere il mondo del cyberspazio da una prospettiva criminale. Saper riconoscere la natura delle minacce digitali e l'importanza delle contromisure, inclusa la prevenzione, l'individuazione e l'applicazione della legge nell'era digitale (ob.5).

- Capacità di applicare conoscenza e comprensione

L'analisi della teoria, supportata anche da verifiche empiriche nella forma di esercitazioni e casi aziendali, permetterà agli studenti di poter acquisire un approccio professionale e di possedere competenze adeguate a ideare e sostenere argomentazioni o per risolvere criticità nel modo corretto. Agli studenti sarà dato modo, in particolare, di acquisire metodi per applicare le teorie attraverso un'applicazione pratica, finalizzata a: conoscere le principali caratteristiche e funzioni alla base dei sistemi di innovazione e sicurezza per la Pubblica Amministrazione (Ob.2); comprendere le strategie raggiunte per migliorare la sicurezza della Pubblica Amministrazione valutandone impatto, validità ed efficacia (Ob.2).

- l'Autonomia di giudizio

Il corso ha l'obiettivo di incoraggiare gli studenti a maturare un proprio approccio critico ai fenomeni gestionali, promuovendo l'autonomia di giudizio attraverso l'analisi di teorie, esercitazioni e casi empirici. Al termine del corso, gli studenti avranno maturato la capacità di raccogliere e interpretare i dati ritenuti utili a determinare giudizi autonomi, inclusa la riflessione su temi sociali, scientifici o etici. Agli studenti, in particolare, saranno esposte le principali criticità che possono palesarsi nell'ambito della soluzione dei problemi relativi all'ambito di applicazione dell'intelligenza artificiale nel campo della ricerca sociale, lasciando opportuno spazio a riflessioni critiche autonome in merito a:

Le teorie riguardanti la trasformazione digitale all'interno della Pubblica Amministrazione (Ob.1);

conoscere i concetti base della gestione strategica della sicurezza informatica per la Pubblica Amministrazione (Ob.2);

comprendere le strategie raggiunte per migliorare la sicurezza della Pubblica Amministrazione valutandone impatto, validità ed efficacia conoscere i concetti base della gestione strategica della sicurezza informatica per la Pubblica Amministrazione (Ob. 3).

comprendere come la digitalizzazione stia rivoluzionando la Pubblica Amministrazione. Esaminando il modo in cui le nuove tecnologie migliorano l'efficienza e i servizi per i cittadini, analizzando al contempo le sfide di sicurezza e le strategie necessarie per proteggere i dati e le infrastrutture digitali. Il focus è sull'equilibrio tra innovazione e cybersecurity (Ob.4);

Saper analizzare il cybercrime in tutte le sue forme, studiando le tecniche usate dai criminali informatici, dal furto di dati al cyberterrorismo. L'apprendimento si concentra sulle minacce digitali e sull'importanza di strategie di prevenzione, identificazione e risposta legale per proteggere individui e organizzazioni nell'era digitale (Ob.5).

- l’Abilità comunicative

Al termine del corso, gli studenti avranno acquisito specifiche competenze con riferimento alla capacità elaborare e di comunicare informazioni, idee, problemi e soluzioni a interlocutori specialisti e non specialisti. In particolare, il corso si propone di stimolare la capacità comunicativa degli studenti con riferimento a temi molto eterogenei tra loro, ma allo stesso tempo estremamente interdipendenti, favorendo quindi l’elaborazione di una comunicazione sintetica e integrata riguardo:

Confini, Ambiti E Contesti Di Analisi Del Cyberspazio (Ob.1);

Il Diritto Di Accesso A Internet, La Sovranità Nella Rete E Le Finalità Degli Over The Top (Ob.2)

Gestire La Liason Tra PA E Cybersecurity Management (Ob.2-3)

Cloud Computing-IA ACT- &Digitalizzazione, innovazione e sicurezza nella PA (Ob.4)

Cyberspace e cybercrime: la nuova dimensione digitale del crimine (Ob.5)

acquisizione ed elaborazione delle informazioni utili a descrivere ed interpretare i fenomeni innovazione e sicurezza più comuni (Ob.1-2); individuazione dei modi e le forme attraverso cui l’uso della tecnologia può favorire ed accelerate il rinnovamento organizzativo e strategico della Pubblica Amministrazione (Ob.2-3)

Digitalizzazione, Innovazione e Sicurezza nella PA (ob. 4)

Riguarda la trasformazione della Pubblica Amministrazione (PA) attraverso la tecnologia. La comprensione delle sfide e delle strategie per garantire la sicurezza dei dati pubblici e dei servizi digitali. L'attenzione è rivolta all'applicazione pratica della tecnologia nel settore pubblico, bilanciando i benefici dell'innovazione con la necessità di una robusta cybersecurity.

Cyberspazio e Cybercrime: La Nuova Dimensione Digitale del Crimine (ob. 5)

Questo obiettivo esamina il mondo del cyberspazio da una prospettiva criminale. Sono analizzati i vari tipi di cybercrime, dal furto di dati e frodi al cyberterrorismo. Il percorso di apprendimento coprirà gli strumenti e le tecniche usate dai cybercriminali, così come l'impatto che questi crimini hanno su individui, aziende e società. L'obiettivo è comprendere la natura delle minacce digitali e l'importanza delle contromisure, inclusa la prevenzione, l'individuazione e l'applicazione della legge nell'era digitale.

PREREQUISITI

“Non sono richieste conoscenze preliminari”

ATTIVITÀ DI DIDATTICA EROGATIVA (TEL-DE)

Le attività di Didattica Erogativa consistono, per ciascun CFU, nell'erogazione di 5 videolezioni della durata di circa 30 minuti. A ciascuna lezione sono associati:

- una dispensa (PDF) di supporto alla videolezione oppure l’indicazione di capitoli o paragrafi di un e-book di riferimento, scelto dal docente tra quelli liberamente consultabili in piattaforma da studentesse e studenti;

un questionario a risposta multipla per l’autoverifica dell’apprendimento.

ELENCO VIDEOLEZIONI

Il programma didattico è articolato in 30 lezioni suddivise in 5 moduli.

ELENCO LEZIONI/MODULI:

DIGITALIZZAZIONE, INNOVAZIONE E SICUREZZA DELLA P.A

1.CYBERSPAZIO: CONFINI, AMBITI E CONTESTI DI ANALISI

2.CYBERSECURITY E RISK MANAGEMENT: L’ANALISI DI IMPATTO R.I.D.

3.BIG DATA E DECISION MAKING: IL TRASFERIMENTO DELLA SOVRANITÀ DAL PUBBLICO AL PRIVATO

4.LA CRISI DI SOVRANITÀ: DALLE MULTINAZIONALI AL RUOLO DEGLI OVER THE TOP

5.IL DIRITTO DI ACCESSO A INTERNET, LA SOVRANITÀ NELLA RETE E LE FINALITÀ DEGLI OVER THE TOP

6.L'EVOLUZIONE DELLA GOVERNANCE ITALIANA PER L'INNOVAZIONE DELLA P.A.

SICUREZZA INFORMATICA, TRA BUSINESS INTELLIGENCE ED INNOVAZIONE

7.INTERNET OF THINGS

8.L'INTELLIGENZA ARTIFICIALE

9.BITCOIN - BLOCKCHAIN E CRYPTOCURRENCIES

10.LA PATRIMONIALIZZAZIONE DEI DATI: IL NUOVO MERCATO DIGITALE

11.LE NUOVE TECNOLOGIE

12.SUPREMAZIA AI SIGNIFICA SOVRANITA' DIGITALE E DEMOCRAZIA DIGITALE

GESTIRE LA LIASON TRA PA E CYBERSECURITY MANAGEMENT

13.L’APPROCCIO FISCALE ALLA NUOVA DIGITAL ECONOMY

14.DATA GOVERNANCE: LA RILEVANZA DELLA GESTIONE DEL DATO A LIVELLO DELLA SINGOLA IMPRESA

15.IL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA E LA PIANIFICAZIONE STRATEGICA PER LA CYBERSECURITY

16.COMPETENZE E CONOSCENZE PER IL DIGITALE

17.L'EVOLUZIONE DELLA GOVERNANCE ITALIANA PER L'INNOVAZIONE DELLA P.A.

18.IL PIANO DI INVESTIMENTI E LA VALUATZIONE ECONOMICO/FINANZIARIA PER LE INNOVAZIONI CYBERSECURITY

CLOUD COMPUTING-IA ACT- &DIGITALIZZAZIONE, INNOVAZIONE E SICUREZZA NELLA PA

19.IL CLOUD COMPUTING

20.INTELLIGENZA ARTIFICIALE-(IA) : REGOLAMENTAZIONE E PROFILI GIURIDICI DELL'INTELLIGENZA

21.NORMATIVA SULL IA: LA REGOLAMENTAZIONE EUROPEA SULL'INTELLIGENZA ARTIFICIALE "AI ACT"

22.LA NORMATIVA NAZIONALE SULL'INTELLIGENZA ARTIFICIALE

23.APPALTI PUBBLICI E INTELLIGENZA ARTIFICIALE

24.LE MISURE DEL PNRR ITALIA DIGITALE 2026: M1C1: DIGITALIZZAZIONE, INNOVAZIONE E SICUREZZA NELLA PA

CYBERSPACE E CYBERCRIME: LA NUOVA DIMENSIONE DIGITALE DEL CRIMINE

25. IL CYBERSPACE: LA QUINTA DIMENSIONE DELLA CONFLITTUALITA? E IL CYBERCRIME

26.IL QUADRO NORMATIVO ITALIANO IN MATERIA DI CYBERCRIME: EVOLUZIONE E SFIDE ATTUALI

27. IL DARK WEB

28. ANALISI DEI TRATTI CARATTERISTICI DEL RANSOMWARE NEL CONTESTO DELLA CYBERSECURITY

29 CRIME AND CRYPTOCURRENCIES

30. IL CYBER MONEYLAUNDERING

ATTIVITÀ DIDATTICA INTERATTIVA (TEL-DI)

Le attività di Didattica Interattiva (TEL-DI) consistono, per ciascun CFU, in 2 ore erogate in modalità sincrona su piattaforma Class, svolte dal docente anche con il supporto del tutor disciplinare, e dedicate a una o più tra le seguenti tipologie di attività:

- sessioni live, in cui il docente guida attività applicative, stimolando la riflessione critica e il confronto diretto con gli studenti tramite domande in tempo reale e discussioni collaborative;
- webinar interattivi, arricchiti da sondaggi e domande dal vivo, per favorire il coinvolgimento attivo e la co-costruzione della conoscenza;
- lavori di gruppo e discussioni in tempo reale, organizzati attraverso strumenti collaborativi come le breakout rooms, per sviluppare strategie di problem solving e il lavoro in team;
- laboratori virtuali collettivi, in cui il docente guida esperimenti, attività pratiche o l'analisi di casi di studio, rendendo l'apprendimento un'esperienza concreta e partecipativa.

Tali attività potranno essere eventualmente supportate da strumenti asincroni di interazione come per esempio:

- forum;
- wiki;
- quiz;
- glossario.

Si prevede l’organizzazione di almeno due edizioni di didattica interattiva sincrona nel corso dell’anno accademico.

Si precisa che il ricevimento degli studenti, anche per le tesi di laurea, non rientra nel computo della didattica interattiva.

TESTI CONSIGLIATI

Pur precisando che ai fini della preparazione dei candidati e della valutazione in sede d'esame sarà sufficiente il materiale didattico fornito dal docente, per ulteriori approfondimenti di carattere volontario rispetto ai temi trattati, si consiglia di fare riferimento alla bibliografia contenuta in calce alle dispense e, principalmente, al seguente libro di testo:

- Statistica per le decisioni aziendali, Seconda edizione, Biggieri et al, 2023 - ISBN9788891931924 – Pearson.

- Sistemi informativi aziendali, Terza edizione, Pighin & Marzona, 2018 - ISBN9788891911872 – Pearson.

MODALITÀ DI VERIFICA DELL’APPRENDIMENTO

L’esame può essere sostenuto sia in forma scritta che in forma orale. L’esame orale consiste in un colloquio con la Commissione sui contenuti dell’insegnamento. L’esame in forma scritta consiste nello svolgimento di un test composto da 31 domande. Per ogni domanda lo studente deve scegliere una delle 4 possibili risposte. Solo una risposta è corretta e, in caso di risposte errate o mancanti, non sarà attribuita alcuna penalità. Rispondendo correttamente a tutte le 31 domande, si conseguirà la lode.

Oltre alla prova d’esame finale, il percorso prevede attività di didattica interattiva sincrona e prove intermedie che consentono alle studentesse e agli studenti di monitorare il proprio apprendimento, attraverso momenti di verifica progressiva e consolidamento delle conoscenze.

La partecipazione alle attività di didattica interattiva sincrona consente di maturare una premialità fino a 2 punti sul voto finale, attribuiti in funzione della qualità della partecipazione alle attività e dell’esito delle prove.

Per accedere alle prove intermedie è necessario aver seguito almeno il 50% di ogni ora di didattica interattiva.

Le prove intermedie possono consistere in un test di fine lezione o nella predisposizione di un elaborato. Le prove intermedie si considerano superate avendo risposto correttamente ad almeno l’80% delle domande di fine lezione. In caso di prove intermedie che prevedano la redazione di un elaborato, il superamento delle stesse ai fini della premialità sarà giudicata dal docente titolare dell’insegnamento.

I punti di premialità, previsti per le prove intermedie, sono sommati al voto finale d’esame solo se la prova d’esame è superata con un punteggio pari ad almeno 18/30 e possono contribuire al conseguimento della lode.

Le modalità d’esame descritte sono progettate per valutare il grado di comprensione delle nozioni teoriche e la capacità di applicazione delle stesse e consentiranno di valutare il livello di competenza e l’autonomia di giudizio maturati dalla studentessa e dallo studente. Le abilità di comunicazione e la capacità di apprendimento saranno valutate anche attraverso le interazioni dirette che avranno luogo durante la fruizione dell’insegnamento.

OBBLIGO DI FREQUENZA

A studentesse e studenti viene richiesto di partecipare ad almeno il 70% dell’attività di didattica erogativa (70% della TEL-DE).

RECAPITI

michelegabriele.cristiano@unipegaso.it