PROGRAMMA DEL CORSO DI INNOVATION & CYBERSECURITY MANAGEMENT PER LA PA

SETTORE SCIENTIFICO

SECS-P/08

CFU

6

OBIETTIVI FORMATIVI PER IL RAGGIUNGIMENTO DEI RISULTATI DI APPRENDIMENTO PREVISTI NELLA SCHEDA SUA

/**/
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).

- 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).

- 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)

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)

MODALITÀ DI VERIFICA DELL'APPRENDIMENTO

/**/
L'esame può essere sostenuto sia in forma scritta che in forma orale.

Gli appelli orali sono previsti nella sola sede centrale. L'esame orale consiste in un colloquio con la Commissione sui contenuti del corso. L'esame scritto consiste nello svolgimento di un test con 30 domande. Per ogni domanda lo studente deve scegliere una di 4 possibili risposte. Solo una risposta è corretta.

Sia le domande orali che le domande scritte sono formulate per valutare il grado di comprensione delle nozioni teoriche e la capacità di ragionare utilizzando tali nozioni. Le domande sulle nozioni teoriche consentiranno di valutare il livello di comprensione. Le domande che richiedono l'elaborazione di un ragionamento consentiranno di valutare il livello di competenza e l'autonomia di giudizio maturati dallo studente.

Le abilità di comunicazione e le capacità di apprendimento saranno valutate ance attraverso le interazioni dirette tra docente e studente che avranno luogo durante la fruizione del corso (videoconferenze ed elaborati proposti dal docente).

RECAPITI

/**/

OBBLIGO DI FREQUENZA

/**/
Obbligatoria online. Ai corsisti viene richiesto di visionare almeno l'80% delle videolezioni presenti in piattaforma.

ATTIVITÀ DI DIDATTICA INTERATTIVA (DI)

/**/
Le attività di Didattica interattiva consistono, per ciascun CFU, in un'ora dedicata a una o più tra le seguenti tipologie di attività:

- Redazione di un elaborato
- Partecipazione a una web conference
- Partecipazione al forum tematico
- Lettura area FAQ
- Svolgimento delle prove in itinere con feedback

ATTIVITÀ DIDATTICA EROGATIVA (DE)

/**/
Le attività di didattica erogativa consistono, per ciascun CFU, nell'erogazione di 6 videolezioni corredate di testo e questionario finale.

Il format di ciascuna videolezione prevede il video registrato del docente che illustra le slide costruite con parole chiave e schemi esemplificativi.

Il materiale testuale allegato a ciascuna lezione corrisponde a una dispensa (PDF) composta da almeno 10 pagine con le informazioni necessarie per la corretta e proficua acquisizione dei contenuti trattati durante la lezione.

TESTO CONSIGLIATO

/**/
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.

AGENDA

In Informazioni Appelli nella home del corso per ogni anno accademico vengono fornite le date degli appelli.

PROGRAMMA DIDATTICO: ELENCO VIDEOLEZIONI/MODULI

Il programma didattico è articolato in 36 lezioni suddivise in 6 moduli.

ELENCO LEZIONI/MODULI:

MODULO 1: DIGITALIZZAZIONE, INNOVAZIONE E SICUREZZA DELLA P.A

CYBERSPAZIO: CONFINI, AMBITI E CONTESTI DI ANALISI

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

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

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

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

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

MODULO 2: IL PROCESSO DI TRASFORMAZIONE DELLA PA

LE TEORIE MANAGERIALI DELLA PA

LE PREMESSE NORMATIVE

IL QUADRO DI RIFERIMENTO EUROPEO

IL PERCORSO ITALIANO

IL CONTESTO SOCIO-ECONOMICO E LE TECNOLOGIE EMERGENTI

IL DECENNIO DIGITALE: COME SI POSIZIONA L'ITALIA

MODULO 3: SICUREZZA INFORMATICA, TRA BUSINESS INTELLIGENCE ED INNOVAZIONE

INTERNET OF THINGS

L'INTELLIGENZA ARTIFICIALE

BITCOIN - BLOCKCHAIN E CRYPTOCURRENCIES

LA PATRIMONIALIZZAZIONE DEI DATI: IL NUOVO MERCATO DIGITALE

LE NUOVE TECNOLOGIE

SUPREMAZIA AI SIGNIFICA SOVRANITA' DIGITALE E DEMOCRAZIA DIGITALE

MODULO 4: GESTIRE LA LIASON TRA PA E CYBERSECURITY MANAGEMENT

L’APPROCCIO FISCALE ALLA NUOVA DIGITAL ECONOMY

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

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

COMPETENZE E CONOSCENZE PER IL DIGITALE

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

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

MODULO 5: CLOUD COMPUTING & BLOCKCHAIN

IL MONDO DIGITALE NELLA NUVOLA: IL CLOUD COMPUTING

INTELLIGENZA ARTIFICIALE (IA): IL RAPPORTO TRA UOMO E MACCHINA

DIRITTO DELL’INTELLIGENZA ARTIFICIALE: LA REGOLAZIONE EUROPEA E L’ARTIFICIAL INTELLIGENCE ACT

L’UTILIZZO DI ALGORITMI E INTELLIGENZA ARTIFICIALE NELL’ATTIVITÀ DELLA PUBBLICA AMMINISTRAZIONE

DISTRIBUTED LEDGER TECHNOLOGIES (DLT) E BLOCKCHAIN: CARATTERISTICHE TECNICHE

BLOCKCHAIN: DIRITTO E STRATEGIE

MODULO 6: PUBBLICA AMMINISTRAZIONE DIGITALE & REATI INFORMATICI

SOCIETÀ TECNOLOGICA E ISTITUZIONI PUBBLICHE: LA PUBBLICA AMMINISTRAZIONE DIGITALE E APERTA

I DIRITTI DIGITALI DEI CITTADINI E LE RESPONSABILITÀ DELLE PUBBLICHE AMMINISTRAZIONI

LA GOVERNANCE DIGITALE

ELEMENTI DI DIRITTO PENALE DELL’INFORMATICA: CYBERSECURITY E CYBERCRIMES

I REATI INFORMATICI NELL’ORDINAMENTO GIURIDICO ITALIANO

IL PHISHING