MINISTERUL EDUCAŢIEI ŞI CERCETĂRII
UNIVERSITATEA OVIDIUS DIN CONSTANŢA
Aleea Universităţii, nr.1, Campus, Corp A, cod 900470 Constanța, România
Tel./Fax: +4 0241 606.407 / +4 0241 606.467
E-mail: rectorat@univ-ovidius.ro - Web page: www.univ-ovidius.ro

**Facultatea: Matematică și Informatică**
**Domeniul de masterat: Informatică**
**Programul de studii universitare de masterat: Securitate cibernetică și învățare automată (în limba engleză)**
**Forma de învățământ: cu frecvență**

# CONCORDANȚA DINTRE MISIUNEA ŞI OBIECTIVELE PROGRAMULUI DE STUDII CYBER SECURITY AND MACHINE LEARNING (SECURITATE CIBERNETICĂ ŞI ÎNVĂȚARE AUTOMATĂ) ŞI OCUPAȚIILE DECLARATE CONFORM RNCIS

| UNIVERSITATEA „OVIDIUS" DIN CONSTANȚA<br>FACULTATEA DE MATEMATICĂ ŞI INFORMATICĂ | |
|---|---|
| Domeniul fundamental: | Matematică și științe ale naturii |
| Domeniul de masterat: | INFORMATICĂ |
| Ciclu de studii: | MASTER |
| Programul de studii: | CYBER SECURITY AND MACHINE LEARNING (SECURITATE CIBERNETICA ŞI ÎNVĂȚARE AUTOMATA) |
| Durata studiilor: | 2 ani |
| Forma de învățământ: | cu frecvență (IF) |

## 1. MISIUNEA ŞI OBIECTIVELE PROGRAMULUI DE STUDII:

Programul de master Securitate cibernetică și învățare automată/Cyber Security and Machine Learning din cadrul domeniului Informatică are ca scop pregătirea specialiştilor în două domenii importante ale informaticii: cel al securității informatic / cibernetice şi cel al învățării automate.
Programul vizează crearea unor specialiști cu înaltă pregătire în asigurarea protecției sistemelor de calcul și a sistemelor informatice, protecției datelor, administrării rețelelor de calculatoare, dezvoltării de software specific şi dezvoltării sistemelor cu inteligență artificială pentru cele mai diverse arii de aplicaţie, utilizând cele mai recente tehnologii din domeniul învățării automate.

## 2. RNCIS – OCUPAȚII CARE POT FI PRACTICATE PE PIAȚA MUNCII:

Cod COR: 251402 / Denumire COR: Specialist in proceduri si instrumente de securitate a sistemelor informatice

Aleea Universităţii, nr.1, Campus, Corp A, cod 900470 Constanța, România
Tel./Fax: +4 0241 606.407 / +4 0241 606.467
E-mail: rectorat@univ-ovidius.ro - Web page: www.univ-ovidius.ro

# CONCORDANȚA DINTRE MISIUNEA ŞI OBIECTIVELE PROGRAMULUI DE STUDII CYBER SECURITY AND MACHINE LEARNING (SECURITATE CIBERNETICĂ ŞI ÎNVĂȚARE AUTOMATĂ) ŞI OCUPAȚIILE DECLARATE CONFORM RNCIS

**Competențe ESCO pentru ocupația** *Specialist in proceduri si instrumente de securitate a sistemelor informatice* **(COR 251402/ESCO 2529.5)**
https://www.anc.edu.ro/rnc/competente-esco

| Cunoștințe | Abilități/Competențe | Responsabilitate & autonomie |
|---|---|---|
| 1. Tehnici de recuperare TIC<br>2. Securitate cibernetică<br>3. Politică internă de gestionare a riscurilor<br>4. Reziliență organizațională<br>5. Inginerie de securitate<br>6. Cele mai bune practici pentru backup-ul sistemului<br>7. Riscuri de securitate a rețelelor TIC<br>8. Modele de calitate a proceselor TIC<br>9. Siguranța TIC<br>10. Cerințe ale utilizatorilor sistemului TIC<br>11. Modelarea proceselor de afaceri<br>12. Securitatea și conformitatea în cloud<br>13. Principii de hacking etic | C1. Capacitatea de a implementa gestionarea riscurilor in TIC: Dezvolta si implementează proceduri pentru identificarea, evaluarea, tratarea si atenuarea riscurilor TIC, Analizează si gestionează riscurile si incidentele de securitate, Recomanda masuri de îmbunătățirea a strategiei de securitate digitala.<br>C2. Capacitatea de a dezvolta strategia de securitate a informațiilor, pentru a maximiza integritatea informatiilor, disponibilitatea si confidentialitatea datelor.<br>C3. Capacitatea de a conduce exercitii de recuperare a datelor in urma dezastrelor in functionarea sau securitatea sistemelor TIC, cum ar fi în ceea ce priveste recuperarea datelor, protectia identitatii si a informatiilor si masurile | Absolventul își asumă responsabilitatea pentru coordonarea proceselor de identificare și evaluare a riscurilor TIC, acționând autonom în luarea deciziilor privind măsurile de atenuare și strategia de răspuns la incidente.<br>Elaborează independent politici și strategii de securitate la nivel organizațional, asigurând integritatea, confidențialitatea și disponibilitatea datelor, în conformitate cu standardele internaționale.<br>Planifică, organizează și conduce autonom exerciții de simulare și recuperare, asumându-și responsabilitatea pentru refacerea sistemelor TIC și pentru |

Aleea Universităţii, nr.1, Campus, Corp A, cod 900470 Constanța, România
Tel./Fax: +4 0241 606.407 / +4 0241 606.467
E-mail: rectorat@univ-ovidius.ro - Web page: www.univ-ovidius.ro

| | |
|---|---|
| care trebuie luate pentru a preveni alte probleme. | minimizarea impactului operațional al incidentelor. |
| C4. Capacitatea de a efectua teste de securitate TIC, cum ar fi testele de penetrare a retelei, testarea fara fir, evaluarile codurilor, evaluarile de tip wireless si/sau firewall, în conformitate cu metodele si protocoalele acceptate la nivel de industrie pentru a identifica si a analiza eventuale vulnerabilitati. | Acționează independent în planificarea și realizarea testelor de penetrare și evaluărilor de securitate, asumându-și responsabilitatea pentru acuratețea analizelor și pentru propunerea contramăsurilor. |
| C5. Capacitatea de a gestiona planurile de recuperare in urma dezastrelor ce pot cauza pirderi de date din sistemul informational. | Coordonează implementarea și actualizarea planurilor de continuitate a activității, exercitând autonomie decizională în prioritizarea și execuția măsurilor de restaurare a sistemelor informatice. |
| C6. Capacitatea de a gestiona securitatea sistemelor TIC: Aplica tehnici de detectare pentru securitate. Înțelege tehnicile de atac cibernetic si pune în aplicare contramasuri eficiente. | Administrează și monitorizează infrastructurile TIC complexe, luând decizii autonome pentru detectarea și contracararea atacurilor cibernetice, menținând un nivel ridicat de siguranță operațională. |
| C7. Capacitatea de a realiza analize de date, de a culege date si statistici în vederea testarii si evaluarii pentru a genera afirmatii si previziuni de tipare, cu scopul de a descoperi informatii utile în procesul de decizie. | Manifestă autonomie în proiectarea și implementarea analizelor de date avansate, asumându-și responsabilitatea pentru validitatea interpretărilor și pentru sprijinirea deciziilor strategice prin metode bazate pe AI. |

| | |
|---|---|
| C8. Capacitatea de a mentine securitatea bazelor de date. | Asigură în mod autonom protecția bazelor de date, controlul accesului și recuperarea informațiilor, răspunzând de confidențialitatea și integritatea datelor organizației. |
| C9. Capacitatea de a crea modele de date, utilizand tehnici si metodologii specifice. | Proiectează și documentează modele conceptuale și logice de date, asumându-și responsabilitatea pentru coerența, consistența și aplicabilitatea acestora în sisteme informatice complexe. |
| C10. Capacitatea de a proiecta arhitecturi de tip cloud si de a dezvolta servicii de tip cloud computing. | Conduce în mod autonom procesele de proiectare, configurare și evaluare a arhitecturilor cloud, garantând securitatea, scalabilitatea și conformitatea soluțiilor implementate. |

| **Nr.** | **Abilități transversale** | **Descriere** |
|---|---|---|
| CT1 | Aplicarea regulilor de organizare a muncii, înțelegerea responsabilităților și respectarea regulilor de etică profesională, precum și a celor de securitate și confidențialitate a datelor | Absolventul demonstrează capacitatea de a respecta normele de etică profesională, regulile de organizare a activității și principiile de confidențialitate a informațiilor. El aplică standardele de securitate cibernetică și legislația privind protecția datelor, asumându-și responsabilitatea pentru acțiunile sale profesionale și impactul acestora asupra organizației și societății. |
| CT2 | Identificarea rolului unei echipe interdisciplinare și asumarea responsabilităților corespunzătoare profilului profesional și personal | Absolventul recunoaște importanța colaborării interdisciplinare în proiecte complexe de securitate și inteligență artificială, contribuind activ la atingerea obiectivelor comune. El își asumă responsabilități |

| | | |
|---|---|---|
| | | în funcție de competențele proprii, manifestând respect, cooperare și inițiativă în cadrul echipelor mixte formate din specialiști IT, cercetători și decidenți. |
| CT3 | Utilizarea eficientă a surselor de informare și comunicare și a pregătirii profesionale | Absolventul utilizează în mod critic și eficient surse diverse de informare — științifice, tehnice și profesionale — pentru actualizarea permanentă a cunoștințelor și îmbunătățirea performanței profesionale. El comunică clar și argumentat, în formă scrisă și orală, în contexte academice și profesionale, inclusiv internaționale. |
| CT4 | Gândire analitică, capacitatea de rezolvare a problemelor | Absolventul demonstrează gândire logică și analitică, identificând probleme complexe și formulând soluții inovatoare bazate pe metode științifice și instrumente informatice. Este capabil să analizeze date, să evalueze riscuri și să ia decizii argumentate în contexte tehnologice și organizaționale diverse. |
| CT5 | Capacitatea de interpretare, sintetizare și analiză critică a rezultatelor | Absolventul manifestă autonomie în interpretarea și corelarea datelor tehnice și științifice, sintetizând informațiile într-un mod coerent și relevant pentru luarea deciziilor. Evaluează critic rezultatele analizelor, cercetărilor și experimentelor, formulând concluzii și recomandări bazate pe argumente solide și principii științifice. |

**Decan,**
**Conf. dr. Nicola Aurelian**

**Coordonator program de studii,**
**Conf. dr. Băutu Elena**