

# **PLAN DE ÎNVĂȚĂMÂNT**

## **al promoției 2023 - 2025**

**Universitatea Transilvania din Brașov**

Programul de studii universitare demasterat	<b>SECURITATE CIBERNETICĂ (în limba engleză)</b>
Domeniul fundamental	<b>Ştiinţe ingineresci</b>
Domeniul de masterat	<b>Inginerie electronică, telecomunicații și tehnologii informaționale</b>
Facultatea	<b>Facultatea de Inginerie electrică și știința calculatoarelor</b>
Durata studiilor:	<b>2 ANI</b>
Forma de învățământ:	<b>cu frecvență (IF)</b>

## 1. OBIECTIVE DE FORMARE ȘI COMPETENȚE

Obiectivul general al programului de masterat este de a dezvolta deprinderi și competențe pentru o carieră profesională /de cercetare în interacțiunea ramurilor de știință și tehnologie de electronică, comunicații digitale, ingineria calculatoarelor și tehnologia informației. Totodată, se urmărește formarea de capabilități de a administra și a transforma contextul de studiu sau de lucru la cerințe noi, neprevizibile, care solicită abordări strategice noi în situația dinamică a tehnologiei în electronica programată, cu extensii și către comunicațiile digitale, urmărind să se respecte și cerințele EQF-Level 7 – Master.

Scopul masteratului este de a asigura deprinderi și competențe pentru o carieră profesională/de cercetare pentru proiectarea și implementarea securității cibernetice la nivel de organizație, local, național și regional. Pregătirea specialiștilor în securitate cibernetică va fi bazată pe prezentarea conceptelor de securitate cibernetică, infrastructuri critice, securitate informațională și pe dobândirea de abilități practice în ce privește determinarea amenințărilor, riscurilor și vulnerabilităților de securitate cibernetică și de gestionare rapidă și eficientă a sistemelor în cazul unor incidente de securitate.

Obiectivele și profilul de competente dezvoltat în concordanță cu nevoile identificate pe piața muncii și cu cadrul național al calificărilor sunt prezentate sintetic mai jos și detaliat în fișele disciplinelor din planul de învățământ.

### Competențe profesionale

Absolventul

#### C1. Gestionarea securității sistemului

R.Î.1.1. Analizează activele critice ale unei întreprinderi și identifică punctele slabe și vulnerabilitățile care au condus la intruziune sau atac.

R.Î.1.2. Aplică tehnici de detectare pentru securitate.

R.Î.1.3. Înțelege tehnici de atac cibernetic și pune în aplicare contramasuri eficiente

#### C2. Defineste politici de securitate

R.Î.2.1. Concep și executa un set de norme și politici scrise care au scopul de a asigura o organizare în ceea ce privește constrângerile legate de comportamentul partilor interesate, constrângerile mecanice de protecție și constrângerile legate de accesul la date.

#### C3. identifica riscurile la adresa securitatii TIC

R.Î.3.1. Aplică metode și tehnici de identificare a eventualelor amenințări la adresa securitatii, a breselor de securitate și a factorilor de risc prin utilizarea de instrumentele TIC pentru supravegherea sistemelor TIC, analizarea riscurilor, a vulnerabilităților și a amenințărilor și evaluarea planurilor de urgență.

#### C4. Implementeaza gestionarea riscurilor în TIC

R.Î.4.1. Dezvoltă și implementează proceduri pentru identificarea, evaluarea, tratarea și atenuarea riscurilor TIC, cum ar fi accesul neautorizat sau surgerile de date, în conformitate cu strategia, procedurile și politicile de risc ale societății.

R.Î.4.2. Analizează și gestionează riscurile și incidentele de securitate.

R.Î.4.3. Recomanda măsuri de îmbunătățire a strategiei de securitate digitală.

#### C5. Efectueaza audituri în TIC

R.Î.5.1. Organizează și efectuează audituri în vederea evaluării sistemelor TIC, a conformității componentelor sistemelor, a sistemelor informative de prelucrare a informațiilor și a securitatii informațiilor.

R.Î.5.2. Identifica si colecteaza eventualele probleme critice si recomanda solutii bazate pe standardele si solutiile necesare.

#### C6. Gestioneaza conformitatea cu standardele de securitate în TI

R.Î.6.1. Îndruma punerea în aplicare si îndeplinirea standardelor, a celor mai bune practici si a cerintelor legale în materie de securitate a informatiilor relevante la nivelul industriei.

#### C7. Protejeaza dispozitive TIC

R.Î.7.1. Protejeaza dispozitive TIC si continutul digital si înțelege risurile si amenintarile din mediile digitale.

R.Î.7.2. Cunoaste masurile de siguranta si securitate si tine seama în mod corespunzator de încredere si de viata privata.

R.Î.7.3. Utilizeaza instrumente si metode care sa maximizeze securitatea dispozitivelor si informatiilor TIC prin controlul accesului, cum ar fi parolele, semnaturile digitale, biometria si sistemele de protectie precum firewall, antivirus, filtre spam

#### C8. Dezvolta strategia de securitate a informatiilor

R.Î.8.1. Creeaza strategia întreprinderii legata de siguranta si securitatea informatiilor, pentru a maximiza integritatea informatiilor, disponibilitatea si confidentialitatea datelor.

#### C9. Identifica punctele slabe ale sistemelor TIC

R.Î.9.1. Analizeaza sistemul si arhitectura retelei, componentele hardware si software, precum si datele pentru a identifica punctele slabe si vulnerabilitatile la intruziuni sau atacuri.

R.Î.9.2. Efectueaza operatiuni de diagnosticare privind infrastructura cibernetica, inclusiv cercetarea, identificarea, interpretarea si clasificarea vulnerabilitatilor, a atacurilor asociate si a codului daunator (de exemplu, pentru activitati specifice analizei criminalistice malware si activitati rau-intentionate în reteau).

R.Î.9.3. Compara indicatorii sau elementele observabile cu cerintele si revizuieste jurnalele pentru a identifica dovezi ale unor intruziuni din trecut.

#### C10. Gestioneaza chei pentru protectia datelor

R.Î.10.1. Selecteaza mecanismele adecvate de autentificare si autorizare.

R.Î.10.2. Concep, pune în aplicare gestionarea si utilizarea cheilor si remediază problemele aferente acestora.

R.Î.10.3. Concep si pune în aplicare o solutie de criptare a datelor pentru datele statice si datele în curs de transmitere.

#### C11. Gestioneaza date în cloud si stocarea acestora

R.Î.11.1. Creeaza si gestioneaza pastrarea datelor în cloud.

R.Î.11.2. Identifica necesitatile în materie de protectie a datelor, criptare si planificare a capacitatilor si pune în aplicare masurile necesare.

#### C12. Raspunde la incidentele din cloud

R.Î.12.1. Remediază problemele legate de cloud si stabileste modalitatatile de restabilire a operatiunilor.

R.Î.12.2. Concep si automatizeaza strategii de recuperare în caz de dezastru si evalueaza implementarea pentru punctele critice.

#### C13. Prezinta rapoarte privind rezultatele testelor

R.Î.13.1. Prezinta rapoarte privind rezultatele testelor, axându-se pe constatari si recomandari si diferentiind rezultatele pe niveluri de gravitate.

R.Î.13.2. Include informatiile relevante din planul de testare si prezinta metodologiile de testare, utilizând metrici, tabele si metode vizuale pentru clarificare, daca este necesar.

#### **C14. Mentine planul pentru continuitatea operatiunilor**

R.Î.14.1. Actualizeaza metodologia care contine masuri de asigurare a faptului ca unitatile unei organizatii pot functiona în continuare în cazul unei game largi de evenimente neprevazute.

#### **C15. Implementeaza o retea virtuala privata**

R.Î.15.1. Creeaza o conexiune criptata între retele private, cum ar fi diferite retele locale ale unei companii, pe internet, pentru a se asigura ca numai utilizatorii autorizati pot avea acces la ele si ca datele nu pot fi interceptate.

#### **C16. Analizează grupuri masive de date**

R.Î.16.1. Aplică tehniciile de inteligență artificială asupra masivelor de date

R.Î.16.2. Programează inteligență distribuită la nivelul deciziei, al semnalizării și al serviciului

R.Î.16.3. Realizează servicii pentru rețele inteligente de comunicații, cu control sporit la nivel de utilizator

### **Competențe transversale și rezultatele învățării**

Absolventul

#### **CT1. Aplică competențe de comunicare în domeniul tehnic**

R.Î.1.1. Adaptează limbajul și repertoriul de comunicare la particularitățile interlocutorilor

R.Î.1.2. Comunică cu potențiali clienți în modul cel mai eficient și adekvat pentru a le permite accesul la produsele sau serviciile dorite sau la orice alt tip de sprijin de specialitate.

#### **CT2. Soluționează probleme**

R.Î.2.1. Dezvoltă strategii pentru rezolvarea problemelor

R.Î.2.2. Găsește soluții la probleme

R.Î.2.3. Aplică diverse strategii pentru rezolvarea problemelor

#### **CT3. Sprijină utilizatorii sistemelor TIC**

R.Î.3.1. Comunică pentru identifică cerințele utilizatorilor, a le formula ca specificații funcționale și a le documenta într-un mod inteligibil și logic pentru analize ulterioare și pentru planurile de acceptanță

R.Î.3.2. Comunică cu utilizatorii finali în manieră "Agilă", privitor la stadiul dezvoltării/ implementării/ integrării/ testării

R.Î.3.3. Documentează activități de formare a personalului de exploatare a sistemului TIC proiectat

R.Î.3.4. Organizează distribuirea de documente structurate, în formate diverse

#### **CT4. Demonstrează spirit antreprenorial**

R.Î.4.1. Analizează procese de afaceri pornind de la raportul cost/beneficiu al unui proiect pornind de la bugetul unei societăți de profil sau al unei întreprinderi proprii.

R.Î.4.2. Stabilește contribuția proceselor de lucru la obiectivele comerciale și planifică alocarea de resurse și măsuri investiționale și operaționale de mare productivitate

#### **CT5. Vorbește mai multe limbi străine**

R.Î.5.1. Utilizează cel puțin limba engleză pentru a putea comunica cu specialiștii

R.Î.5.2. Comunică informații tehnice pentru nespecialiști într-o limbă străină.

## **2. STRUCTURA PE SĂPTĂMÂNI A ANULUI UNIVERSITAR**

Număr de semestre: 4 semestre.

Număr de credite pe semestrul: 30 de credite

Număr de ore de activități didactice / săptămână: 26

Numărul de săptămâni: 14

	Activități didactice		Sesiuni de examene			Vacanțe		
	Sem. I	Sem. II	Iarnă	Vară	Restante	Iarnă	Primăvară	Vară
Anul I	14	14	3	4	2	3	1	10
Anul II	14	14	3	4	2	3	1	-

### 3. ASIGURAREA FLEXIBILIZĂRII INSTRUIRII. CONDIȚIONĂRI

Flexibilizarea programului de studii este asigurată prin discipline opționale și discipline facultative. Disciplinele opționale sunt propuse pentru semestrele 2-4, prin pachete de discipline de specialitate.

### 4. CONDIȚII DE ÎNSCRIERE ÎN ANUL DE STUDII URMĂTOR. CONDIȚII DE PROMOVARE A UNUI AN DE STUDII

Înscrierea în anul următor este condiționată de întrunirea condițiilor de promovare cuprinse în Regulamentul privind activitatea profesională a studentilor.

### 5. EXAMENUL DE FINALIZARE A STUDIILOR

Perioada de întocmire a lucrării disertație: începând cu penultimul semestru de studii.

Definitivarea lucrării de disertație: în ultimul semestru de studii.

Perioada de susținere a lucrării de disertație: în sesiunea iunie-iulie a ultimului an de studii.

Numărul de credite pentru susținerea proiectului de licență: 10 credite (în plus față de cele 120).

### 6. DISCIPLINELE DE STUDII PE ANI

## ANUL I

Nr. crt.	Discipline cu criteriu: Obligatoriu	C <sub>1</sub> **	C <sub>2</sub> **	Semestrul I							Semestrul II							
				C	S	L	P	SI	V	Cr	C	S	L	P	SI	V	Cr	
1	Fundamente de criptografie scenarii de aplicare	DAP	DI	2	0	2	0	69	E	5								
2	Securitatea cibernetică a sistemelor și serviciilor informatici	DAP	DI	2	0	2	1	80	E	6								
3	Gestionarea identității și accesului în spațiul virtual	DAP	DI	2	0	2	0	69	E	5								
4	Tipuri de atacuri și amenințări cibernetice	DAP	DI	1	0	1	0	72	E	4								
5	Etică și integritate academică	DS	DI	1	0	0	0	86	C	4								
6	Practică I	DS	DI	0	0	0	10	10	C	6								
7	Gestionarea incidentelor de securitate cibernetică	DAP	DI								1	0	1	1	58	E	4	
8	Securitatea rețelelor și izolarea perimetrală	DAC	DI								2	0	2	0	69	E	5	
9	Securitatea infrastructurilor critice	DS	DI								1	0	1	0	72	E	4	
10	Securitatea sistemelor de control industrial	DAC	DI								1	0	2	0	58	E	4	
11	Gestionarea proceselor de afaceri	DS	DI								1	0	0	0	61	C	3	
13	Practică II	DS	DI								0	0	0	10	10	C	6	
Total				8	0	7	11	386	E 4	C 2	30	6	0	6	11	328	E 4	C 2
Total ore didactice pe săptămână				26							23							

Nr. crt.	Discipline cu criteriu: Optional	C <sub>1</sub> **	C <sub>2</sub> **	Semestrul I							Semestrul II							
				C	S	L	P	SI	V	Cr	C	S	L	P	SI	V	Cr	
12	Tehnologii securizate de web și internet	DS	DO								2	0	1	0	58	C	4	
12	Securitate în programare și securitatea aplicațiilor	DS	DO								2	0	1	0	58	C	4	
Total				0	0	0	0	0	E 0	C 0	0	2	0	1	0	58	E 0	C 1
Total ore didactice pe săptămână				0							3							

Legendă:C<sub>1</sub> = criteriu conținutului.

DAP – discipline de aprofundare

C<sub>2</sub> = criteriu obligativitatea.

DI – discipline obligatorii (impuse)

DS – discipline de sinteză

DO – discipline opționale

DCA – discipline de cunoaștere avansată

DFc – discipline facultative

SI = ore de studiu individual

RECTOR,

PROF. DR. IOAN VASILE ABRUDAN

DIRECTOR DEPARTAMENT,

LECT. DR. AUREL CORNEL STANCA

DECAN,

LECT. DR. SEPTIMIU DANIEL MOTOASCA *✓*

COORDONATOR PROGRAM STUDII,

CONF. DR. TITUS CONSTANTIN BALAN

FO2.1.1-PS7.2-01/ed.3,rev.5

CONFORM CU *✓*  
ORIGINALUL

## ANUL II

Nr. crt.	Discipline cu criteriul: Obligatoriu	C <sub>1</sub> ''	C <sub>2</sub> ''	Semestrul I							Semestrul II							
				C	S	L	P	SI	V	Cr	C	S	L	P	SI	V	Cr	
1	IT forensics	DAC	DI	1	0	1	0	72	E	4								
2	Data mining și data warehousing	DAP	DI	2	0	2	0	69	E	5								
3	Hacking etic și audit de securitate	DAP	DI	1	0	2	1	44	E	4								
4	Asigurarea informațională și managementul riscului	DS	DI	1	0	0	1	72	C	4								
5	Practică I	DS	DI	0	0	0	10	10	C	6								
8	Practică II	DS	DI								0	0	0	10	110	C	10	
9	Practica pentru elaborarea lucrării de disertatie	DS	DI								0	0	0	8	138	C	10	
10	Elaborarea lucrării de disertatie	DS	DI								0	0	0	8	138	C	10	
Total				5	0	5	12	267	E	C	23	0	0	0	26	386	E	C
									3	2						0	3	30
Total ore didactice pe săptămână				22							26							

Nr. crt.	Discipline cu criteriul: Optional	C <sub>1</sub> ''	C <sub>2</sub> ''	Semestrul I							Semestrul II							
				C	S	L	P	SI	V	Cr	C	S	L	P	SI	V	Cr	
6	Analiză malware	DAP	DO	2	0	1	0	58	E	4								
6	Securitatea cibernetică a dispozitivelor mobile	DAP	DO	2	0	1	0	58	E	4								
7	Protecția datelor și legislația privind securitatea	DS	DO	1	0	0	0	61	C	3								
7	Arhitectura organizației și performanța afacerii	DS	DO	1	0	0	0	61	C	3								
Total				3	0	1	0	119	E	C	7	0	0	0	0	0	E	C
									1	1						0	0	0
Total ore didactice pe săptămână				4							0							

Legendă:C<sub>1</sub> = criteriul conținutului.

DAP – discipline de aprofundare

C<sub>2</sub> = criteriul obligativității.

DI – discipline obligatorii (impuse)

DS – discipline de sinteză

DO – discipline opționale

DCA – discipline de cunoaștere avansată

DFc – discipline facultative

SI = ore de studiu individual



RECTOR,

PROF. DR. IOAN VASILE ABRUDAN

DIRECTOR DEPARTAMENT,

LECT. DR. AUREL CORNEL STANCA

DECAN,

LECT. DR. SEPTIMIU DANIEL MOTOASCA

COORDONATOR PROGRAM STUDII,

CONF. DR. TITUS CONSTANTIN BALAN

Universitatea Transilvania din Brașov  
 Facultatea de Inginerie electrică și știința calculatoarelor  
 Programul de studii universitar de masterat: Securitate Cibernetică (în limba engleză)  
 Domeniul fundamental: Științe ingineresti  
 Domeniul de masterat: Inginerie electronică și telecomunicații  
 Durata studiilor: 2 ani  
 Forma de învățământ: Zi

Ministerul Educației  
 Valabil în an universitar 2023-2025

### BILANȚ GENERAL I

Nr crt	Disciplina	Nr de ore		Total		Nr credite	
		An I	An II	ore	%	An I	An II
1	Obligatorii	686	672	1358	93,27	56	53
2	Optionale	42	56	98	6,73	4	7
TOTAL		728	728	1456	100	60	60

### BILANȚ GENERAL II

Nr crt	Disciplina	Nr de ore		Total		Nr credite	
		An I	An II	ore	%	An I	An II
1	Discipline integral/ parțial asistate	448	224	672	46,1	48	24
2	Practică de specialitate	280	308	588	40,4	12	16
3	Practică pentru elaborarea disertației	0	196	196	13,5	0	20
TOTAL		728	728	1456	100	60	60

RECTOR,  
 PROF. DR. IOAN VASILE ABRUDAN



DIRECTOR DEPARTAMENT,  
 LECT. DR. AUREL CORNEL STANCA

DECAN,  
 LECT. DR. SEPTIMIU DANIEL MOTOASCA

COORDONATOR PROGRAM STUDII,  
 CONF. DR. TITUS CONSTANTIN BALAN