



Irakaskuntza Gidaliburua

2026/27 ikasturtea

Datu Orokorrak

Irakasgaia: THREAT INTELLIGENCE - MEHATXU-ADIMENA

Titulazioa: ZIBERSEGURTASUNeko GRADUA

Mota: DERRIGORREZKOA.

ECTS kredituak: 6 ECTS

Maila: 3.

Denbora-banaketa: 1. SEIHILEKOA.

Hizkuntza: GAZTELANIA.

Irakasle-taldea: Javier Valencia

Ikasgela(k): Gela informatizatua

Irakasgaiaren aurkezpena:

Ikasgai honen helburua da mehatxu-adimena aztertzea, biltzea eta estrategikoki erabiltzea, ingurune digitaletan arriskuak aurreikusteko, identifikatzeko eta arintzeko. Ziber-mehatxuen detekzio proaktiborako metodologiak landuko dira, konpromiso-adierazleak aztertuko dira eta iturri irekiak eta plataforma espezializatuak erabiliko dira ezagutza eragingarria sortzeko.

Datu espezifikoak

Prestakuntza- eta ikaskuntza-prozesuaren emaitzak (PIE)¹

Ezagutzak edo edukiak (E)	E1	Programazio-lengoiak aztertzeke kalkul-trebetasunak garatzeko.
	E2	Zibersegurtasun-sareen arkitekturaren mailan segurtasun-irtenbideak inplementatzeko egiturak eta protokoloak ezagutzea.
	E3	Datuen babesari eta informazioaren segurtasunari buruzko ezagutzak hainbat mailatan aplikatzeko.
	E6	Birus informatikoen tipologiak identifikatzea.
	E7	Auzitegien aurkako teknikak eta horien aplikazioa ezagutzea.

¹ PIEren sailkapena 822/2021 Errege Dekretuan definitutakoari dagokio, eta titulua egiaztatzeke memorian definituta dago.

* Edukia zabaltzea, horretarako irakaskuntza-programazioa erabiliz. Zabaltzea tarteko puntuan egon behar da, hau da, irakaskuntza-gidako informazioa zabaldu behar da, baina ez da iritsi behar irakaskuntza-programazioaren mugetara. Puntu puntu aztertu beharreko gaien aurkibidea sartu behar da (garatu gabe). Gehienez hiru azpial sar daitezke, ideia giltzarriekin/azpigaiekin Gehienez 2 orrialde izango ditu.

	E8	Kriptografiari eta zibersegurtasunari algoritmoak diseinatzeko teknikak eta oinarri matematikoak aplikatzea.
	E11	Malware-topologiak ezagutzeko, ondoren aztertu eta arintzeko.
	E13	Identitateen kudeaketa, zifratzea, autentifikazioa, konfidentzialtasuna, osotasuna eta informazioaren eskuragarritasuna aztertzea.
	E14	Gertaera jakin baten arriskuak balioestea, metodo estatistikoen eta probabilitikoen bidez.
Gaitasunak (GA)	GA2	Ingeniaritza- eta zibersegurtasun-tresnak erabiltzea ziberjazarpenekin lotutako arazoak konpontzeko.
	GA3	Hainbat azterketa-prozesu gauzatzea zibersegurtasunaren hainbat arlotan.
	GA5	Sistema informatiko batean erasoak prebenitzeko, detektatzeko eta babesteko teknikak aplikatzea.
	GA7	Soluzio kriptografikoak inplementatzea.
	GA11	Ahulezien ebidentziak kudeatzea.
	GA12	Auzitegiko analisiak egitea.
Trebetasunak eta abileziak (T)	T1	Taldean lan egitea eta eskuratutako ezagutzak eta trebetasunak transmititzea.
	T2	Proiektuak aztertzeko, lantzeko eta lankidetzan aritzeko trebetasunak garatzea, merkatuaren berezko premietatik abiatuta.
	T4	Lanbide-esparruan erabakiak hartzea, jarduera akademikoan zehar eskuratutako ezagutzak eta teknikak aplikatuta.
	T5	Era guztietako entzuleei, ezagutzei, ideiei, konponbideei, datuei eta abarri modu argi eta laburrean komunikatzea, azterlanaren
	T6	Ingeleseko informazio teknikoarekin lan egiteko gai izatea, bai kontsultari dagokionez, bai hura lantzeari dagokionez.

Irakasgaiaren Edukia*

1. unitatea: Threat Intelligence-ren sarrera eta oinarriak

- 1.1. Mehatxu-adimenaren definizioa eta helburuak
- 1.2. Datuen, informazioaren eta adimenaren arteko aldeak
- 1.3. Adimenaren bizi-zikloa
- 1.4. Estandarrak eta erreferentzia-esparruak

- 1.5. ITren rola defentsa proaktiboan, detekzioan eta erantzunean

2. unitatea. Datu-iturriak eta inteligentzia-bilketa

- 2.1. Iturburu irekiak (OSINT) eta itxiak
- 2.2. Sareko adimena
- 2.3. Adimena endpoint sistemetan
- 2.4. Konpromiso-adierazleak biltzea (IoCs)
- 2.5. Biltzeko eta aztertzeko tresnak

3. unitatea. Analisia eta korrelazioa

- 3.1. Pivoting teknikak eta adierazleak aberastea
- 3.2. IoCs eta SIEM eta TIPen arteko korrelazioa
- 3.3. Kanpainen azterketa eta gertakarien taldekatzea
- 3.4. MITRE ATT & CK erabiltzea TTPak mapatzeko
- 3.5. Patroien analisirako eta mehatxuak egozteko sarrera
- 3.6. Feeds integratzea SIEM/MISPN eta korrelazioa

4. unitatea. Mehatxu-eragileak eta TTPak

- 4.1. Aurkarien sailkapena
- 4.2. Motibazio-ereduak, gaitasunak eta aukerak
- 4.3. Azterketa-kasuak
- 4.4. Iraunkortasun, ihes, komando eta kontroleko teknikak (C2)

5. unitatea. Adimen-plataformak eta -tresnak

- 5.1. Threat Intelligence Platforms (TIPs)
- 5.2. Inteligentzia-trukea estandarizatzea
- 5.3. SIEMak eta horiek adimenarekin integratzea

6. unitatea. Adimenaren aplikazio praktikoa

- 6.1. ITak KSAetan eta KSIRTetan integratzea
- 6.2. Erabilera Threat Hunting-en
- 6.3. Mehatxu espezifikoaren detekzio goiztiarra

7. unitatea. Adimena eta komunikazioa sortzea

- 7.1. Txostenak egitea entzunaldiaren arabera
- 7.2. Jardunbide onenak idazketan eta bistaratzean
- 7.3. Benetako txostenen azterketa-kasuak

8. unitatea. Threat Intelligence-ren joerak eta etorkizuna

- 8.1. Elkarlaneko adimena: ISACak eta proiektu komunitarioak
- 8.2. Adimenari aplikatutako automatizazioa eta AA
- 8.3. Sortzen ari diren arriskuak
- 8.4. Etika, legezkotasuna eta erantzukizuna



Irakaskuntza Gidaliburua

2026/27 ikasturtea

Irakaskuntza-metodologiak eta prestakuntza-jarduerak²

Irakasgai honetan erabilitako irakaskuntza-metodologiak honako hauek dira:

IM1	Azalpenezko metodoa.
IM2	Kasu-azterketak.
IM3	Arazoetan oinarritutako ikaskuntza.
IM4	Proiektuetan oinarritutako ikaskuntza.
IM5	Ikasketa kooperatiboa.
IM6	Tutoretzak.

Irakasgai honetan erabilitako prestakuntza-jarduerak honako hauek dira:

Prestakuntza-jarduerak	Aurreikusitako orduak	presentzialtasuna (%)
PJ1: Klase teorikoa.	22,5	100
PJ9: Laborategiko klaseak	15	100
PJ3: Lanak egitea (banakakoak eta/edo taldekoak).	12,5	50
PJ3: Tutoretzak (banakakoak eta/edo taldekoak).	5	50
PJ5: Ikasketa independentea eta ikaslearen lan autonomoa.	89	0
PJ6: Ebaluazio-probak.	6	100
Guztira	150	--

Ebaluazioa: Ebaluazio-sistemak eta -irizpideak

Ebaluazio-asteak unibertsitatearen webgunean argitaratutako egutegi akademikoan zehaztuta daude; datak irakaskuntza hasi ondoren zehaztuko dira.

² Titulutik egiaztatutako memoriatik irakaskuntza-metodologiak, prestakuntza-jarduerak eta ebaluazio-sistemak atera beharko dira. (1 ECTS = ikaslearen 25 lanordu).



Irakaskuntza Gidaliburua

2026/27 ikasturtea

Irakasgai honetan honako ebaluazio-sistema hauek erabili dira:

Izendapena	Gutx. hazt.	Gehi. hazt.
ES1 Ikaslearen bertaratzea eta parte-hartzea ebaluatzea.	0	5
ES2 Lanen ebaluazioa.	10	35
ES6: Laborategien ebaluazioa	50	70

Ikasleak bi ebaluazio-modalitate ditu irakasgaia gainditzeko:

- Etengabeko ebaluazioa, urtean 2 deialditan: ohikoa eta ezohikoa.
- Ebaluzio bakarra, urtean 2 deialdirekin.

Euneiz Unibertsitatean, ebaluazio jarraitua (irakasleek definitutako irakasgaiaren jardura ebaluagarrien batezbesteko haztatua) da ebaluazio nagusia, baina Euneizek ebaluazio bakarrari heltzeko aukera ematen dio ikasleari.

Ezin da aldatu ikasturtean zehar ikasleak aukeratutako ebaluazio-modalitatea (jarraitua izatetik bakarra izatera).

Ebaluazio bakarreko modalitateari heldu nahi dion ikasleak hori justifikatzen duen idazki formal bat aurkeztu beharko du irakasgaiaz arduratzen diren irakasleei eta tituluaren koordinazioari zuzenduta, modalitate hori hasi eta lehenengo bi asteetan.

Ikaslea ez bada joaten eskola presentzialetara % 80ra, ebaluazio bakarraren ezohiko deialdira igaroko da zuzenean.

Salbuespen gisa, irakasgaiaz arduratzen den irakasleak beste irizpide gehigarri batzuen bidez baloratu ahal izango du, hala nola parte hartzea, jarrera, ikaslearen jardun- eta aprobetxamendu-maila, etab., ikasleari ohiko deialdian jarraitzeko aukera, betiere haren gutxieneko bertaratzea % 70etik gorakoa bada.

Hutsegiteak irakasgaiaz arduratzen den irakasleari justifikatu behar zaizkio, astebeteko epean gehienez ere. Egiaztagiri ofiziala posta elektronikoz aurkeztu beharko zaio irakasle arduradunari.

Ikaslea SOILIK etendako zatiekin joango da ezohiko ebaluaziora.

Irakasgaiaren kalifikazio-sistemak 1125/2003 Errege Dekretuan ezarritakoari jarraitzen dio, eta lortutako emaitzak 0tik 10era bitarteko zenbakizko eskalari jarraituz kalifikatuko dira, dezimal baten adierazpenarekin.



Irakaskuntza Gidaliburua 2026/27 ikasturtea

- 0-4,9: Gutxiegia (GT).
- 5,0-6,9: Nahiko (NK).
- 7,0-8,9: Oso ongi (OO).
- 9,0-10: Bikain (BI).

«Ohorezko matrikula» aipamena 9.0 edo gehiagoko kalifikazioa lortu duten ikasleei eman ahal izango zaie. Kopurua ez da izango dagokion ikasturtean ikasgai batean matrikulatutako ikasleen ehuneko bost baino handiagoa, matrikulatutako ikasleen kopurua 20tik beherakoa denean izan ezik; kasu horretan, «Ohorezko Matrikula» bakarra eman ahal izango,

Ebaluazio-jarduerarik egiten ez duen ikasle matrikulatua ez-aurkeztutzat (EA) joko da.

Iratzizko ebaluazio-jarduera orok (lanak, azterketak...) akats ortotipografikoak hartuko ditu kontuan azken kalifikazioan.

Plagioa debekatuta dago, bai lanetan, bai azterketetan, kalifikazioa detektatuz gero, eten egingo da. Campus birtualaren bidez entregatutako lanak Turnitin tresnak aztertuko ditu:

- Irakasleak % 20 eta % 30 arteko antzekotasun-indizea duten txostenak berrikusiko ditu, plagio-iturri posibleak aztertzeko eta justifikatuta dauden ebaluatzeko.
- Irakaslearen analisia egin ondoren, % 30etik gorako antzekotasun-indizea duen edozein lan ez da ebaluatuko.

Beharrezko baliabide materialak eta azpiegiturak

Baliabide material edota azpiegitura mota
Irakaskuntza-materiala (apunteak, aurkezpenak, gidak, zereginak...)
Ikus-entzunezko baliabideak
Irakasgaiaren material espezifikoa
Gela informatizatua
Zibersegurtasuneko laborategia

Bibliografia eta ikasteko beste baliabide batzuk

Oinarrizko Bibliografia



Irakaskuntza Gidaliburua

2026/27 ikasturtea

- Wilhoit, K., & Opacki, J. (2022). Operationalizing Threat Intelligence: A guide to developing and operationalizing cyber threat intelligence programs. Packt.
- Bergmann, I. (2023). OSINT and Threat Intelligence: Building a Robust Security Framework. Independently published.
- Bodmer, S., Kilger, M., Carpenter, G., & Jones, J. (2012). Reverse Deception: Organized Cyber Threat Counter-Exploitation. McGraw-Hill.

Bibliografia Osagarria

- Conti, M., Dehghantanha, A., & Dargahi, T. (2018). Cyber Threat Intelligence: Challenges and Opportunities. ArXiv.
- Roccia, T. (2024). Visual Threat Intelligence. Security Break.
- Sindiramutty, S. R. (2023). Autonomous Threat Hunting: A Future Paradigm for AI-Driven Threat Intelligence. ArXiv.

Gomendatutako Beste Ikaskuntza-baliabide Batzuk³

- GitHub – Awesome Threat Intelligence – Komunitate-biltegia tresnekin, formatuekin (STIX/TAXII/VERIS), eta liburutegiekin
- 2024 Global Threat Intelligence Report (CyberProof) – mehatxuen egungo ikuspegia

³ Ikasteko beste baliabide batzuen artean, web-orriak, softwarea, ikus-entzunezko gaia eta abar sar daitezke.