



Datu Orokorrak

Irakasgaia: AZPIEGITURA KRITIKOAK BABESTEA

Titulazioa: ZIBERSEGURTASUNeko GRADUA

Mota: HAUTAZKOA.

ECTS kredituak: 6 ECTS

Maila: 3.

Denbora-banaketa: 2. SEIHILEKOA.

Hizkuntza: GAZTELANIA.

Irakasle-taldea: Dk. Lorenzo Fanari lorenzo.fanari@euneiz.com

Ikasgela(k): Gela informatizatua

Irakasgaiaren aurkezpena:

Azpiegitura kritikoak arrisku fisiko eta zibernetikoetatik babesteko estrategiak aztertzea eta diseinatzea bideratutako irakasgaia. Arau-esparruak, mehatxuak eta ahuleziak ebaluatzen direnak eta funtsezko sektoreei (energia, ura, osasuna, garraioa edo telekomunikazioak) aplikatutako defentsa-sistemak aztertuko dira.

Datu espezifikoak

Prestakuntza- eta ikaskuntza-prozesuaren emaitzak (PIE)¹

Ezagutzak edo edukiak (E)	E1	Programazio-lengoiak aztertzeko kalkulu-trebetasunak garatzeko.
	E16	Azpiegitura kritikoaren eta elementu ziberfisikoen kontzeptua ulertzea, jasan ditzaketen arrisku espezifikoak aztertzeko eta haiek kudeatzeko kontraneurri egokiak hedatzeko, indarrean dagoen legeria kontuan hartuta.
	E17	Osasun-sistemen sistemak eta tresnak ezagutzea, baita horien inplikazioak eta babes-metodologiak eta -tresnak ere.
Gaitasunak (GA)	GA1	Ordenagailuak, sistema eragileak, sareak, datu-baseak eta

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

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

		hodeiaren ingurunea erabiltzea eta programatzea, zibersegurtasunean aplikatzeko.
	GA4	Zibersegurtasunari aplikatutako ingeniartza-diseinuak egitea.
	GA6	Egoera errealean inplementatzeko gehien erabiltzen diren programazio-lengoaiak segurtasunez erabiltzea.
	GA9	ITn oinarritutako konponbideak eraginkortasunez integratzea erabiltzailearen ingurunean.
	GA10	Softwarea egiaztatze eta baliozkotzeko garapen seguruko teknikak eta tresnak aplikatzea.
Trebetasunak eta abileziak (T)	T1	Taldean lan egitea eta eskuratutako ezagutzak eta trebetasunak transmititzea.
	T2	Proiektuak aztertze, lantze 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. gaia. Azpiegitura kritikoen hastapenak
 - o Azpiegitura kritikoen eta lotutako sektoreen definizioa
 - o Eragin sistemikoa eta sektoreen arteko mendekotasunak
 - o IKen babesaren bilakaera historikoa
- 2. gaia. Mehatxuak eta ahuleziak
 - o Mehatxuaren, kalteberatasunaren eta arriskuaren kontzeptuak
 - o ZKI sistemen ahulezia espezifikoak
 - o Ransomware-erasoak eta arriskuak hornidura-katean
- 3. gaia. ZKI eta SIS
 - o ZKI eta SIS sistemen arkitektura
 - o BPCSren eta SISren arteko aldeak
 - o Segurtasunaren bizi-zikloa (security) eta segurtasun funtzionala
- 4. gaia. Diseinu segurua industria-inguruneetan
 - o Estrategia Defense in Depth

- o Industria-segmentazioko Purdue eredua
- o Eremuak eta konduktak OT estandarren arabera
- 5. gaia. Eraso errealeen analisia
 - o Stuxnet kasua
 - o Pipeline kolonialaren aurkako erasoak
 - o Malware TRITON/TRISIS segurtasun-sistemetan
- 6. gaia. Arriskua kudeatzea industria-inguruneetan
 - o Arriskuen ebaluazioa SIS sisteman
 - o IEC 62443-3-2 metodologia
 - o BowTie eta LOPA teknikak arrisku-analisirako
- 7. gaia. Araudia eta estandarrak
 - o IEC 61511 eta IEC 62443
 - o NIST CSF eta NIST SP 800-82
 - o NERC CIP erregulazioa energia-sektorean
- 8. gaia. Azpiegitura kritikoen etorkizuna
 - o Zero Trust OT inguruneei aplikatuta
 - o Adimen artifiziala eta automatizazioa IKn
 - o Erresilientzia operatiboa eta suspertzea gorabeheren aurrean

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:

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



Irakaskuntza Gidaliburua

2026/27 ikasturtea

Prestakuntza-jarduerak	Aurreikusitako orduak	presentzialtasuna (%)
PJ1: Klase teorikoa.	18	100
PJ2: Praktika-klasea.	5	100
PJ3: Lanak egitea (banakakoak eta/edo taldekoak).	17	50
PJ3: Tutoretzak (banakakoak eta/edo taldekoak).	2	50
PJ5: Ikasketa independentea eta ikaslearen lan autonomoa.	96	0
PJ6: Ebaluazio-probak.	2	40
PJ9: Laborategiko klaseak	10	100
Guztira	150	--

Ebaluazioa: Ebaluazio-sistemak eta -irizpideak

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

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.	5	15
ES3 Ebaluazio- eta/edo azterketa-probak	50	70
ES6: Laborategien ebaluazioa	10	30

Ikasleak bi ebaluazio-modalitate ditu irakasgaia gainditzeko:



Irakaskuntza Gidaliburua 2026/27 ikasturtea

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

Euneiz Unibertsitatean, ebaluazio jarraitua (irakasleek definitutako irakasgaiaren jarduera 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 irakasgaiak 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, irakasgaiak 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 irakasgaiak 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.

- 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.

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



Irakaskuntza Gidaliburua

2026/27 ikasturtea

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 espezifikoak
Gela informatizatua
Zibersegurtasuneko laborategia

Bibliografia eta ikasteko beste baliabide batzuk

Oinarrizko Bibliografia

- Robertson, E. (2021). Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Wiley.
- Stouffer, K., Falco, J., & Scarfone, K. (2018). Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Industrial Control System Foundations. NIST Special Publication.
- Johnson, C. (2022). Cyber Security: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. Routledge.

Bibliografia Osagarria

- Radvanovsky, R., & Brodsky, J. (2016). Handbook of SCADA/Control Systems Security. CRC Press.
- Maglaras, L., Ferrag, M. A., Derhab, A., Mukherjee, M., Janicke, H., & Rallis, S. (2019).



Irakaskuntza Gidaliburua

2026/27 ikasturtea

Threats, Protection and Attribution of Cyber Attacks on Critical Infrastructures. ArXiv.

- Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for Industrial Control Systems: A Survey. ArXiv.

Gomendatutako Beste Ikaskuntza-baliabide Batzuk³

- NIST Cybersecurity Framework y NIST SP 800-82 (ICS Security) – OT/IT arriskuak eta segurtasuna kudeatzeko erreferentzia-esparruak.
- IEC 62443 – nazioarteko funtsezko estandarrak industria-azpiegiturak babesteko

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