



Irakaskuntza Gidaliburua

2026/27 ikasturtea

Datu Orokorrak

Irakasgaia: PROGRAMAZIO SEGURUA (SDLC)

Titulazioa: ZIBERSEGURTASUNEO GRADUA

Mota: DERRIGORREZKOA.

ECTS kredituak: 6 ECTS

Maila: 2.

Denbora-banaketa: 1. SEIHILEKOA.

Hizkuntza: GAZTELANIA.

Irakasle-taldea: Patxi Galán patxi.galan@euneiz.com

Ikasgela(k): Ikasgela informatizatua

Irakasgaiaren aurkezpena:

Programazio Segurua irakasgaiak software sendoa eta segurua garatzeko beharrezkoak diren oinarriak, printzipioak eta praktikak ematen dizkie ikasleei, zibersegurtasuna softwarearen garapenaren bizi-zikloaren fase guztietan integratuz (SSDLC).

Datu espezifikoak

Prestakuntza- eta ikaskuntza-prozesuaren emaitzak (PIE)¹

Ezagutzak edo edukiak (E)	E2	Zibersegurtasun-sareen arkitekturaren mailan segurtasun-irtenbideak inplementatzeko egiturak eta protokoloak ezagutzea.
	E3	Datuen babesari eta informazioaren segurtasunari buruzko ezagutzak hainbat mailatan aplikatzeko.
	E4	Garapen- eta sartze-teknikak gauzatzea, hobekuntza teknikoak, konponbideak eta jardunbide egokiak aztertuta.
	E5	Garapen seguruak egitea eta kontraneurriak aplikatzea kode-mailan.
	E13	Identitateen kudeaketa, zifratzea, autentifikazioa, konfidentzialtasuna, osotasuna eta informazioaren eskuragarritasuna aztertzea.

¹ PIEren sailkapena 822/2021 Errege Dekretuan definitutakoari dagokio, eta titulua egiaztatzeko 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. Puntuaz puntu aztertu beharreko gaien aurkibidea sartu behar da (garatu gabe). Gehienez hiru azpialde sar daitezke, ideia giltzarriekin/azpigaiekin Gehienez 2 orrialde izango ditu.

	E14	Gertaera jakin baten arriskuak balioestea, metodo estatistikoaren eta probabilitateko bidez.
Gaitasunak (GA)	GA1	Ordenagailuak, sistema eragileak, sareak, datu-baseak eta hodeiaren ingurunea erabiltzea eta programatzea, zibersegurtasunean aplikatzeko.
	GA2	Ingeniaritza- eta zibersegurtasun-tresnak erabiltzea ziberjazarpenekin lotutako arazoak konpontzeko.
	GA3	Hainbat azterketa-prozesu gauzatzea zibersegurtasunaren hainbat arlotan.
	GA4	Zibersegurtasunari aplikatutako ingeniaritza-diseinuak egitea.
	GA6	Egoera errealean inplementatzeko gehien erabiltzen diren programazio-lengoiak segurtasunez erabiltzea.
	GA8	Sistema informatikoetan sartzeko testa aztertzea eta gauzatzea.
	GA10	Softwarea egiaztatzea eta baliozkotzeko garapen seguruko teknikak eta tresnak aplikatzea.
	GA14	Teknologia berrien ahuleziak ulertzea eta zibersegurtasuneko irtenbideak ematea.
Trebetasunak eta abileziak (T)	T1	Taldean lan egitea eta eskuratutako ezagutzak eta trebetasunak transmititzea.
	T2	Proiektuak aztertzea, lantzea eta lankidetzan aritzeko trebetasunak garatzea, merkatuaren berezko premietatik abiatuta.
	T3	Ingelesean ahoz zein idatziz komunikatzen trebea izatea.
	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: Programazio seguruaren eta SSDLC (Secure Software Development Life Cycle) sistemaren hastapenak



Irakaskuntza Gidaliburua

2026/27 ikasturtea

- 2. gaia: Zibersegurtasuneko printzipioak, estandarrak eta funtsezko erreferentziak (OWASP, CWE, ISO)
- 3. gaia: Mehatxu komunak: OWASP Top 10 (A1–A5)
- 4. gaia: Mehatxu komunak: OWASP Top 10 (A6–A10)
- 5. gaia: Sarrerak baliozkotzea, erroreak kudeatzea eta zifratzea
- 6. gaia: Sarbide-kontrola, autentifikazio segurua eta saioen kudeaketa •
- 7. gaia: Iturburu-kodearen analisi estatikoa eta dinamikoa
- 8. gaia: DevSecOps-erako sarrera eta mendekotasun-analisia
- 9. gaia: Segurtasuna APIetan REST eta Cloud inguruneetan hedatzea
- 10. gaia: SOLID patroia eta printzipioekin kode segurua diseinatzea

Praktika: API seguru bat diseinatzea

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.	23	100
PJ2: Praktika-klasea.	15	100
PJ3: Lanak egitea (banakakoak eta/edo taldekoak).	12	20
PJ3: Tutoretzak (banakakoak eta/edo taldekoak).	5	0

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



Irakaskuntza Gidaliburua

2026/27 ikasturtea

PJ5: Ikasketa independentea eta ikaslearen lan autonomoa.	90	0
PJ6: Ebaluazio-probak.	12	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.	10	35
ES3 Ebaluazio- eta/edo azterketa-probak.	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 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 irakasgaiaz arduratzen diren irakasleei eta tituluaren koordinazioari zuzenduta, modalitate hori hasi eta lehenengo bi asteetan.



Irakaskuntza Gidaliburua 2026/27 ikasturtea

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.

- 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-aurrezkatat (EA) joko da.

Idatzizko 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 Gidaliburua

2026/27 ikasturtea

Irakaskuntza-materiala (apunteak, aurkezpenak, gidak, zereginak...)
Ikus-entzunezko baliabideak
Irakasgaiaren material espezifikoak
Ikasgela informatizatua
Zibersegurtasun laborategia

Bibliografia eta ikasteko beste baliabide batzuk

Oinarrizko Bibliografia

- Howard, M., & LeBlanc, D. (2003). *Writing Secure Code* (2nd ed.). Microsoft Press.
- McGraw, G. (2006). *Software Security: Building Security In*. Addison-Wesley Professional.
- Howard, M., & Lipner, S. (2006). *The Security Development Lifecycle: SDL, a Process for Developing Demonstrably More Secure Software*. Microsoft Press.

Bibliografia Osagarria

- Viega, J., & McGraw, G. (2001). *Building Secure Software: How to Avoid Security Problems the Right Way*. Addison-Wesley Professional.
- Shostack, A. (2014). *Threat Modeling: Designing for Security*. Wiley.
- Saltzer, J. H., & Schroeder, M. D. (1975). *The Protection of Information in Computer Systems*. Proceedings of the IEEE, 63(9), 1278–1308.
- Martin, R. C. (2008). *Clean Code: A Handbook of Agile Software Craftsmanship*. Prentice Hall.

Gomendatutako Beste Ikaskuntza-baliabide Batzuk³

- Leithead, A., & Graham, M. (2017). *Agile Application Security: Enabling Security in a Continuous Delivery Pipeline*. O'Reilly Media.
- Allen, J. H. (2003). *Security Code Review: Finding Security Flaws*. SANS Institute.
- Viega, J., McGraw, G., & Rios, T. (2009). *Secure Programming Cookbook for C and C++*. O'Reilly Media.

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



Irakaskuntza Gidaliburua

2026/27 ikasturtea

- Zalewski, M. (2011). *The Tangled Web: A Guide to Securing Modern Web Applications*. No Starch Press.
- Eason, S., & McDermott, M. (2008). *Microsoft Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software*. Microsoft Press.
- Williams, L., & Osborne, A. (2009). *Peer Code Review to Reduce Defects in Software: A Meta-Analysis*. *Empirical Software Engineering*, 14(2), 135–165.