



Irakaskuntza Gidaliburua

2026/27 ikasturtea

Datu Orokorrak

Irakasgaia: KRIPTOGRAFIA

Titulazioa: ZIBERSEGURTASUNeko GRADUA

Mota: DERRIGORREZKOA.

ECTS kredituak: 6 ECTS

Maila: 2.

Denbora-banaketa: 2. SEIHILEKOA.

Hizkuntza: GAZTELANIA.

Irakasle-taldea: Dk. Aitor Gómez Goiri aitor.gomez@euneiz.com

Ikasgela(k): Ikasgela informatizatua

Irakasgaiaren aurkezpena:

Zibersegurtasunaren esparruan kriptografiarekin zerikusia duten kontzeptu guztiak ezagutzeko eta finkatzeko irakasgaia. Kontzeptu horiek oso garrantzitsuak izango dira ezagutzak zibersegurtasunaren esparruan zifratutako inguruneetan aplikatzeko eta inplementatzeko. Irakasgaiaren zati teorikoan hainbat kontzeptu finkatuko dira, hala nola protokoloak eta jatorrizko kriptografikoak garatzen laguntzen duten oinarri matematikoak. Praktikan, gehien erabiltzen diren protokoloak gure garapenetan segurtasunez aplikatu ahal izateko liburutegiak erabiliko ditugu.

Datu espezifikoak

Prestakuntza- eta ikaskuntza-prozesuaren emaitzak (PIE)¹

Ezagutzak edo edukiak (E)	E1	Programazio-lengoiak aztertzeke kalkulu-trebetasunak garatzeko.
	E2	Zibersegurtasun-sareen arkitekturaren mailan segurtasun-irtenbideak inplementatzeko egiturak eta protokoloak ezagutzea.
	E3	Datuen babesari eta informazioaren segurtasunari buruzko

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 zabaltzeke behar da, baina ez da iritsi behar irakaskuntza-programazioaren mugetara. Puntuz puntu aztertu beharreko gaien aurkibidea sartu behar da (garatu gabe). Gehienez hiru azpialde sar daitezke, ideia giltzarrekin/azpigaiekin Gehienez 2 orrialde izango ditu.

		ezagutzak hainbat mailatan aplikatzeko.
	E6	Birus informatikoen tipologiak identifikatzea.
	E7	Auzitegien aurkako teknikak eta horien aplikazioa ezagutzea.
	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.



Irakaskuntza Gidaliburua 2026/27 ikasturtea

- **1. unitatea** (teoria): Erroreak zuzentzeko kodeen oinarriak
 - Kode linealak eta akatsak zuzentzeko duten garrantzia.
 - Hamming-aren distantzia eta akatsak detektatzeko eta zuzentzeko duen zeregina definitzea.
 - Kode perfektuak eta baliokideak aztertzea.
- **2. unitatea** (teoria): Kode linealen egitura eta propietateak
 - Matrize sortaileak eta kontrolekoak erabiltzea kodetzeko eta deskodetzeko.
 - Kode linealen oinarrizko propietateak.
 - Adibide garrantzitsuak: Hamming kodeen aplikazioak.
- **3. unitatea** (teoria): Primalitate-probak eta zenbakizko aplikazioak
 - Zenbaki lehenak egiaztatzeko metodoak eta kontzeptuak.
 - Fermat testa eta zenbaki pseudoprimeen propietateak.
 - Miller-Rabin testaren eta zenbaki pseudoprime indartsuen hastapenak.
- **4. unitatea** (teoria): Zifratze klasikoa eta gako pribatuko sistema kriptografikoak
 - Ordezkapen-sistemak, afinitatea eta Hillen metodo kriptografikoa.
 - DES algoritmoaren hastapenak.
- **5. unitatea** (teoria): Zifratze modernoa eta gako publikoko sistema kriptografikoak
 - RSA eta ElGamal sistemen printzipioak.
 - Gako publikoko zifratzeak segurtasun modernoan dituen aplikazioak.
- **6. unitatea** (teoria): Protokolo eta tresna kriptografikoak
 - Gakoak trukatzeko Diffie-Hellman protokoloaren bidez.
 - Sinadura digitalak erabiltzea, egiazkotasuna eta arbuiorik eza bermatzeko.
- **7. unitatea** (praktikoa): Fluxuan zifratzea
 - One-time-passwords (OTP) eta haren mugak.

Irakaskuntza-metodologiak eta prestakuntza-jarduerak²

Irakasgai honetan erabilitako irakaskuntza-metodologiak honako hauek dira:

IM1	Azalpenezko metodoa.
-----	----------------------

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



Irakaskuntza Gidaliburua

2026/27 ikasturtea

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
PJ2: Praktika-klasea.	15	100
PJ3: Lanak egitea (banakakoak eta/edo taldekoak).	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.

Irakasgai honetan honako ebaluazio-sistema hauek erabili dira:

Izendapena	Gutx. hazt.	Gehi. hazt.
ES1 Ikaslearen bertaratzea eta parte-hartzea ebaluatzea.	0	5



Irakaskuntza Gidaliburua

2026/27 ikasturtea

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 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.

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).



Irakaskuntza Gidaliburua 2026/27 ikasturtea

«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.

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
Ikasgela informatizatua
Zibersegurtasun laborategia

Bibliografia eta ikasteko beste baliabide batzuk

Oinarrizko Bibliografia

- Understanding Cryptography: A Textbook for Students and Practitioners. Christof Paar et al. Springer, 2014
- Manual básico de criptología. Introducción a la ciencia del secreto. Luis Hernandez Encinas. Pinolia, 2023.
- Criptografía. Técnicas de desarrollo para profesionales. Ariel Maiorano. RA-MA S.A.



Irakaskuntza Gidaliburua 2026/27 ikasturtea

Editorial y Publicaciones, 2010.

Bibliografia Osagarria

- Aplicaciones criptográficas. Segunda edición. Jorge Ramió.
- Técnicas criptográficas de protección de datos. Amparo Fuster, Dolores de la Guía, Luis Hernández Encinas, Fausto Montoya eta Jaime Muñoz
- Criptografía y seguridad en computadores. Manuel J. Lucena López.

Gomendatutako Beste Ikaskuntza-baliabide Batzuk³

- <https://www.udemy.com/course/cursodecriptografia>
- Paredes, G. G. (2006). Introducción a la criptografía.
- Marrero Travieso, Y. (2003). La Criptografía como elemento de la seguridad informática. *Acimed*, 11(6), 0-0.

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