



Irakaskuntza Gidaliburua

2025/26 ikasturtea

Datu Orokorrak

Irakasgaia: KRIPTOGRAFIA

Titulazioa: ZIBERSEGURTASUNeko GRADUA

Mota: DERRIGORREZKOa

ECTS kredituak: 6 ECTS

Maila: 2.

Denbora-banaketa: sei hilekoa, urtea, etab. 2. SEIHILEKOA

Hizkuntza: GAZTELANIA

Irakasle-taldea: Iratxe González iratxe.gonzalez@euneiz.com

Irakasgaiaren aurkezpena:

Zibersegurtasunaren esparruan kriptografiarekin zerikusia duten kontzeptu guztiak ezagutzeko eta finkatzeko irakasgaia. Kontzeptu horiek oso garrantzitsuak izango dira ezagutzak zibersegurtasunaren esparruan enkriptatutako inguruneetan aplikatzeko eta inplementatzeko.

Datu espezifikoak

Prestakuntza- eta ikaskuntza-prozesuaren emaitzak (PIE)

Ezagutzak edo edukiak (E)	E1	Programazio-lengoiak aztertzeako kalkulu-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.
	E8	Kriptografiari eta zibersegurtasunari algoritmoak diseinatzeko teknikak eta oinarri matematikoak aplikatzea.
	E11	Malware-topologiak ezagutzeko, ondoren aztertu eta arintzeko.
	E13	Identitateen kudeaketa, zifratzea, autentifikazioa,



Irakaskuntza Gidaliburua 2025/26 ikasturtea

		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. Kriptologia, kriptografia eta kriptanalisi.
2. Kriptologia klasikoaren eta kriptologia modernoaren historia.
3. Gako publikoko eta gako pribatuko kriptosistemak.
4. Oinarrizko teknikak: zifratze-deszifratzea eta sinadura.
5. Gako pribatuko eta gako publikoko kriptologia.
6. Kriptografiaren oinarri matematikoak.

(* Garatutako edukia eskuragarri dago Unibertsitateko Campus Birtualean argitaratutako irakasgaiaren irakaskuntza-programazioan)



Irakaskuntza Gidaliburua

2025/26 ikasturtea

Irakaskuntza-metodologiak eta prestakuntza-jarduerak

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
PJ4: Tutoretzak (banakakoak eta/edo taldekoak)	5	50



Irakaskuntza Gidaliburua

2025/26 ikasturtea

PJ5: Ikasketa independentea eta ikaslearen lan autonomoa	89	0
PJ6: Ebaluazio-probak	6	100
Guztira	150	

Ebaluazioa: Ebaluazio-sistemak eta -irizpideak

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-aukera ditu irakasgaia gainditzeko:

- Etengabeko ebaluazioa, urtean 2 deialditan: ohikoa eta ezohikoa.
- Ebaluazio bakarra, urteko deialdi batekin.
- Euneiz Unibertsitatean, ebaluazio jarraitua (irakasleek definitutako irakasgaiaren jardura ebaluagarrien batez besteko haztatua) funtsezko ebaluazioa da, baina Euneizek ebaluazio bakarra egiteko aukera ematen dio ikasleari (azterketa bakarra).
- Ezin da aldatu ikasturtean zehar ikasleak hautatutako ebaluazio-sistema.
- Ebaluazio bakarrari heldu nahi dion ikasleak idatziz eskatu beharko du, justifikatu dezan, irakasgaiaren ardura duten irakasleei eta tituluaren koordinazioari zuzenduta, ikasturtea hasten den lehenengo bi asteetan.
- Ikaslearen % 80 eskola presentzialetara joaten ez bada, ezingo da ohiko deialdira aurkeztu eta automatikoki ezohiko deialdira igaroko da.



Irakaskuntza Gidaliburua 2025/26 ikasturtea

- Hutsegiteak irakasgaiaren ardura duen irakasleari justifikatu behar zaizkio.
- Salbuespen gisa, irakasgaiaz arduratzen den irakasleak beste irizpide osagarri batzuk ere erabili ahal izango ditu, hala nola ikaslearen parte-hartzea, jarrera, jardun- eta aprobetxamendu-maila eta abar, ikasleak deialdi arruntean jarraitzeko aukera izan dezan, baldin eta gutxieneko bertaratzea % 70etik gorakoa bada.
- Ikaslea ezohiko ebaluaziora joango da BAKARRIK suspenditutako zatiekin.
- 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 da.
- Ebaluazio-jarduerarik egiten ez duen ikasle matrikulatua ez-aurrezkatat (EA) joko da.
- Idatzizko ebaluazio-jarduera orok (lanak, azterketak...) ortotipografia-hutsegiteak hartuko ditu kontuan azken kalifikazioan.
- Plagioa debekatuta dago, bai lanetan, bai azterketetan; antzemanek gero, kalifikazioa gainditu gabe geratuko 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.
 - % 30etik gorako antzekotasun-indizea duen edozein lan ez da ebaluatuko.

Bibliografia eta ikasteko beste baliabide batzuk

Oinarrizko Bibliografia

- Understanding Cryptography: A Textbook for Students and Practitioners. Christof Paar et al.



Irakaskuntza Gidaliburua

2025/26 ikasturtea

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. 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 Batzuk

- <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.