Mondragon Unibertsitatea

ZIBERSEGURTASUNEAN ETENGABEKO PRESTAKUNTZAKO MASTERRA (ONLINE)

Merkatuak informazioaren segurtasunaren arloan (IT) eta ingurune industrialetako segurtasunaren arloan (OT) trebatutako profesionalak behar ditu ezinbestez, eta merkatuaren eskaera zorrotz horri erantzuten dio Zibersegurtasun Masterrak

GAIA	Informatika, Telekomunikazio Sistemak eta Sistema Txertatuak
ECTS/ORDUAK	60 ECTS
EGUTEGIA	2025/10/17 - 2026/07/17 Or
HIZKUNTZA	Gaztelania
MODALITATEA	Online

Informazio gehiago eta izen-ematea

AURKEZPENA

Zibersegurtasuneko masterra teknologiaren arloko profesionalentzat eta informazioaren segurtasunaren arloan espezializatu nahi duten tituludun berrientzat da. Praktikak egiteko aukera eta proiektua enpresan.

Master honek informazioaren segurtasunaren arloan prestatutako profesionalen merkatuaren eskaera zorrotzari erantzuten dio.

NABARMENTZEN DUGU

- **Hautazko praktikak enpresan**
- **Ikaskuntza praktikoan oinarritutako metodologia**
- **Online formatua 100%ean**
- **Master amaierako proiektua enpresan aplikatuta**

KONTAKTUA

KONTAKTURAKO PERTSONA

AINHOA GORONAETA
+34 664 266 716
cursosingenieria@mondragon.edu

HELBURUAK

Master honen helburu nagusia da partaideei ezagutza, trebetasun praktikoak eta beharrezko konpetentziak ematea enpresatan zibersegurtasunaren elementuak txertatu ahal izateko.

Prestakuntzako Programak segurtasunaren arloan goraka doazen arazoen proaktiboki jokatzen irakasten die partaideei, hainbat erantzun alternatibo planteatuz eta emaitza posibleak aurreikusiz, agertzen ari zaizkigun azken-azken segurtasun mehatxuei modu eraginkorrenean erantzun ahal izateko.

Horretarako, konpetentzia hauek landuko dira:

- Segurtasun perimetraleko soluzio guztien ezaugarriak ezagutzea eta ulertzea.
- Soluzio kriptografikorik sendoenak ezagutzea eta ulertzea, eta euren erabileraren egokitasunari buruzko erabakiak argudiatzea.
- Sare eta interneteko azpiegiturek dituzten mehatxu informatiko garrantzitsuenak eta ahultasunak antzematea.
- Softwarean edo sare azpiegituretan ahultasunak antzemateko gai izatea.
- Segurtasun informatikoko auditoria prozedura bat diseinatu, inplementatu eta exekutatzeko gai izatea.
- Ahultasunen analisia egiteko eta gertaerak ikuskatzeko tresna nagusiak ezagutzea.
- Gertakarien analisirako alderdi metodologikoak ezagutzea.
- Erabaki egokiak hartzeko gai izatea, segurtasun gertakari bat jasotzen denean, horiek antzemateko eta ebazteko kontzeptuak eta tresnak aplikatuz.
- Hainbat arlo eta aplikaziotan softwarearen garapen sendoa egiteko teknikak ezagutzea.
- Informazioaren Segurtasun Kudeaketa Sistema bat ezartzeko prozedura ezagutzea.
- Ezbeharrak gertatzen direnean onera egiteko dauden metodologiak barneratzeko gai izatea.
- Datu pertsonalen babeserako indarrean den legedia (DPBL) eta jabetza intelektualaren legea edo Informazioaren eta Merkataritza Elektronikoaren Gizartearen Zerbitzuen Legea (IMEGZL) ezagutzea.
- Datuak prozesatzeko zentroetan (CPD) segurtasun fisikoko arriskuak gutxitzeko aplikatu beharreko teknologiak ezagutzea.
- Segurtasun kopiak egiteko egun dauden teknologiak ezagutzea eta bereiztea.
- Ingurune industrialetan zibersegurtasun arloan egun dauden arriskuak eta arrisku horiek gutxitzeko diren mekanismoak xehetasunez ezagutzea.
- Gauzen interneta (IoT) darabilten tresnek eragin ditzaketen segurtasun arazoak identifikatzea.

NORI ZUZENDUA

Zibersegurtasun-arriskuen tratamenduan espezializatu nahi duten teknologia-profesionalentzat eta/edo industria-prozesuentzat da master hau, baita azaleratzen ari den sektore horretara bideratu nahi duten tituludun berrientzat ere..

Master hau ondorengo tituludun profesionalentzat zuzenduta dago:

Ingeniería informática, telecomunicaciones o matemáticas y diferentes títulos de la rama de la ingeniería y ciencias con especialidades próximas a las redes y la computación

Ciclo formativo de grado superior en informática o similares con experiencia de 3 años en el sector (Para el reconocimiento de la experiencia profesional se solicitará se entregue CV, vida laboral y se realizará una entrevista).

Carlos Lacasa

bideoa:

PROGRAMA

M1 Fundamentos de redes y sistemas

- Redes de comunicaciones
- Programación y sistemas
- Bases de datos

M2 Criptografía

- Criptografía de clave simétrica y asimétrica
- Funciones hash
- Firma digital
- Blockchain
- Criptografía post-cuántica

M3 Seguridad en redes

- Seguridad en el nivel físico y de enlace
- Seguridad en el nivel de red
- Seguridad en el nivel de transporte
- Seguridad en el nivel de aplicación
- Seguridad WIFI

M4 Seguridad del Software

- Vulnerabilidades y ataques habituales
- Programación segura
- Herramientas de análisis

M5 Seguridad de Sistemas y Cloud

- Gestión de indentidades y control de accesos
- Seguridad en entornos Linux
- Seguridad en entornos Windows

- Seguridad Cloud
- Seguridad en contenedores (Dockers)
- Seguridad de Bases de Datos

M6 Hacking ético y auditoría de seguridad

- Técnicas de hacking
- Pivoting y movimientos laterales
- Análisis de vulnerabilidades
- Auditoría de seguridad

M7 Mecanismos de protección y defensa

- Cortafuegos y segmentación de redes
- Endpoint Protection
- IDS/IPS
- Zero Trust
- MFA
- Seguridad física del CPD
- Copias de seguridad

M8 Gestión de incidentes de ciberseguridad

- Cyber Threat Intelligence
- Threat Hunting
- SIEM
- Gestión de incidentes
- Máquinas trampa
- Análisis forense

M9 Ciberseguridad industrial e IoT

- Seguridad en entornos industriales
- Seguridad en IoT
- Seguridad del hardware
- Norma IEC 62443

M10 Sistemas de gestión de la ciberseguridad y aspectos legales

- Sistemas de Gestión de la Seguridad de la Información (ISO 27000)
- Análisis de Riesgos
- Legislación y normas

POPBL: Project Oriented Project Based Learning

TFM: Trabajo Fin de Máster

METODOLOGIA

Programaren garapenean, IRAKASKUNTZA AKTIBOA erabiliko da irizpide orokor gisa, Funtsean, prozesu parte hartzailea izango da, non ikasketen jarraipena eta kontrola egingo baita, partaideek edukiei eta

jarduerei ahalik eta probetxurik handiena ateratzea bermatzeko. Irakaskuntza – ikaskuntza prozesua kontzeptu metodologiko hauetan oinarrituko da:

- Planteamenduaren eta kontzeptu teorikoen azalpena.
- Lantaldean kasu praktiko eta ariketak egitea.
- Laborategiko praktikak.
- Enpresaren testuinguruan aplikatzea.
- Enpresan proiektu erreala burutzea.

Masterrak 15 modulu ditu, eta Master Amaierako Proiektua. Modulu bakoitzak hainbat gai ditu, eta gai bakoitzak, berriz, ikasteko hainbat eduki eta ariketa ditu. Gai bakoitzaren ordu kopurua da partaide bakoitzak gaia ondo bukatzeko gutxi gorabahera guztira egin beharko dituenak. Modulu bakoitzak azken ebaluazio bat izango du.

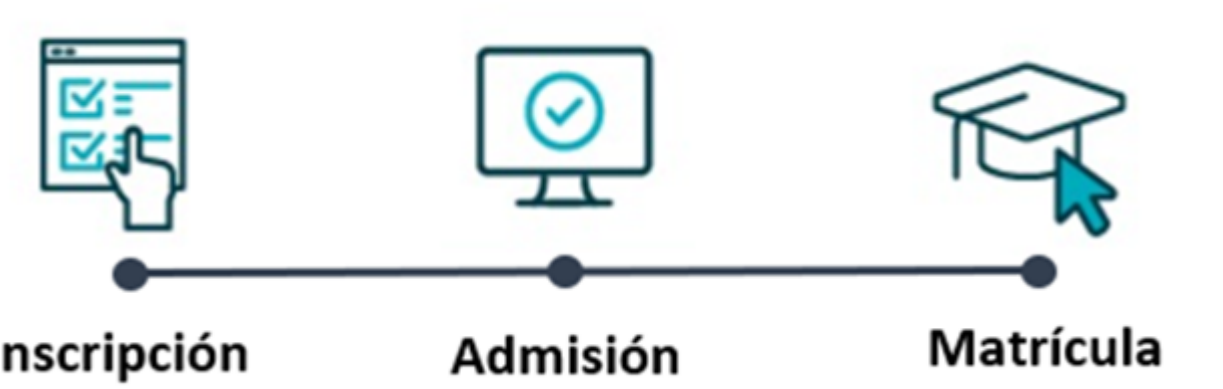
Gai bakoitzak tutore bat izango du, eta tutore horrek partaideei lagunduko die, gidari lanak eginda eta ikasleak parte hartzera bultzatuta, lan egiten egongo diren egunetan. Tutorea, halaber, gai bakoitzaren edukien arduradun izango da, eta partaideen zalantzak argitu behar ditu, eta azken ebaluazioa egin.

Proiektuak ikaskuntza katalizatzea ahalbidetuko du, emaitza jakin batzuk lortzera bideratuta. Proiektu hori Masterreko irakasle batek gainbegiratuta egongo da, eta amaiera gisa planteatzen da parte hartzaile bakoitzak proiektua zabaltzeko/batera jartzeko saio bat egitea.

ONARPEN BALDINTZAK ETA PROZESUA

Zibersegurtasuneko Masterraren onarpen prozesuak hiru fase ditu, ikastaroa hasi aurreko hilabeteetan egingo direnak (izen-ematea -“onarpena-–matrikula”):

1.



Inskripzioa

- Aurreinskripzioa web orrialde honetatik egin behar da
- Izena emateko eta NAN/AIZ igotzeko esteka duen mezu elektroniko bat bidaliko dizugu
- NAN/DNI baliozkotuko dugu, eta falta den dokumentazioa igo ahal izango duzu: CV eta unibertsitate-tituluak

Izena emateko epea zabalik egonen da lanpostuak bete arte.

2. Onarpena

Jasotako dokumentazioa ebaluatuko dugu; lehentasuna emanen zaie sarrerako espezialitateetako unibertsitate-tituludunei eta haien esperientzia profesionalari, bereziki master honen esparruan. Hiru onarpen fase egongo dira:

- 2023ko maiatzaren 15ean, maiatzaren 12a baino lehen egindako izen-emate guztietan..
- 2023ko ekainaren 15ean, ekainaren 12a baino lehen egindako izen-emate guztietan.
- 17 de julio de 2023 para todas las inscripciones realizadas antes del 14 de julio.

3. Matrkula

Matrikula online egiten da unibertsitateak emandako estekatik, onartu ondoren. Masterraren lehen kuota ordainduta formalizatuko da matrikula..

LEKUKOTZAK

David Barroso

Fundador de CounterCraft

Nadie puede dudar hoy en día de la importancia de la ciberseguridad en nuestro día día. Cada vez estamos más conectados y somos más dependientes de la tecnología, lo que provoca que existan más riesgos relacionados con la ciberseguridad. No importa el sector, tipo de empresa o gobierno; cada vez son más necesarios profesionales que puedan aportar conocimiento y experiencia en esta temática. Si te gusta la tecnología, estar al día con las últimas noticias, y enfrentarte continuamente a desafíos, esta es tu oportunidad.

Gerard Vidal

CEO de Enigmedia

Las empresas necesitan crecer y medir riesgos. La ciberseguridad es un nuevo campo lleno de amenazas pero también de nuevas oportunidades, donde las empresas pueden y deben colaborar para ser más competitivas y obtener un beneficio mutuo.

Roberto Velasco Sarasola

CEO

La transformación de las empresas hacía el mundo digital han convertido a los sistemas de información en elementos primarios sin los que una empresa literalmente puede dejar de funcionar. Uniendo a esta realidad el aumento de los incidentes de cyberseguridad con el todavía muy bajo nivel medio de protección de las empresas, estimamos que va a ser necesario la incorporación de personal cualificado en cyberseguridad para hacer frente a esta nueva situación.

César Tascón

Socio PwC. Responsable Ciberseguridad Industrial

La ciberseguridad es ya una de las principales preocupaciones de los directivos de todas las organizaciones, porque reconocen el impacto que les puede causar pero necesitan confort en que han tomado las decisiones adecuadas para proteger a su organización. Los datos que manejan, sus procesos cada vez más digitales o el mundo industrial necesitan ser sujetos a actividades de ciberseguridad continuas, rigurosas y adaptadas a sus necesidades para garantizar su correcto funcionamiento.

Jesús Urien

Director PwC. Responsable Business Security Solutions en Euskadi y Navarra

La transformación digital es un proceso que las organizaciones deben afrontar para poder ser competitivas y ofrecer valor diferencial a sus clientes. En este escenario, disponer de una función de ciberseguridad con las capacidades adecuadas se convierte en un aspecto esencial. Serán necesarios profesionales que combinen el conocimiento del negocio y tecnologías propias de los diferentes sectores industriales con capacidades organizativas y técnicas en ciberseguridad. Poder conocer la experiencia y casos de éxito profesionales que han comenzado ya este camino diversas organizaciones, será un apoyo extraordinario para una nueva generación de profesionales de referencia en el ámbito de la ciberseguridad industrial.

JASOKO DEN TITULAZIOA

Ebaluazioaren baldintzak bete eta ikasketak behar bezala egiaztatu dituzten parte-hartzaile guztiek Mondragon Unibertsitatearen ZIBERSEGURTASUNEKO MASTER PROFESIONALEKO titulua eskuratuko dute.

UNIBERTSITATE-ENPRESA ERLAZIOA

Lanean ari den profesionala bazara, masterraren garapena eta zure enpresan egiten duzun lana uztartu ahal izango d

Gaur egun lanean ari ez bazara, egunean 4 orduko praktikak egingo dira enpresa laguntzaileetan. Enpresek finantzatu

PLAZAK

20 toki

Gehienez ere 20 lagun sartzen dira, prestakuntza horrek eskatzen duen arreta pertsonalizatua eman ahal izateko.

IRTEERAKO PROFILA

Zibersegurtasuneko Masterra amaitzean, parte-hartzaileak hainbat esparrutan egin dezake lan:

- *Responsable de Sistemas Informáticos*
- *Responsable de Seguridad IT y OT*
- *Director de Proyectos de Seguridad*
- *Integrador de Sistemas de Seguridad*
- *Técnico de Seguridad*

- *Consultor de Seguridad*
- *Auditor de Seguridad*
- *Analista de Seguridad*
- *Administrador de redes y sistemas*

PRAKTIKAK ETA PROIEKTUA

Mondragon Unibertsitateak partaideek enpresa laguntzaileetan praktika ordainduak egitea sustatzen du, eta horrek masterreko ikasketak finantzatzea errazten du; masterraren hasieratik, lanean ari ez diren parte-hartzaileek egunean 4 orduko praktikak egingo dituzte enpresa laguntzaileetan. Enpresek finantzatutako beka hau hilean 600 €ingurukoa da.

Lanean ari diren parte-hartzaileei alderdi hau onartuko zaie.

IOT y OT bideoa

KOLABORATZAILEAK/ BABESLEAK

Zibersegurtasun Masterra Gipuzkoako Foru Aldundiak eta Mondragon Unibertsitateak antolatua da, eta segurtasun informatikoaren arloko enpresa garrantzitsuen laguntza du, esaterako, hauena: S21sec, ITS-security, Countercraft, Tinanium Security…

PREZIOA

8.400 €

2025-26 ikasturterako aurreikusitako zenbatekoa

60 ECTS

Kantitate hau ordainketa bakarrean edo zatika ordaindu ahalko da.

Lehen ordainketa onartua izandakoan (900€)

- Gainontzekoa **ordainketa bakarrean**
- Gainontzekoa **hilabetero**

Ikasleari baja ematen bazaio ikastaroaren baldintzak aldatzeagatik (datak, ordutegiak edo formatua aldatzea), hasierako kuotaren %100 itzuliko zaio. Beste arrazoi batzuengatik baja emanez gero,% 50 itzuliko da eskolak hasi arte. Eskolak hasi ondoren, hasierako kuota ez da itzuliko.

INFORMAZIO GEHIAGO

Informazioa jaso nahi baduzu edo edozein zalantza argitu nahi baduzu, idatzi helbide elektroniko honetara: cursosingenieria@mondragon.edu edo deitu 664266716 telefonora.

KONTAKTURAKO PERTSONA

AINHOA GORONAETA
+34 664 266 716
cursosingenieria@mondragon.edu
