

## DATUEN ANALISIA, ZIBER SEGURTASUNA ETA KONPUTAZIOA LAINOAN MASTERRA MÁSTER EN ANÁLISIS DE DATOS, CIBERSEGURIDAD Y COMPUTACIÓN EN LA NUBE

Koordinatzailea / Coordinador:  
**Urko Zurutuza**  
[uzurutuza@mondragon.edu](mailto:uzurutuza@mondragon.edu)

### IKASLEAREN PROFIL PROFESIONALA

Unibertsitateko master honek gaur egungo, profil profesionala eskuratzeko aukera eskaintzen die ikasleei. Ezagutzaren abangoardian dauden hiru arlo teknologiko integratuta ditu masterrak. Ikasturtearen amaieran eta masterraren erdian ikasleak hurrengo egiteko gai izan behar du:

- Datuen balioa lortu, diseinatuz eta honen bizitza ziklo osoa kudeatuz.
- Ziber-segurtasuna osorik kudeatzea, bai antolaketa mailan, bai produktu eta zerbitzuen mailan.
- Softwareak eta azpiegiturak optimizatzeko eta garatzeko prozesuen antolakuntzan eta kudeaketan laguntzen duen enpresak duen balioa ezagutu.
- Azpiegitura seguruak zabaldu eta kudeatu eta bertan sortutako datuak ustiatu.



### PRESTAKUNTZAKO EZAGUTZA-ARLOAK

Masterrean eskuratutako ezagutzak hiru arloetan sailkatzen dira:

#### DATUEN ANALISIA

- Datuak diseinatzea, garatzea eta ezartzea datuak prestatzeko eta sailkatzeko teknikak, datuak aurreratzeko, sailkatzeko eta taldean sailkatzeko, ezagutzak erazteko sortutako ereduak interpretatu eta balioztatu ahal izateko.
- Datuen ingestazioa, biltegitratzea eta prozesatze paraleloaren bidez Big Data teknologiak erabiliz prozesua diseinatu, garatu eta abian jartzea.
- Diseinatu, garatu eta ezarri multi-sare neuronal bat (Deep Learning) datuen izaerari eta zereginaren xedeari erantzuteko.
- Datuen irudikapenaren ereduak diseinatu, garatu eta inplementatu euren izaeraren arabera eta horiek interpretatzeko ezagutza ateratzeko.

#### ZIBER-SEGURTASUNA

- Sistema eta sareen mehatxuak ordenagailuen aitortu, ahuleziak eta lehendik dauden segurtasun irtenbideak ezagutzea.

### PERFIL PROFESIONAL DEL ALUMNO/A

Este máster ofrece al alumnado la posibilidad de adquirir un perfil profesional actual, completo y demandado, donde se integran tres áreas tecnológicas que están en la vanguardia del conocimiento. Al final del año y medio del máster el alumnado deberá:

- Ser capaz de obtener valor del dato, diseñando, implementando y gestionando todo el ciclo de vida del mismo.
- Gestionar la ciberseguridad en su totalidad, tanto a nivel de organización como al de los productos y servicios.
- Conocer el valor que aporta en una empresa la organización y gestión de los procesos de desarrollo, despliegue y optimización de software e infraestructuras.
- Ser capaz de desplegar y gestionar infraestructuras seguras, y explotar los datos producidos en la misma.



### ÁREAS DE CONOCIMIENTO DE SU FORMACIÓN

Los conocimientos adquiridos en el máster se clasifican en tres áreas:

#### ANÁLISIS DE DATOS

- Diseñar, desarrollar e implementar técnicas de preprocesamiento y modelado de datos para predecir, clasificar y agrupar los mismos, siendo capaz de interpretar y validar los modelos creados para la extracción del conocimiento.
- Diseñar, desarrollar e implementar el proceso de ingesta, almacenamiento y procesamiento paralelo de datos mediante tecnologías Big Data.
- Diseñar, desarrollar e implementar una red neuronal multi-capas (Deep Learning) para responder a la naturaleza de los datos y el objetivo de la tarea.
- Diseñar, desarrollar e implementar el modelo de la representación de los datos según su naturaleza e interpretar las mismas para extraer conocimiento.

#### CIBERSEGURIDAD

- Reconocer las principales amenazas informáticas, vulnerabilidades y soluciones de seguridad existentes a nivel de sistemas y redes.

## PRESTAKUNTZAKO EZAGUTZA-ARLOAK

- Softwarea ikuskatzea, segurtasun ahuleziak bilatzeko aukera ematen duten tresnak erabiliz eta software seguruagoak garatzeko euskarri izatea.
- Ziber segurtasunari buruzko legeria eta araudia ulertzea, hala nola, estandarrak, datu pertsonalen babesa eta gertakariei erantzuna.

### GARAPEN ETA OPERAZIOAK (DEVOPS)

- "Cloud plataformetan" oinarritutako zerbitzuak garatu eta zabaltzeko prozesua automatizatu.
- Softwarea garatzeko eta probatzeko aukera ematen duten garapen ingurune bat eskaini ekoizpen-antzeko inguruneetan.
- Azpiegitura bat eskaintzeko SW inplementazioak prozesu errepikagarri eta fidagarrien bidez burutzeko.
- SW produktuaren funtzionamenduaren kalitatea kontrolatzeko eta balioztatzeko tresnak eskaintzea.

## PROIEKTU TIPOLOGIA

Hona hemen proiektu esanguratsuak:

### -DATA-ANALISIA:

- Mantentze prediktiboa:
  - Prophesy, Productive 4.0, Mantis.
- Produktuaren kalitatea vs. prozesua:
  - MC-Suite, Data Fabric, Edermine, iMetal Pro.
- Monitorizazioa
  - Plenisense, Central Cloud, Basic Internet.
- Iragarpena / optimizazioa:
  - Precoz, Edar4.0.
- Osasun datuen analisia:
  - OMEGA3, Cardiodata, Optimus, Healsys II.

### ZIBER-SEGURTASUNA

- Segurtasuna CS/SCADA:
  - SEKUTEK, SIND, IS\_INCLOUD
- Sistema Txertatuen segurtasuna:
  - Azterketarako zailtasunak CNC Fagor Automation
  - Elkarlaneko ikerketa con Orona
- Segurtasuna Cloud y Big Data:
  - Datuen babesa CP-ABE bidez, Hadoop ingurunean banatuta (Prophesy, Productive, MC-SUITE, BID3A)
  - Smart phone security (SIMPLE, Malandro)
  - Spam & text fraud detection (SocialSpam, Ski4spam)

### GARAPEN ETA OPERAZIOAK (DEVOPS):

- SW kontrolatzeko edukiontzia zabaltzea:
  - TESTOMAT
- Micro-zerbitzuak eta Cloud Computing:
  - Cloud Computing diseinua eta ezarpena.
    - TEKINTZE
  - Cloud arkitekturaentzako mikro-zerbitzuak erregistratzea, osatzea eta aurkitzea.
    - SMARTENCITY
  - Interoperabilitatea gailuen artean web zerbitzuak erabiltzea Cloud arkitekturak batera.
    - PRODUCTIVE 4.0
  - Elkarreragingarritasun plataformak eta biki digitalak ho-deian.
    - PING

## ÁREAS DE CONOCIMIENTO DE SU FORMACIÓN

- Ser capaz de auditar software, utilizando herramientas que permitan la búsqueda de vulnerabilidades de seguridad y poder apoyar en el desarrollo de software más seguro.
- Comprender la legislación y normativa existente en materia de ciberseguridad, como son los estándares, la protección de datos personales y la respuesta a incidentes.

### DESARROLLO Y OPERACIONES (DEVOPS)

- Automatizar el proceso de desarrollo y despliegue de servicios basados en "plataformas cloud".
- Ofrecer un entorno de desarrollo que permita desarrollar y testear el software en entornos similares a producción.
- Ofrecer una infraestructura para realizar despliegues del SW mediante procesos repetibles y fiables.
- Ofrecer herramientas que permitan supervisar y validar la calidad operativa del producto SW.

## TIPOLOGÍA DE LOS PROYECTOS

A continuación, se muestran algunos proyectos significativos:

### ANÁLISIS DE -DATOS:

- Mantenimiento predictivo:
  - Prophesy, Productive 4.0, Mantis.
- Calidad de producto vs proceso:
  - MC-Suite, Data Fabric, Edermine, iMetal Pro.
- Monitorización:
  - Plenisense, Central Cloud, Basic Internet.
- Predicción/Optimización:
  - Precoz, Edar4.0.
- Análisis de datos en salud:
  - OMEGA3, Cardiodata, Optimus, Healsys II.

### CIBERSEGURIDAD:

- Seguridad ICS/SCADA:
  - SEKUTEK, SIND, IS\_INCLOUD
- Seguridad de Sistemas Embebidos:
  - Análisis Vulnerabilidades CNC Fagor Automation
  - Investigación Colaborativa con Orona
- Seguridad Cloud y Big Data:
  - Protección del dato mediante CP-ABE, distribuido en entorno Hadoop (Prophesy, Productive, MC-SUITE, BID3A)
  - Smart phone security (SIMPLE, Malandro)
  - Spam & text fraud detection (SocialSpam, Ski4spam)

### DESARROLLO Y OPERACIONES (DEVOPS):

- Despliegue de contenedores para SW de control:
  - TESTOMAT
- Microservicios y Cloud Computing:
  - Diseño e implementación de arquitecturas Cloud.
    - TEKINTZE
  - Registro, composición y descubrimiento de Microservicios para arquitecturas Cloud.
    - SMARTENCITY
  - Interoperabilidad entre dispositivos mediante el uso de servicios web en combinación con arquitecturas Cloud.
    - PRODUCTIVE 4.0
  - Plataformas de interoperabilidad y gemelos digitales en la nube.
    - PING