

## Ikastaroa Segurtasun-gorabeherak (on line)

Gaia Informatika, Telekomunizio Sistemak eta Sistema Txertatuak

ECTS/orduak 100 ORDU

Egutegia 2017/05/01 - 2017/05/21 As-At-Az-Og-Or

Ordutegia 08:00-18:00

Hizkuntzak Gaztelania

Modalitatea Online

Prezioa 625 €

### Helburuak

"Erakundearen barruan segurtasun informatikoa hobeto kudeatzeko aukera emango duten segurtasun-politikak garatu ahal izatea.

"Informazio sistema batek eta harekin lotutako inguruneak dituen arriskuak aztertzea, hau da, kaltea edo kaltea gertatzeko arriskua.

"Segurtasun informatikoko arriskuak prebenitzeko, saihesteko, murrizteko edo kontrolatzeko hartu behar diren neurri egokiak ezagutzea.

"Jarraipen-mekanismoak arrakastaz ezartzeko gai izatea.

"Erakundearen segurtasun maila ebaluatzeko eta hobetu beharreko alderdiak identifikatzeko gai izatea.

### Nori zuzendua

Segurtasun informatikoko arduradunak.

Sare eta sistemen administratzaileak.

Informatikako teknikariak.

### Egitaraua

- Gorabeheren kudeaketa
  - Gertaerei erantzuteko taldeak
    - CERT
- Gertaerei erantzuteko prozedura
  - Prestakuntza

- Detekzioa eta analisisa
- Gertakaria ezabatzea eta berreskuratzea
- Gertakariaren ondorengoa: gertakarien txostena
- Tresnak
  - RTIR: Request Tracker for Influent Response
  - OTRS: Open Ticket Request System
- Baimenik gabe sartzeko saiakerak atzematea
  - Definizioak
  - IDSen historia
  - Sailkapena
    - Informazio-iturriak
- Host Based Intrusion Detektatzea (HIDS)
- Network Based Intrusion Detection (NIDS)
- Azterketa-metodoak
  
- Arazoak detektatzea
- Denbora
- IDS denbora errealean
- IDS Batch-en
- Erantzuna
- Pasiboa
- Aktibo (IPS)
- Gertaeren korrelazioa
- Tresnak
- Nortasun-agiri nazionala
- OSSEC
- Samhain
- Prelude/OSSIM
- Tranpa sistemak: honeypots eta honeynets
  - Definizioak

#### Abantailak eta eragozpenak

- Tranpa sistemen sailkapena
  - Helburuaren arabera
  - Elkarrekintza-mailaren arabera
- Tranpa sistemen arkitektura
  - Tranpa fisikoak
  - Tranpa birtualen sistemak
  - Datuak hartzea
- Honeynet-ak edo tranpa-sareak
- HoneyClients
- Auzitegi-azterketa

- Definizioak
  - Auzitegiko informatika: Locard-en trukearen printzipioa
  - Ebidentzia digitala
  - Krimenaren tokia
- Gertaera baten aurreko urratsak
  - Aurregertakaria
  - Gorabehera detektatzea
  - Ikerketa (Metodologiak)
  
- Krimenaren eszena
- Ebidentziak biltzea
- Ebidentzien interpretazioa
- Hipotesia eta azken txostena egitea
  
- Legedia
  - Auzitegi ondoko ekintzak
- Tresnak
  - Ebidentziak biltzeko
  - Auzitegi-azterketarako
  - Live CDak

## **Irakasleak**

Fernández Arrieta, Miguel

Lizarraga, Jesús

Lizarralde, Miren Osane

Perez Reguera, Itziar

Uribeetxeberria Ezpeleta, Roberto

Velez De Mendizabal, Iñaki

Zurutuza Ortega, Urko

---

<https://www.mondragon.edu/cursos/en/topics/informatics/course/incidentes-de-seguridad-online>