

CURSO ONLINE EN INCIDENTES DE SEGURIDAD (ONLINE)

TEMÁTICA	Informática, Telecomunicaciones y Sistemas Empotrados
HORAS/ECTS	100 HORAS
CALENDARIO	01/05/2017 - 21/05/2017 Lun-Mar-Mie-Jue-Vie
IDIOMA	Español
MODALIDAD	Online

**Más información
e inscripción**

OBJETIVOS

- " Poder desarrollar políticas de seguridad que permitan una mejor gestión de la seguridad informática dentro de la organización.
- " Estudiar los riesgos que soporta un Sistema de Información y el entorno asociado con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio.
- " Conocer las medidas apropiadas que deberían adoptarse para prevenir, impedir, reducir o controlar los riesgos de seguridad informática.
- " Ser capaz de implantar con éxito mecanismos de seguridad.
- " Ser capaz de evaluar el nivel de seguridad de la organización e identificar los aspectos a mejorar.

DIRIGIDO A

Responsables de Seguridad Informática.
Administradores de Redes y Sistemas.
Técnicos informáticos.

PROGRAMA

- Gestión de Incidentes
 - Equipos de respuesta a incidentes
 - CERT
- Procedimiento de respuesta a incidentes
 - Preparación
 - Detección y Análisis
 - Eliminación y Recuperación del incidente
 - Post-Incidente: Informe de incidentes

- Herramientas
 - RTIR: Request Tracker for Incident Response
 - OTRS: Open Ticket Request System
 - Detección de intrusiones
 - Definiciones
 - Historia de los IDS
 - Clasificación
 - Fuentes de Información
 - Host Based Intrusion Detection (HIDS)
 - Network Based Intrusion Detection (NIDS)
 - Métodos de Análisis
-
- Detección en Anomalías
 - Tiempo
 - IDS en Tiempo Real
 - IDS en Batch
 - Respuesta
 - Pasiva
 - Activa (IPS)
 - Correlación de Eventos
 - Herramientas
 - Snort NIDS
 - OSSEC
 - Samhain
 - Prelude/OSSIM
 - Sistemas trampa: honeypots y honeynets
 - Definiciones
 - Ventajas e Inconvenientes
 - Clasificación de los Sistemas Trampa
 - Según su objetivo
 - Según su nivel de interacción
 - Arquitectura de los sistemas trampa
 - Sistemas trampa físicos
 - Sistemas trampa virtuales
 - Captura de datos
 - Honeynets o redes trampa
 - HoneyClients
-
- Análisis forense
 - Definiciones
 - Informática Forense: El principio de intercambio de Locard
 - Evidencia Digital
 - Escena del Crimen
 - Pasos ante un Incidente
 - Pre-incidente
 - Detección del Incidente
 - Investigación (Metodologías)
-
- La Escena del Crimen

- Recogida de Evidencias
- Interpretación de las Evidencias
- Elaboración de la Hipótesis e Informe Final
 - Legislación
 - Acciones post-forense
 - Herramientas
 - Para la Recolección de Evidencias
 - Para Análisis Forense
 - Live CDs

PROFESORADO

Fernandez Arrieta, Miguel

Lizarraga Durandegui, Jesus Maria

Lizarralde Urrutia, Miren Osane

Perez Reguera, Itziar

Uribeetxeberria Ezpeleta, Roberto

Velez De Mendizabal Gonzalez, Iñaki

Zurutuza Ortega, Urko

<https://www.mondragon.edu/cursos/es/curso/incidentes-de-seguridad-online>