Protección contra amenazas y malware

PROTECCIÓ CONTRA AMENACES I MALWARE

PDI-PAS | Formació En línia | Espanyol | 12 (10+2) hores | Edició IV

PDI-PAS | Formación En línea | Español | 12 (10+2) horas | Edición IV

PLANIFICACIÓ DE L'ACCIÓ FORMATIVA – *Planificación de la acción formativa*

Sessió Sesión	Data Fecha	Horari Horario	Lloc Lugar
1	08/02/2021	10:00 – 12:00	En línea síncrono
2	01/03/2021	Asíncrona	Finalización del curso
3	Desde el 08/02/2021 y hasta el 01/03/2021 el curso se desarrollará en modalidad asíncrona vía Aula Virtual		

PROFESSORAT DE L'ACCIÓ FORMATIVA – *Profesorado de la acción formativa*

Ramón Onrubia Pérez

Ingeniero Superior de Telecomunicación por la UPV y docente en formación profesional superior desde el año 2005, así como profesor asociado en la universidad durante varios años. Es coordinador y profesor del curso de especialización de FP de ciberseguridad en el CIPFP de Mislata e imparte cursos de ciberseguridad para el profesorado de FP de la comunidad valenciana. Es instructor Cisco y formador de instructores Cisco desde el año 2006 y posee varias certificaciones industriales de seguridad (CCNA Security, Cisco CyberOps). Actualmente se está preparando para el CCIE Security. Es autor de publicaciones relacionadas con la seguridad y ha participado en distintos eventos y congresos relacionados con la ciberseguridad.

OBJECTIUS FORMATIUS I CONTINGUTS – *Objetivos formativos y contenidos*

El objetivo general que pretende esta acción formativa es dotar al participante de una visión general del panorama actual de amenazas y software malicioso (malware) existente en Internet y darle a conocer distintas herramientas de protección contra las

mismas así como un manual de recomendaciones y buenas prácticas en el uso de herramientas TIC e Internet.

CONTENIDO FORMATIVO:

- Amenazas de internet:
  - Scam, spam, hoax, phising, smishing, vishing, web skimmers, carding, site spoofing, man in the browser, sexting, grooming, DDoS, etc.
- Tipos de software malicioso (malware):
  - APTs, ransomware y criptovirus, rogueware, troyanos bancarios, botnets, keyloggers, spyware, dialers, worms, backdoors, etc.
- Impacto y riesgos del malware en el entorno empresarial y personal.
- Herramientas y medidas de alerta y protección contra amenazas:
  - Medidas de seguridad activa
  - Medidas paliativas
  - Concienciación y formación
  - Centros de respuesta ante emergencias informáticas (CSIRT)
- Recomendaciones y buenas prácticas en el uso de las TIC e Internet.

COMPETÈNCIES QUE ES DESENVOLUPARAN – *Competencias que se desarrollarán*

Al finalizar la acción formativa los alumnos alcanzarán las siguientes competencias:

- Conocer las diferentes amenazas que existen en Internet.
- Clasificar los distintos tipos de malware, su impacto y riesgos.
- Aprender a protegerse e informarse contra las amenazas y el malware.
- Aplicar buenas prácticas en el uso cotidiano de las TIC e Internet.

CRITERIS D'AVALUACIÓ – *Criterios de evaluación*

- Visualización y lectura de los contenidos y obtención del APTO en las actividades planteadas.