MF0488_3: GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

Certificado de Profesionalidad IFCT0109_SEGURIDAD INFORMÁTICA

Lugar de impartición: Aemta, C/ Roa de la Vega 14, ent.dcha, León
Dirigido prioritariamente a trabajadores (por cuenta ajena y autónomos) y desempleados

Acción gratuita financiada por el Servicio Público de Empleo Estatal

Objetivo: Planificar e implantar los sistemas de detección de intrusos según las normas de seguridad.
Duración: 90 horas presenciales.

Nivel del Certificado: 3

Si estás interesad@ en participar debes cumplimentar la solicitud que se adjunta y enviarla a cursos@aemta.es , junto a la siguiente documentación:

TRABAJADORES y DEMANDANTES DE EMPLEO
○ Solicitud de participación (ANEXO III) ○ Fotocopia DNI ○ Fotocopia Tarjeta de la seguridad Social ○ Fotocopia Cabecera de la última Nomina o último recibo de autónomo o tarjeta de demandante de empleo ○ CV actualizado ○ Fotocopia de titulación académica

*Debes cumplir alguno de los **requisitos de acceso** según artículo 20 del RD 189/2013, de 15 de marzo, que modifica el RD 34/2008, de 18 de enero:*

a) Graduado en ESO para el nivel 2 o título de Bachiller para nivel 3.
b) Certificado de profesionalidad del mismo nivel del módulo o módulos formativos y/o del certificado de profesionalidad al que desea acceder.
c) Certificado de profesionalidad de nivel 1 de la misma familia y área profesional para el nivel 2 o de un certificado de profesionalidad de nivel 2 de la misma familia y área profesional para el nivel 3.
d) Cumplir el requisito académico de acceso a los ciclos formativos de grado medio para el nivel 2 o de grado superior para el nivel 3, o bien haber superado las correspondientes pruebas de acceso reguladas por las administraciones educativas.
e) Tener superada la prueba de acceso a la universidad para mayores de 25 años y/o de 45 años.
f) Tener las competencias clave necesarias, de acuerdo con lo recogido en el anexo IV de este real decreto, para cursar con aprovechamiento la formación correspondiente al certificado de profesionalidad.

Contenidos

1. Sistemas de detección y prevención de intrusiones (IDS/IPS)

- Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
- Identificación y caracterización de los datos de funcionamiento del sistema
- Arquitecturas más frecuentes de los sistemas de detección de intrusos
- Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
- Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

2. Implantación y puesta en producción de sistemas IDS/IPS

- Análisis previo de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio.
- Definición de políticas de corte de intentos de intrusión en los IDS/IPS
- Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS
- Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión
- Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

3. Control de código malicioso

- Sistemas de detección y contención de código malicioso
- Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar
- Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso
- Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso
- Relación de los registros de auditoría de las herramientas de protección frente a código maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
- Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso

- Análisis de los programas maliciosos mediante desensambladores y entornos de ejecución controlada

4. Respuesta ante incidentes de seguridad

- Procedimiento de recolección de información relacionada con incidentes de seguridad
- Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad
- Proceso de verificación de la intrusión
- Naturaleza y funciones de los organismos de gestión de incidentes tipo CERT nacionales e internacionales

5. Proceso de notificación y gestión de intentos de intrusión

- Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones
- Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial
- Criterios para la determinación de las evidencias objetivas en las que se soportara la gestión del incidente
- Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones
- Guía para la clasificación y análisis inicial del intento de intrusión o infección, contemplando el impacto previsible del mismo
- Establecimiento del nivel de intervención requerido en función del impacto previsible
- Guía para la investigación y diagnóstico del incidente de intento de intrusión o infecciones
- Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección
- Proceso para la comunicación del incidente a terceros, si procede
- Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

6. Análisis forense informático

- Conceptos generales y objetivos del análisis forense
- Exposición del Principio de Lockard
- Guía para la recogida de evidencias electrónicas:
    - Evidencias volátiles y no volátiles
    - Etiquetado de evidencias
    - Cadena de custodia
    - Ficheros y directorios ocultos
    - Información oculta del sistema
    - Recuperación de ficheros borrados
- Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta del sistema y la recuperación de ficheros borrados
- Guía para la selección de las herramientas de análisis forense