

## MF0488\_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA (ONLINE)



**250,00 € - 350,00 €**

Con este curso el alumnado podrá adquirir los conocimientos necesarios que permitan planificar e implantar los sistemas de detección de intrusos según las normas de seguridad, aplicar los procedimientos de análisis de la información y contención del ataque ante una incidencia detectada y analizar el alcance de los daños y determinar los procesos de recuperación ante una incidencia detectada.

**SKU:** N/A | **Categorías** [Informática y Comunicaciones](#) |

### INFORMACIÓN

<b>Duración</b>	90 h
<b>Modalidad</b>	Online
<b>Docencia</b>	TUTOR PERSONAL

<b>Prácticas</b>	GESTIÓN DE PRÁCTICAS EN EMPRESAS
<b>Método de pago</b>	FINANCIACIÓN SIN INTERESES
<b>Centro de empleo</b>	AGENCIA DE COLOCACIÓN
<b>Formación acreditada</b>	CENTRO ACREDITADO POR EL SEPE
<b>Precio</b>	Particular, Empresa

## CONTENIDO

### MÓDULO 1. GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

#### UNIDAD DIDÁCTICA 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

#### UNIDAD DIDÁCTICA 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

#### UNIDAD DIDÁCTICA 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

#### UNIDAD DIDÁCTICA 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

#### UNIDAD DIDÁCTICA 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

#### UNIDAD DIDÁCTICA 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

