**Código:** 13341

**Unidad Formativa:**
MF0488_3 - Gestión de incidentes de seguridad informática

**Módulo:** MF0488_3 - GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

**Certificado de Profesionalidad:**
IFCT0109 - SEGURIDAD INFORMÁTICA

**Modalidad:** DISTANCIA

**Duración:** 90h.

## Metodología

El Curso está desarrollado con una metodología Online. Este sistema de enseñanza e-learning está organizado de tal forma, que el alumno pueda compatibilizar el estudio con sus ocupaciones laborales o profesionales. Esta modalidad también permite el acceso al curso a aquellas personas que viven en zonas rurales y que tienen interés en continuar formándose.
El alumno tiene que seguir un aprendizaje sistemático y un ritmo de estudio, adaptado a su disponibilidad de tiempo.

Se dispondrá de un extenso material sobre los aspectos teóricos del curso que deberá estudiar para la realización de pruebas objetivas tipo test. Para el aprobado, se exigirá un mínimo de 50% del total de las respuestas acertadas. Durante todo el transcurso de la formación, dispondrá de la atención de los tutores, así como la posibilidad de realizar consultas a través de la plataforma de teleformación para cursos online. También podrá acceder a la *Guía didáctica del alumno* dónde aparece el horario de tutorías y demás información relevante.

El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá de la modalidad elegida y de las horas de formación. La titulación será puesta a disposición del alumno en la plataforma de teleformación una vez finalizado el curso.

## Profesorado, medios y titulación

Nuestro centro de formación ha sido fundado en 1996 y en la actualidad, tiene presencia a nivel nacional disponiendo de una plantilla de más de 800 docentes entre personal laboral y freelance. Todos ellos son especialistas en diferentes familias profesionales y les acreditan los numerosos cursos que han impartido para nuestro grupo empresarial. Entre nuestro staff de formadores se encuentran ingenieros, arquitectos, economistas, informáticos, publicistas, diseñadores, médicos, enfermeros, veterinarios, fisioterapeutas, psicólogos, sociólogos, periodistas, filólogos, abogados, cocineros, licenciados en administración de empresas, licenciados en actividades físicas y deportivas, jardineros, peluqueros, educadores sociales, etc.

En todos nuestros cursos, independientemente de la metodología, se ponen a disposición del alumno los medios y materiales docentes necesarios para el desarrollo del mismo.
En los cursos en modalidad e-learning, las consultas y tutorías se pueden realizar a través de teléfono, email y la propia plataforma de teleformación.

En cuanto a la titulación, mostramos a continuación, el modelo de diploma que obtendrás a la finalización del curso:

## Requistos previos

Estar en posesión de uno de los siguientes títulos:
Título de Bachillerato.
Certificado de profesionalidad del mismo nivel.
Prueba de Acceso a Ciclo Formativo de Grado Superior.
Certificado de profesionalidad de nivel 2 de la misma familia profesional.
Prueba de Acceso a la Universidad (PAU) para mayores de 25 y/o 45 años.

## Salidas profesionales

Un certificado de profesionalidad, es un documento que acredita a un trabajador/a en una cualificación profesional del *Catálogo Nacional de las Cualificaciones Profesionales*. Son emitidos por el Servicio Público de Empleo Estatal o, en su caso, por las Comunidades Autónomas, y tienen validez en todo el territorio nacional.

Poseer un certificado de profesionalidad, supone sin lugar a dudas incrementar sustancialmente tu currículum profesional, ya que al ser un documento oficial, se valora en cualquier proceso de selección que convoquen las Administraciones Públicas, y te acredita profesionalmente ante la empresa privada.

Nosotros te formaremos para que puedas optar a conseguir el certificado de profesionalidad elegido, participando en las pruebas que convoque la Administración al amparo del R.D. 1224/2009 de 17 de julio y pudiendo además, convalidar módulos formativos para la obtención de un título de Formación Profesional.

## Objetivos

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.
Analizar el alcance de los daños y determinar los procesos de recuperación ante una incidencia de seguridad.
Estandarizar métodos de recuperación de desastres de equipos informáticos ante la detección de intrusiones.

## Contenidos

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.

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.

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.

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.

Proceso 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.

Análisis forense informático
Conceptos generales y objetivos del análisis forense.
Exposición del Principio de Lockard.
Guía para la recogida de evidencias electrónicas.
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.