Código: 13339

Unidad Formativa:
MF0486_3 - Seguridad en equipos informáticos

Módulo: MF0486_3 - SEGURIDAD EN EQUIPOS INFORMÁTICOS

Certificado de Profesionalidad:
IFCT0109 - SEGURIDAD INFORMÁTICAIFCT0510 - GESTIÓN DE SISTEMAS INFORMÁTICOS

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

Analizar los planes de implantación de la organización, para identificar los elementos del sistema implicados, y los niveles de seguridad a implementar.
Analizar e implementar los mecanismos de acceso físicos y lógicos a los servidores, según especificaciones de seguridad.
Evaluar la función y necesidad de cada servicio en ejecución en el servidor, según las especificaciones de seguridad.
Instalar, configurar y administrar un cortafuegos de servidor, con las características necesarias según especificaciones de seguridad.

Contenidos

Criterios generales comúnmente aceptados sobre seguridad de los equipos informáticos
Modelo de seguridad orientada a la gestión del riesgo, relacionado con el uso de los sistemas de información.
Relación de las amenazas más frecuentes, los riesgos que implican, y las salvaguardas más frecuentes.
Salvaguardas y tecnologías de seguridad más habituales.
La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas.

Análisis de impacto de negocio
Identificación de procesos de negocio soportados por sistemas de información.
Valoración de los requerimientos de confidencialidad, integridad, y disponibilidad de los procesos de negocio.
Determinación de los sistemas de información, que soportan los procesos de negocio y sus requerimientos de seguridad.

Gestión de riesgos
Aplicación del proceso de gestión de riesgos, y exposición de las alternativas más frecuentes.
Metodologías comúnmente aceptadas de identificación y análisis de riesgos.
Aplicación de controles, y medidas de salvaguarda para obtener una reducción del riesgo.

Plan de implantación de seguridad
Determinación del nivel de seguridad existente de los sistemas, frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio.
Selección de medidas de salvaguarda, para cubrir los requerimientos de seguridad de los sistemas de información.
Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas.

Protección de datos de carácter personal
Principios generales de protección de datos de carácter personal.
Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal.
Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización.
Elaboración del documento de seguridad, requerido por la legislación vigente en materia de protección de datos de carácter personal.

Seguridad física e industrial de los sistemas. Seguridad lógica de sistemas
Determinación de los perímetros de seguridad física.
Sistemas de control de acceso físico más frecuentes a las instalaciones de la organización, y a las áreas en las que estén ubicados los sistemas informáticos.

Criterios de seguridad para el emplazamiento físico de los sistemas informáticos.
Exposición de elementos más frecuentes, para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos.
Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos.
Elaboración de la normativa de seguridad física e industrial para la organización.
Sistemas de ficheros más frecuentemente utilizados
Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización.
Configuración de políticas y directivas del directorio de usuarios.
Establecimiento de las listas de control de acceso (ACL) a ficheros.
Gestión de altas, bajas, y modificaciones de usuarios y los privilegios que tienen asignados.
Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo.
Sistemas de autenticación de usuarios débiles, fuertes, y biométricos.
Relación de los registros de auditoría del sistema operativo, necesarios para monitorizar y supervisar el control de accesos.
Elaboración de la normativa de control de accesos a los sistemas informáticos.

Identificación de servicios
Identificación de los protocolos, servicios, y puertos utilizados por los sistemas de información.
Utilización de herramientas de análisis de puertos y servicios abiertos, para determinar aquellos que no son necesarios.
Utilización de herramientas de análisis de tráfico de comunicaciones, para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos.

Robustecimiento de sistemas
Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información.
Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios.
Eliminación y cierre de las herramientas, utilidades, servicios, y puertos prescindibles.
Configuración de los sistemas de información, para que utilicen protocolos seguros siempre que sea posible.
Actualización de parches de seguridad de los sistemas informáticos.
Protección de los sistemas de información frente a código malicioso.
Gestión segura de comunicaciones, carpetas compartidas, impresoras, y otros recursos compartidos del sistema.
Monitorización de la seguridad y el uso adecuado de los sistemas de información.

Implantación y configuración de cortafuegos
Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad.
Criterios de seguridad para la segregación de redes en el cortafuegos mediante zonas desmilitarizadas / DMZ.
Utilización de redes privadas virtuales / VPN, para establecer canales seguros de

comunicaciones.
Definición de reglas de corte en los cortafuegos.
Relación de los registros de auditoría de los cortafuegos, necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad.
Establecimiento de la monitorización y pruebas del cortafuegos.