



## IFCT102 Ciberseguridad en el trabajo

## IFCT102 Ciberseguridad en el trabajo

**Duración:** 60 horas

**Precio:** consultar euros.

**Modalidad:** e-learning

### Metodología:

El Curso será desarrollado con una metodología a Distancia/on line. El sistema de enseñanza a distancia está organizado de tal forma que el alumno pueda compatibilizar el estudio con sus ocupaciones laborales o profesionales, también se realiza en esta modalidad para permitir el acceso al curso a aquellos alumnos que viven en zonas rurales lejos de los lugares habituales donde suelen realizarse los cursos y que tienen interés en continuar formándose. En este sistema de enseñanza el alumno tiene que seguir un aprendizaje sistemático y un ritmo de estudio, adaptado a sus circunstancias personales de tiempo

El alumno 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 75% del total de las respuestas acertadas.

El Alumno tendrá siempre que quiera a su disposición la atención de los profesionales tutores del curso. Así como consultas telefónicas y a través de la plataforma de teleformación si el curso es on line. Entre el material entregado en este curso se adjunta un documento llamado Guía del Alumno dónde aparece un horario de tutorías telefónicas y una dirección de e-mail dónde podrá enviar sus consultas, dudas y ejercicios El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá del tipo de curso elegido y de las horas del mismo.

## Profesorado:

Nuestro Centro fundado en 1996 dispone de 1000 m2 dedicados a formación y de 7 campus virtuales.

Tenemos una extensa plantilla de profesores especializados en las diferentes áreas formativas con amplia experiencia docentes: Médicos, Diplomados/as en enfermería, Licenciados/as en psicología, Licenciados/as en odontología, Licenciados/as en Veterinaria, Especialistas en Administración de empresas, Economistas, Ingenieros en informática, Educadores/as sociales etc...

El alumno podrá contactar con los profesores y formular todo tipo de dudas y consultas de las siguientes formas:

- Por el aula virtual, si su curso es on line
- Por e-mail
- Por teléfono

## Medios y materiales docentes

-Temario desarrollado.

-Pruebas objetivas de autoevaluación y evaluación.

-Consultas y Tutorías personalizadas a través de teléfono, correo, fax, Internet y de la Plataforma propia de Teleformación de la que dispone el Centro.



## Titulación:

Una vez finalizado el curso, el alumno recibirá por correo o mensajería la titulación que acredita el haber superado con éxito todas las pruebas de conocimientos propuestas en el mismo.

## Programa del curso:

Objetivo principal: Desarrollar competencias en ciberseguridad para identificar, prevenir y responder a amenazas digitales en el entorno laboral, garantizando la protección de la información y el cumplimiento de buenas prácticas de seguridad informática. ? Objetivos específicos Comprender los principales riesgos y amenazas cibernéticas en el ámbito laboral, como malware, phishing y ataques de ingeniería social. Aplicar buenas prácticas de seguridad informática para la protección de datos personales y corporativos en el uso diario de dispositivos y redes. Identificar métodos seguros de autenticación y control de acceso para prevenir accesos no autorizados a sistemas y documentos sensibles. Utilizar herramientas y protocolos de ciberseguridad para la gestión segura de contraseñas, correos electrónicos y navegación en internet. Reconocer la importancia de la formación continua en ciberseguridad y la responsabilidad individual en la protección de la información dentro del entorno laboral. El curso incluye material educativo adicional para reforzar el aprendizaje, entre los que se encuentran: ? 24 vídeos explicativos ? 13 guías descargables ? 8 supuestos prácticos ? 7 Recursos extra ? Glosario de términos y bibliografía especializada Este contenido complementario permitirá a los participantes profundizar en cada tema y aplicar los conocimientos adquiridos en situaciones reales.

ÍNDICE 32120 IFCT102 CIBERSEGURIDAD EN EL TRABAJO TEMA 1 DEFINICIÓN DE LOS MÉTODOS DE ACCESO REMOTO 1.1. Concepto, beneficios y riesgos del acceso remoto 1.2. Métodos de acceso remoto en el trabajo TEMA 2 CONTEXTUALIZACIÓN DEL TELETRABAJO 2.1. Concepto y ventajas del teletrabajo 2.2. Herramientas tecnológicas para el teletrabajo TEMA 3 IDENTIFICACIÓN DE LAS PRINCIPALES AMENAZAS PARA LOS TERMINALES DE TELETRABAJO 3.1. Introducción a las amenazas en el teletrabajo 3.2. Malware y software malicioso 3.3. Ataques de ingeniería social y phishing 3.4. Vulnerabilidades en redes y conexiones remotas 3.5. Amenazas en dispositivos personales y corporativos 3.6. Ataques a aplicaciones y servicios en la nube TEMA 4 IDENTIFICACIÓN DE LAS PRINCIPALES MEDIDAS PARA PREVENIR AMENAZAS. RECOPIACIÓN DE EVIDENCIAS 4.1. Seguridad en el acceso en remoto 4.2. Seguridad en los equipos de trabajo 4.3. Seguridad en dispositivos móviles 4.4. Técnicas y recursos para el análisis de los datos TEMA 5 PROTECCIÓN DE DATOS EN LOS TERMINALES DE TELETRABAJO 5.1. Protección de datos en el teletrabajo y su normativa 5.2. Seguridad en el almacenamiento y transmisión de datos 5.3. Control de accesos y autenticación segura Cifrado de datos en discos duros, USBs y dispositivos móviles. 5.4. Prevención de fugas de información (Data Loss Prevention, DLP) TEMA 6 UTILIZACIÓN DE COPIAS DE SEGURIDAD EN DISPOSITIVOS DE TELETRABAJO 6.1 Copias de seguridad y su clasificación 6.2. Métodos y soportes de almacenamiento de copias de seguridad 6.3. Políticas y estrategias de copias de seguridad en teletrabajo 6.4. Seguridad en las copias de seguridad ANEXO ? Glosario de términos ? Bibliografía ? Supuestos prácticos

