# TÉCNICS Y HERRAMIENTAS DE PROTECCIÓN DE REDES, SISTEMAS Y SERVICIOS

# TÉCNICS Y HERRAMIENTAS DE PROTECCIÓN DE REDES, SISTEMAS Y SERVICIOS

**Duración:** 60 horas

**Precio:** consultar euros.

**Modalidad:** e-learning

## Objetivos:

Descripción: Planificar el despliegue de varias máquinas en una red para proporcionar una serie de servicios dados. Conocer los principales tipos de técnicas para la protección de la información en las redes y sistemas telemáticos. Fundamentación: La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

## 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, Licencidos/as en odontología, Licenciados/as en Veterinaria, Especialistas en Administración de empresas, Economistas, Ingenieros en informática, Educadodores/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:

TEMA 1. PROTECCIÓN EN NIVEL DE RED

1. ARQUITECTURA DE RED
2. SEGURIDAD DE RED
3. SEGURIDAD DE CAPA DE APLICACIÓN Y DE TRANSPORTE
4. SEGURIDAD DE CAPA DE RED Y VPNS
5. CONSIDERACIONES DE DISEÑO DE SEGURIDAD DE RED
6. RIESGOS DE DOMINIO CRUZADO Y SOLUCIONES
7. VALIDACIÓN DE DISEÑO

TEMA 2. REDES

1. SISTEMAS DE CONTROL DE ACCESO Y RAZONES
2. CONTROLES
3. ATAQUES DE CONTROL DE ACCESO
4. COMO TRABAJA EN CONTROL DE ACCESO Y LAS TABLAS DE ESTADO
5. REGLAS DE ACCESO DE INTERFAZ
6. ACL GLOBAL
7. ASEGURAR CONMUTADORES
8. DESCRIPCIÓN DEL PROXY BASADO EN USUARIO (CUT-THROUGH)
9. AAA
10. COMPRENDER COMO FUNCIONA NAT

TEMA 3. PROTECCIÓN DE SISTEMAS

1. EVALUAR Y MITIGAR VULNERABILIDADES DE SEGURIDAD
2. HARDWARE
3. PROCESADOR
4. MEMORIA
5. ALMACENAMIENTO
6. DISPOSITIVOS DE ENTRADA Y SALIDA
7. FIRMWARE

TEMA 4. SERVIDORES

1. APLICANDO CONCEPTOS DE OPERACIONES DE SEGURIDAD
2. APROVISIONAMIENTO Y ADMINISTRACIÓN DE RECURSOS
3. ADMINISTRACIÓN DE LA CONFIGURACIÓN
4. ADMINISTRACIÓN DE CAMBIO
5. ADMINISTRACIÓN DE PARCHES Y REDUCCIÓN DE VULNERABILIDADES