Cursos de postgrado

20 créditos

Curso académico 2018-2019

Plataforma docente

Ciberseguridad

del 14 de enero al 18 de noviembre de 2019

DIPLOMA DE EXPERTO UNIVERSITARIO

Características: material impreso, material multimedia, página web, curso virtual y guía didáctica.

Departamento

Sistemas de Comunicación y Control

E.t.s. de Ingeniería Informática

PROGRAMA DE POSTGRADO
Máster, Diploma de Especialización, Diploma de Experto y Certificado de Formación del Profesorado.
Curso 2018/2019

El Programa de Postgrado acoge los cursos que dan derecho a la obtención de un Título Propio otorgado por la UNED. Cada curso se impartirá en uno de los siguientes niveles: Máster, Diploma de Especialización, Diploma de Experto y Certificado de Formación del Profesorado.

Requisitos de acceso:

Estar en posesión de un título de grado, licenciado, diplomado, ingeniero técnico o arquitecto técnico. El director del curso podrá proponer que se establezcan requisitos adicionales de formación previa específica en algunas disciplinas.

Asimismo, de forma excepcional y previo informe favorable del director del curso, el Rectorado podrá eximir del requisito previo de la titulación en los cursos conducentes al Diploma de Experto Universitario. Los estudiantes deberán presentar un curriculum vitae de experiencias profesionales que avalen su capacidad para poder seguir el curso con aprovechamiento y disponer de acceso a la universidad según la normativa vigente.

El estudiante que desee matricularse en algún curso del Programa de Postgrado sin reunir los requisitos de acceso podrá hacerlo aunque, en el supuesto de superarlo, no tendrá derecho al Título propio, sino a un Certificado de aprovechamiento.

Destinatarios

El curso está dirigido a profesionales dispuestos a potenciar su carrera profesional formándose en una disciplina de gran futuro y demanda laboral. La ciberseguridad es un área de gran actualidad y que se aplica en muchos dominios, por lo que el objetivo es formar a los profesionales TIC en los principios de seguridad de la información y sus aplicaciones en diferentes infraestructuras.

Es necesario la titulación de grado o equivalente para la obtención del diploma de experto y se recomienda alguna base teórica en Seguridad básica aunque no es estrictamente necesario. Las titulaciones (grado o equivalente) consideradas en la lista siguiente son las recomendables para el seguimiento del curso

- Ingeniería Informática
- Ingeniería Industrial/Telecomunicaciones
- Físicas / Matemáticas
- Otras titulaciones/grados en ingeniería o afines

1. Presentación y objetivos

El curso tiene como objetivo profundizar y ampliar la formación en relación al ámbito de la seguridad informática desde la perspectiva de la gestión,enfatizando la necesidad de estandarización y cumplimiento de normativas. Por un lado se presentarán distintas políticas, normativas y estándares de seguridad existentes, analizando especialmente el ISO 27001. Por otro lado, se prestará especial atención al análisis de riesgos y al uso de herramientas profesionales para el desarrollo de los estándares y su aplicación a casos concretos.

Otra Información

Será responsabilidad exclusiva del Equipo Docente la información facilitada en la siguiente relación de hipervínculos. En caso de detectarse alguna contradicción, prevalecerá la oferta formativa aprobada por el Consejo de Gobierno para cada convocatoria, así como del Reglamento de Formación Permanente y del resto de la legislación Universitaria vigente.

Más Información

2. Contenidos

Módulo 1: Principios de Seguridad para SGSI

1. Seguridad de la Información

1.1. Introducción a la seguridad de la información

1.2. Ciclo de vida de un SGSI

1.3. Aspectos legales y reguladores

1.4. Gestión de la seguridad

1.5. Estandarización y certificación

2. Criptografía y su aplicación en la seguridad

2.1. Introducción a la criptografía

2.2. Criptografía moderna

2.3. Criptoanálisis

2.3. Esteganografía

2.4. Aplicaciones: redes anónimas, criptomonedas y contratos inteligentes (smart contracts)

3. "Hardening" de sistemas y redes

3.1. Introducción a la seguridad de sistemas operativos y redes

3.2. Protección básica: arranque y sistemas de ficheros.

3.3. Seguridad en sistemas operativos: Microsoft y GNU/Linux

3.4. Redes internas: intranet y redes de área local

3.5. Protección de Aplicaciones y Servicios

3.6. Red perimetral

3.7. "Hardening" de dispositivos de red (routers y switches)

Módulo 2: Operación de los SGSI

1. Recopilación de Información

1.1. Fuentes de información y modelos: Microsoft Thread Modelling, Stride & Dread, OSSTMM

1.2. Footprinting

1.3. Fingerprinting

1.4. Metadatos y logs

2. Explotación de Aplicaciones y sistemas

2.1. Análisis de la información recopilada

2.2. Posibles vulnerabilidades/amenazas y su explotación

2.3. Pentesting

2.5. Post-explotación: técnicas y ejemplos

3. Monitorización de Redes de Datos

3.1. Monitorización y análisis de tráfico

3.2. Capa física y lógica

3.3. Capa de red: IPv4 e IPv6

3.4. Capa de red: ICMP e Ipsec

3.5. Capa de aplicación

3.5. TAPs y SIEMs

Módulo 3: Continuidad del Negocio

1. Respuesta ante incidentes

1.1. Incidentes y su gestión

1.2. Plan de respuesta ante incidentes

1.3. Plan de continuidad del negocio

1.4. Ejemplos y casos prácticos

2. Análisis forense

2.1. Introducción y tipos

2.2. Recopilación de evidencias

2.3. Análisis de imágenes

2.4. Análisis forense en sistemas

2.5. Análisis forense en redes

2.6. Análisis forense en dispositivos móviles

2.7. Análisis forense de malware

2.8. Informe pericial

3. Auditoria de sistemas y redes

3.1. Introducción a la auditoria

3.2. Tipos de auditorías: caja negra,caja blanca y caja gris

3.3. Hacking Etico:RFD/RFI/RFQ/RFT

3.4. Auditoria de sistemas y redes

3.5. Metodologías y estándares

Módulo 4: Ámbitos de aplicación de la ciberseguridad

1. Ámbitos de dominio generalista

1.1 Introducción al ciberterrorismo y espionaje

1.2 Ciberdelincuencia

1.3 E-commerce

1.4 E-Health

1.5 Transacciones y finanzas electrónicas

2. Ámbitos específicos en la seguridad de redes

2.1. Seguridad portatil

2.2. Redes P2P

2.3. Redes WiFi

3. Ámbitos especificos de la identidad personal y la publicación digital

3.1. Phising, robos de identidad y privacidad

3.2. Redes sociales

3.3. Email y Spam

3.4. Spyware

3. Metodología y actividades

La metodología que se empleará es la propia de la educación a distancia, con la tutorización directa de los profesores del curso. Los estudiantes tendrán a su disposición un servicio de consultas mediante correo electrónico, foros temáticos y visita personal con los profesores del curso.

Para superar el curso el estudiante deberá superar una serie de ejercicios prácticos donde aplicará los conocimientos adquiridos a lo largo de las distintas partes del curso.

Durante el curso se realizarán una o dos sesiones presenciales o virtuales. En todo caso, las sesiones presenciales si hubiera se realizarán en la Sede Central de la UNED en Madrid y no serán obligatorias.

Este curso se complementa a través del uso de una comunidad virtual creada en los servidores de la UNED.

4. Material didáctico para el seguimiento del curso

4.1 Material obligatorio

4.1.1 Material en Plataforma Virtual

Tanto la Guía Didáctica del curso, orientaciones sobre el uso de la plataforma así como el material que el equipo docente consideré necesario durante el curso estará disponible en la plataforma que aloja el curso.

Este material se compone de ficheros en formato electrónico, videotutoriales que dan soporte a los contenidos disponibles en los ficheros en formato electrónico, así como enlaces de acceso a las herramientas recomendadas o material adicional.

4.1.2 Material enviado por el equipo docente (apuntes, pruebas de evaluación, memorias externas, DVDs, ...)

El equipo docente puede considerar necesario enviar a los estudiantes algún material adicional. Se informará a los estudiantes con suficiente antelación.

Este material será abonado por el alumno junto a la matrícula del curso.

4.2 Material optativo, de consulta y bibliografía

4.2.1 Otros Materiales

En elaboración

5. Atención al estudiante

La comunicación se realizará preferentemente a través del curso virtual

El equipo docente del curso está formado por los siguientes profesores:

Roberto Hernández, roberto@scc.uned.es

Llanos Tobarra, llanos@scc.uned.es

Rafael Pastor, rpastor@scc.uned.es

También es posible realizar visita personal a los profesores del curso previa cita en la 5ª planta de la Escuela Técnica Superior de Ingeniería Informática de la UNED, calle Juan del Rosal nº 16 de Madrid.

El estudiante del curso tendrá acceso a una comunidad virtual de tutorización, con foros temáticos donde se plantearán y resolverán las dificultades que vayan surgiendo.

6. Criterios de evaluación y calificación

Los requisitos mínimos para superar el curso consisten en la evaluación positiva de los ejercicios de carácter práctico que se propongan en la plataforma virtual y donde se aplicarán los conocimientos adquiridos en las distintas partes que componen el curso. El criterio de evaluación que se considerará será el nivel de cumplimiento de los requisitos pedidos en los enunciados de los ejercicios prácticos, así como la originalidad y complejidad de las soluciones aportadas.

7. Duración y dedicación

La duración del curso es del 14 de Enero 2019 hasta 18 de Noviembre 2019

Este curso tiene reconocidos 20 ECTS (European Credit Transfer System) que representan 500 horas de dedicación.

8. Equipo docente

Codirectores

Codirector - UNED

HERNANDEZ BERLINCHES, ROBERTO

Codirector - UNED

PASTOR VARGAS, RAFAEL

Colaboradores UNED

Colaborador - UNED

HERNANDEZ BERLINCHES, ROBERTO

Colaborador - UNED

TOBARRA ABAD, MARIA DE LOS LLANOS

9. Precio del curso

Precio de matrícula: 1.000,00 €.

Precio del material: 300,00 €.

10. Descuentos

10.1 Ayudas al estudio y descuentos

Se puede encontrar información general sobre ayudas al estudio y descuentos en este enlace.

Debe hacer la solicitud de matrícula marcando la opción correspondiente, y posteriormente enviar la documentación al correo: descuentos@fundacion.uned.es.

11. Matriculación

Del 7 de septiembre al 15 de diciembre de 2018.

12. Responsable administrativo

Negociado de Especialización.