

**40850 - ANÁLISIS DE LA SEGURIDAD EN
LOS SISTEMAS DE INFORMACIÓN**

CENTRO: 180 - Escuela de Ingeniería Informática

TITULACIÓN: 4008 - Grado en Ingeniería Informática

ASIGNATURA: 40850 - ANÁLISIS DE LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Vinculado a : (Titulación - Asignatura - Especialidad)

4008-Grado en Ingeniería Informática - 40850-ANÁLISIS DE LA SEGURIDAD EN LOS SISTEMA - 03

4801-Doble Grado en Ingeniería Informática y - 48144-ANÁLISIS DE LA SEGURIDAD DE LOS SISTEMA - 00

CÓDIGO UNESCO: 1203

TIPO: Obligatoria

CURSO: 3

SEMESTRE: 2º semestre

CRÉDITOS ECTS: 6

Especificar créditos de cada lengua:

ESPAÑOL: 6

INGLÉS: 0

SUMMARY

REQUISITOS PREVIOS

Haber alcanzado los resultados del aprendizaje en Redes de Computadores

Datos identificativos del profesorado que la imparte.

Plan de Enseñanza (Plan de trabajo del profesorado)

Contribución de la asignatura al perfil profesional:

Las Tecnologías de la Información, entendidas como la integración de las tecnologías informática y de Comunicaciones, son un factor esencial para el desarrollo económico y el bienestar social.

Garantizar la seguridad, y muy especialmente, los requisitos que permiten estimar de forma cuantitativa la disponibilidad de las redes de comunicación y sistemas de información es un asunto que preocupa cada vez mas a la sociedad en su conjunto, de forma que se está desarrollando en normativas de obligado cumplimiento como es el Esquema Nacional de Seguridad en nuestro país.

El perfil profesional de la asignatura permite obtener conocimientos que se pueden desarrollar en los ámbitos profesionales de:

- Responsable de red informática o responsable de seguridad informática.
- Profesionales, administradores y responsables de Tecnologías de la Información en ámbitos empresariales, striales, académicos y el sector público.

Competencias que tiene asignadas:

GENERALES:

G1. Poseer y comprender conocimientos en un área de estudio (Ingeniería Informática) que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya

en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.

G2. Aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.

G3. Reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

G4. Transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.

G5. Desarrollar aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.

ULPGC:

N1. Comunicarse de forma adecuada y respetuosa con diferentes audiencias (clientes, colaboradores, promotores, agentes sociales, etc.), utilizando los soportes y vías de comunicación más apropiados (especialmente las nuevas tecnologías de la información y la comunicación) de modo que pueda llegar a comprender los intereses, necesidades y preocupaciones de las personas y organizaciones, así como expresar claramente el sentido de la misión que tiene encomendada y la forma en que puede contribuir, con sus competencias y conocimientos profesionales, a la satisfacción de esos intereses, necesidades y preocupaciones.

N2. Cooperar con otras personas y organizaciones en la realización eficaz de funciones y tareas propias de su perfil profesional, desarrollando una actitud reflexiva sobre sus propias competencias y conocimientos profesionales y una actitud comprensiva y empática hacia las competencias y conocimientos de otros profesionales.

N3. Contribuir a la mejora continua de su profesión así como de las organizaciones en las que desarrolla sus prácticas a través de la participación activa en procesos de investigación, desarrollo e innovación.

N4. Comprometerse activamente en el desarrollo de prácticas profesionales respetuosas con los derechos humanos así como con las normas éticas propias de su ámbito profesional para generar confianza en los beneficiarios de su profesión y obtener la legitimidad y la autoridad que la sociedad le reconoce.

N5. Participar activamente en la integración multicultural que favorezca el pleno desarrollo humano, la convivencia y la justicia social.

ESPECÍFICAS:

SI02: Capacidad para determinar los requisitos de los sistemas de información y comunicación de una organización atendiendo a aspectos de seguridad y cumplimiento de la normativa y la legislación vigente.

Objetivos:

- Describir los principios básicos de la seguridad informática.
- Describir la autenticación.
- Aplicar técnicas para mantener la integridad del sistema.
- Mantener la confidencialidad del sistema.
- Explicar nociones de cifrado.
- Detallar los fundamentos de la seguridad basados en la teoría de la información y la teoría de la complejidad.
- Detallar métodos y técnicas de cifrado.
- Gestionar la seguridad de un sistema informático.
- Realizar una auditoría técnica y de certificación
- Usar las herramientas forenses.
- Plantear y realizar un plan estratégico de seguridad.

Contenidos:

1 CONCEPTOS BÁSICOS EN SEGURIDAD INFORMÁTICA

(Horas Presenciales=20, Horas No Presenciales=30)

Competencias: G1, G2, G3, G4, G5, N1, N2, N3, N4, N5, SI02

Fundamentos de criptografía y criptoanálisis

Sistemas criptográficos horizontales y verticales

Amenazas en entorno local y extendido

Mecanismos de seguridad informática

Bibliografía Básica: Ocón y Rosa, Lucena

2 INSTRUMENTOS PARA LA GESTIÓN DE LA SEGURIDAD

(Horas Presenciales=20, Horas No Presenciales=30)

Competencias: G1, G2, G3, G4, G5, N1, N2, N3, N4, N5, SI02

Análisis de Riesgos

Auditoría Informática

Peritaje Informático

Respuesta ante incidentes

Conceptos de Análisis forense

Plan Estratégico de Seguridad

Bibliografía Básica: Ocón y Rosa, Fernández, Garrido

3 NORMATIVA EN SEGURIDAD INFORMÁTICA

(Horas Presenciales=20, Horas No Presenciales=30)

Competencias: G1, G2, G3, G4, G5, N1, N2, N3, N4, N5, SI02

Buenas prácticas. La biblioteca ITIL

Sistemas de Gestión de Seguridad Informática. Normas ISO 27000

Esquema Nacional de Seguridad. ENS.

Requisitos mínimos para una política de seguridad

Bibliografía: Ocón y Rosa, Varios (Normativa, Internet)

Metodología:

En las clases se impartirán los contenidos ya expuestos anteriormente utilizando una metodología que potencia la participación del grupo y 'aprender haciendo' y así conseguir la participación e implicación de los estudiantes en la asignatura. De esta manera se configura un marco de trabajo donde:

- Los estudiantes adquieren un protagonismo activo y una autonomía en su aprendizaje.
- El profesor realiza una actividad de dirección, marca las líneas de trabajo, supervisa la labor del estudiante y la valora.

Se llevarán a cabo:

- Sesiones académicas teóricas: En las clases teóricas se explicarán los principios y fundamentos de los tópicos especificados en el temario. La teoría se impartirá mediante explicaciones basadas en bibliografía de referencia de la asignatura. El estudiante dispondrá de libros virtuales y diverso material digital en cada unidad temática para que conozca los puntos más importantes de ella.
- Sesiones académicas prácticas: Se propondrán actividades a realizar en el aula y fuera de ella, con el fin de que los estudiantes consoliden o profundicen los contenidos vistos en las sesiones académicas teóricas. Los trabajos prácticos son obligatorios y necesarios para adquirir las competencias. Se promoverán aspectos colaterales de formación, como la capacidad expresiva (oral y escrita) y la calidad de desarrollo, implementación y despliegue de componentes de un sistema de información. Se suministran enunciados, información, y metodología para realizar las prácticas.
- Trabajo de curso dirigido: Se proponen trabajos donde los estudiantes en grupos de dos, o individualmente, elaboran trabajos sobre la asignatura. Esta actividad se realiza con Exposiciones de trabajos, en clase o en tutorías donde se analizan y discuten. Los profesores suministran el asesoramiento, enunciados, guía, y metodología para realizar los trabajos y para su exposición en clase.
- Trabajo Autónomo: trabajo donde el estudiante analiza, reflexiona, comprende y memoriza los conocimientos de la materia.
- Apoyo a la enseñanza presencial mediante las TIC: Se usarán ampliamente tecnologías avanzadas (web, correo electrónico, Moodle) como instrumento de comunicación estudiante/profesor y como repositorio de material (p.ej. los libros, formularios, y presentaciones disponibles en formato electrónico). Estas herramientas permiten romper el espacio, el estudiante puede trabajar en cualquier lugar que tenga un ordenador conectado a internet, y rompe el tiempo en el sentido que el estudiante tiene a su disposición el curso las veinticuatro horas del día. Todo ello favorece el proceso de enseñanza-aprendizaje dotándolo de mayor flexibilidad, facilidad de acceso a la información y el trabajo cooperativo.

Criterios y fuentes para la evaluación:

- Sesiones académicas teóricas con debates y participación
- Sesiones académicas prácticas.
- Trabajos colaborativos en grupo e individuales dirigidos.
- Exposición y defensa oral de trabajos en el ámbito de la clase.
- Lecturas obligatorias.
- Búsqueda, análisis, síntesis y generación de la información.
- Ejercicios de autoevaluación.
- Exámenes de control y aprendizaje
- Tutorías colectivas e individuales.
- Uso de las tecnologías de la información.
- Foros, debates y discusiones en el ámbito de la clase
- Actividades para conexión de la clase como grupo, conocer a los individuos y servicios al colectivo.
- Uso del portafolio.

Sistemas de evaluación:

1. Asistencia y participación activa(10% de la nota final)
 - Asistencia a las clases teóricas y prácticas
 - Evaluación del trabajo cooperativo en grupo
 - Participación en los foros y debates.
2. Evaluación de los trabajos prácticos y tareas personales realizadas.(45% de la nota final)
 - Evaluación de la calidad de los trabajos prácticos, según criterios específicos de cada tarea
 - . Evaluación de la defensa y exposición de los trabajos.
 - . Evaluación de la expresión escrita, y oral de los trabajos y defensa de los mismos.
 - . Evaluación de las búsquedas, síntesis y generación de información.
3. Exámen teórico (45% de la nota final)

Criterios de calificación:

Se exigirá, bajo el sistema de evaluación anteriormente apuntado:

- Un prueba escrita.
- Prácticas de la asignatura.

Para superar la asignatura se han de aprobar obligatoriamente tanto la prueba como las prácticas.

La nota final, en cualquier convocatoria, será: 10% asistencia y participación + 45% evaluación de los trabajos prácticos y tareas personales realizadas + 45 % del Examen teórico

En el caso de suspender cualquiera de las partes, en el acta figurará la nota obtenida de la parte suspendida.

Plan de Aprendizaje (Plan de trabajo de cada estudiante)

Tareas y actividades que realizará según distintos contextos profesionales (científico, profesional, institucional, social)

A lo largo del curso, por cada tema, se realizarán actividades relacionadas con los contenidos de la asignatura, que evidencien el aprendizaje realizado.

Las actividades serán:

- de reflexión personal: mapas de conceptos y realización de portafolios, creación de informes.
Contextos: Profesional, Social, Científico, Institucional
- de trabajo en grupo: debates del grupo en clase y a través del Campus Virtual ULPGC.
Contextos: Profesional, Social, Científico, Institucional
- de aplicación: análisis, diseño, realización, configuración y evaluación de programas, utilidades y aplicaciones informáticas. Trabajo sobre casos prácticos basados en escenarios de situación, reales o simulados. Contextos: Profesional, Social, Científico, Institucional

Temporalización semanal de tareas y actividades (distribución de tiempos en distintas actividades y en presencialidad - no presencialidad)

El proyecto docente presentado se corresponde a una asignatura de 6 créditos, descompuestos en 3 créditos de clases de teoría, 1.5 créditos dedicados a prácticas en Aula y 1,5 créditos a las prácticas de laboratorio.

La distribución en horas presenciales (HP) y no presenciales (HNP) es de 60 y 90,

respectivamente.

Distribución de HP (60):

Horas Clases Teóricas (HCT): 30

Horas Practicas en Aula (HPA): 15

Horas Prácticas de Laboratorio (HPL):15

Distribución HNP (90):

Horas de trabajos tutorizados (HTT): 30

Horas de actividad autónoma(HAA), con uso de plataformas virtuales y sin uso de ellas: 60

Distribución de tiempos relacionados con los contenidos de la asignatura (HCT, HPA, HPL, HTT, HAA) :

Tema 1 (10, 5, 5, 10, 20)

Tema 2 (10, 5, 5, 10, 20)

Tema 3 (10, 5, 5, 10, 20)

Recursos que tendrá que utilizar adecuadamente en cada uno de los contextos profesionales.

Los alumnos utilizarán los medios y recursos que la EII pone a su disposición para la docencia, tanto en las clases teóricas como de prácticas en aula o en laboratorios.

Utilizarán las herramientas dispuestas por la Universidad en el Campus Virtual de la ULPGC.

Deberán conocer y utilizar paquetes ofimáticos para la redacción y presentación de las memorias de las prácticas y trabajos de curso.

Resultados de aprendizaje que tendrá que alcanzar al finalizar las distintas tareas.

El alumnos debe ser capaz de :

- Describir los principios básicos de la seguridad informática.
- Describir la autenticación.
- Aplicar técnicas para mantener la integridad del sistema.
- Mantener la confidencialidad del sistema.
- Explicar nociones de cifrado.
- Detallar los fundamentos de la seguridad basados en la teoría de la información y la teoría de la complejidad.
- Detallar métodos y técnicas de cifrado.
- Gestionar la seguridad de un sistema informático.
- Realizar una auditoría técnica y de certificación
- Usar las herramientas forenses.
- Plantear y realizar un plan estratégico de seguridad.

Plan Tutorial

Atención presencial individualizada (incluir las acciones dirigidas a estudiantes en 5ª, 6ª y 7ª convocatoria)

En el horario establecido por el departamento, asignado a cada profesor.

Atención presencial a grupos de trabajo

En el horario establecido por el departamento, asignado a cada profesor.

Atención telefónica

En el horario establecido por el departamento, asignado a cada profesor.

Atención virtual (on-line)

Los profesores de la asignatura atenderán a los alumnos a través del Campus Virtual ULPGC.

Bibliografía

[1 Básico] Apuntes de emergencias tecnológicas [

Antonio Ocón Carreras, Carlos Rosa Remedios.

Universidad de Las Palmas de Gran Canaria, Vicerrectorado de Ordenación Académica y EEES, Estructura de Teleformación

ULPGC,, Las Palmas de Gran Canaria : (2011)

[2 Básico] Peritajes informáticos /

Emilio Del Peso Navarro (director) ; autores: Carlos Manuel Fernández Sánchez ... [et al.].

Díaz de Santos,, Madrid : (2001) - (2ª ed.)

84-7978-497-0

[3 Básico] Análisis forense digital en entornos windows /

Juan Garrido Caballero ; [con la colaboración de] Juan Luis G. Rambla, Chema Alonso ; prólogo de Pedro Sánchez.

Informática64,, Móstoles (Madrid) : (2009)

978-84-613-3432-2

[4 Básico] Criptografía y seguridad en computadores: versión 4-0.7.51 /

Manuel Lucena López.

El autor,, [s.l.] : (2008) - (4ª ed.)

[5 Recomendado] File system forensic analysis /

Brian Carrier.

Addison-Wesley,, Boston [etc.] : (2005)

0321268172

[6 Recomendado] Incident response and computer forensics /

Chris Prosise, Kevin Mandia.

McGraw-Hill-Osborne,, New York [etc] : (2003) - (2nd ed.)

0-07-222696-X

[7 Recomendado] The codebreakers :the story of secret writing /

David Kahn.

Scribner,, New York : (1996) - (ed. rev. and updated.)

0684831309

[8 Recomendado] Seguridad de sistemas en red /

José Antonio Muñoz Blanco, Víctor Manuel Henríquez Henríquez.

Universidad de Las Palmas de Gran Canaria, Servicio de Publicaciones,, Las Palmas de Gran Canaria : (2007)

97884969710305

[9 Recomendado] Recursos y Sitios de Internet relativos Seguridad Informática

varios autores

- (varios)

no procede