ASIGNATURA DE GRADO:

SEGURIDAD

Curso 2012/2013

(Código:71013124)

1.PRESENTACIÓN DE LA ASIGNATURA

Esta guía presenta las orientaciones básicas que requiere el alumno para el estudio de la asignatura de Seguridad. Por esta razón es muy recomendable leer con atención esta guía antes de iniciar el estudio, para adquirir una idea general de la asignatura y de los trabajos, actividades y prácticas que se van a desarrollar a lo largo del curso.

Seguridad es una asignatura de seis créditos ECTS de carácter obligatorio que se imparte en el segundo semestre del tercer curso de la carrera en la titulación de Grado en Ingeniería Informática dentro de la materia de Redes y Conexión de Dispositivos. Esta asignatura inicia el contacto del alumno con el mundo real de la seguridad informática de sistemas, datos y comunicaciones.

El objetivo esencial de la asignatura es adquirir los conocimientos asociados a todos los aspectos del problema de la seguridad informática, orientándolos a la consecución de la creación de una política de seguridad de una organización. En ese sentido, se analizan los problemas de seguridad física y lógica asociados con los componentes hardware (cableado, repetidores, encaminadores, etc.) así como software (sistemas operativos, aplicaciones y protocolos). Se estudian los distintos tipos de ataques a la seguridad, haciendo una taxonomía lo más exhaustiva posible, así como los distintos tipos de defensas posibles. Se estudian las distintas herramientas de defensa habituales como cortafuegos, analizadores de vulnerabilidades, sistemas de detección de intrusiones y otros.

2.CONTEXTUALIZACIÓN EN EL PLAN DE ESTUDIOS

La asignatura de Seguridad, como ya se mencionó en la introducción, se encuentra englobada dentro de la materia de Redes y Conexión de Dispositivos segundo semestre del tercer curso de la carrera en la titulación de Grado en Ingeniería Informática.

Dentro de esta misma materia, nos encontramos con las siguientes asignaturas:

- *Redes de Computadores*, asignatura de segundo curso de grado de carácter obligatorio.
- *Sistemas distribuidos*, asignatura de tercer curso de grado de carácter obligatorio.
- *Periféricos e Interfaces*, asignatura de cuatro curso de grado de carácter opcional.

Una posible extensión de esta asignatura la encontramos en 4º curso con la asignatura optativa de "*Teoría de la Información y criptografía básica*" que amplia los contenidos de la asignatura profundizando en los métodos criptográficos.

En relación con las competencias de la materia, la asignatura Bases de Datos contribuye al desarrollo de las siguientes competencias, generales y específicas, que son comunes a los dos grados en que se imparte:

- Competencias generales:
  - Competencia de gestión y planificación: iniciativa y motivación. Planificación y organización así como un manejo adecuado del tiempo.
  - Trabajo en equipo, desarrollando distinto de funciones o roles. En la Sociedad del Conocimiento se presta especial atención a las potencialidades del trabajo en equipo y a la construcción conjunta de conocimiento, por lo que las competencias relacionadas con el trabajo colaborativo son particularmente relevantes: habilidad para coordinarse con el trabajo de otros y la habilidad para negociar de forma eficaz.
  - Competencias cognitivas superiores: selección y manejo adecuado de conocimientos, recursos y estrategias cognitivas de nivel superior apropiados para el afrontamiento y resolución de diversos tipos de tareas/problemas con distinto nivel de complejidad y novedad.
  - Competencias en el uso de las herramientas y recursos de la Sociedad del Conocimiento:
    - Manejo de las TIC.
    - Competencia en la búsqueda de información relevante.

- Competencia en la gestión y organización de la información.
- Competencia en la recolección de datos, el manejo de bases de datos y su presentación.

- Competencias de bloque común de la rama de Informática:
  - Capacidad para diseñar, desarrollar, seleccionar y evaluar, aplicaciones y sistemas informáticos, asegurando su
  - fiabilidad, seguridad y calidad, conforme a los principios éticos y a la legislación y normativa vigente.
  - Capacidad para elaborar el pliego de condiciones técnicas de una instalación informática que cumpla los estándares y normativas vigentes.
- Competencias del bloque tecnológico de Tecnologías de la Información:
  - Capacidad para seleccionar, diseñar, implantar, integrar, evaluar, explotar y mantener las tecnologías de hardware, software y redes, dentro de los parámetros de coste y calidad adecuados.

Como es evidente, esta asignatura requiere de los conocimientos y competencias adquiridas en materias de segundo curso, concretamente en las asignaturas de *Sistemas Operativos* y *Redes de Computadores.*
El nivel de conocimientos alcanzado de la materia está entre bajo y medio, un nivel considerado suficiente para poder integrar con éxito la seguridad informática como un criterio más, y esencial, en cualquier proyecto de ingeniería informática.

3.REQUISITOS PREVIOS REQUERIDOS PARA CURSAR LA ASIGNATURA

Como se ha descrito previamente esta asignatura, que inicia el estudio de una nueva materia, se apoya fuertemente en los conocimientos y competencias adquiridos en asignaturas de segundo curso. Sin esta base de conocimientos la asignatura presentará un nivel alto de dificultad al alumno que la aborde por primera vez.
En concreto, guarda gran relación con las asignaturas de:

- *Sistemas Operativos.* Por una parte, todos los sistemas operativos ofrecen herramientas de seguridad propias. El conocimiento del funcionamiento del sistema operativo y sus posibilidades nos permiten una primera aproximación a la seguridad. Por otra parte, las herramientas de detección y prevención de ataques se instalar en contextos específicos que incluyen las características del sistema operativo. Así que es recomendable conocer los procesos de instalación y configuración de aplicaciones en el sistema operativo objetivo. Junto que existen vulnerabilidades orientadas a explotar defectos de programación de algunos sistemas operativos.
- *Redes de computadores*. Es evidente que gran parte del proceso de seguridad se va centrar en las redes como origen de posibles amenazas. Por ello es importante conocer los diferentes protocolos de comunicación así como los diferentes elementos de interconexión entre dichas redes, que dan lugar a las arquitecturas de redes. Luego, será fundamental un conocimiento de la arquitectura OSI así como la arquitectura TCP/IP que engloban la mayoría de los protocolos en los que se basa Internet.

Además es recomendable el conocimiento de lenguajes de programación orientado a objetos, tales como Java ó C#, que permitan el desarrollo de pequeñas herramientas propias de prevención o detección de intrusiones así como pequeños simuladores de ataques a sistemas informáticos que permitan la realización de actividades prácticas fundamentadas en los contenidos de la asignatura.

4.RESULTADOS DE APRENDIZAJE

El objetivo básico de la asignatura Seguridad es dar una visión completa y clara de los fundamentos básicos de la seguridad informática aplicada. Como resultado del estudio y aprendizaje de los contenidos de esta asignatura el estudiante será capaz de:
RA9. *Comprender el entorno operativo de seguridad de red (NSM) y las buenas prácticas asociadas a la implementación de dicho modelo. Por ello se plantean los siguientes objetivos:*

Objetivo 1.Comprender la trascendencia de introducir (o no) la seguridad como un criterio de diseño en cualquier sistema o aplicación informática.
Objetivo 2.Comprender los problemas más habituales actuales que implica la falta de seguridad en sistemas, aplicaciones y redes.
Objetivo 3.Clasificar los diferentes ataques desde el punto de vista de peligrosidad, organización y necesidad de recursos.
Objetivo 4.Comprender la necesidad de la puesta en marcha de una política de seguridad informática en cualquier organización.
Objetivo 5.Entender la trascendencia para las organizaciones de una correcta implementación de la LOPD (Ley Orgánica de Protección de Datos).

Objetivo 6.Entender la relevancia de la puesta en marcha de un Sistema de Gestión de Seguridad Informática que siga las buenas prácticas recomendadas en los estándares internacionales ISO/IEC 27001 e ISO/IEC 27002.

RA10. *Utilizar toda una gama de herramientas de software libre, entre las que se encuentran Sguil, Argus y Wireshark, para hacer prospecciones en el tráfico de red en busca de datos de contenido completo, de sesión, estadístico y de alerta. Por ello se plantean los siguientes objetivos:*

Objetivo 7.Entender, y saber implantar, las defensas básicas en sistemas operativos, aplicaciones y dispositivos básicos de comunicaciones.

Objetivo 8.Aplicar los conceptos más elementales aprendidos, relacionados con la seguridad en redes, sistemas y datos, a una organización concreta.

Objetivo 9.Comprender qué son los analizadores de vulnerabilidades de seguridad y cómo se usan.

Objetivo 10.Comprender qué son los cortafuegos y herramientas de scanning de seguridad, cómo se usan y qué papel juegan en una política de seguridad.

Objetivo 11.Comprender qué son los sistemas de detección de intrusiones (IDS) y qué papel juegan en una política de seguridad.

Objetivo 12.Conocer herramientas de software libre para el análisis del tráfico de red en busca de datos de contenido completo, de sesión, estadístico y de alerta.

RA11. *Conocer y emplear las mejores herramientas para generar paquetes arbitrarios, explorar defectos, manipular el tráfico y efectuar reconocimientos. Por ello se plantean los siguientes objetivos:*

Objetivo 13.Describir las mejores herramientas para la puesta en marcha de una política de seguridad.

Así mismo, y como resultados de aprendizaje transversales del grado de Ingeniería Informática tenemos los siguientes objetivos:

Objetivo 14.Revisar, conocer y juzgar los conocimientos adquiridos.

Objetivo 15.Reconocer el espacio de trabajo virtual personalizado del curso y diferenciar las herramientas disponibles por parte del equipo docente.

Objetivo 16.Conocer el funcionamiento básico de la entrega de actividades y/o ejercicios prácticos relativos al seguimiento y evaluación de los progresos del curso.

5.CONTENIDOS DE LA ASIGNATURA

Los contenidos de la asignatura se dividen en cuatro módulos:

Módulo 1: *Conceptos e implementación de la monitorización de la seguridad en redes.*

En este primer módulo introducimos los problemas de la seguridad informática. Debemos tener en cuenta que la seguridad no es un estado que se debe alcanzar, sino un proceso que se adapta al contexto según evoluciona el sistema. Pero para comprender mejor el proceso de la seguridad se presentan los problemas de seguridad que podemos encontrarnos tanto a nivel físico como software. También se dedica atención a la normativa legal vigente que afecta al proceso de seguridad. El proceso de seguridad quedará reflejado en una política de seguridad, que dictamina las principales defensas contra estos posibles ataques. Una vez definida una política de seguridad el siguiente paso es el seguimiento del cumplimiento de esta política. Por último, caracterizaremos el conjunto de intrusiones que se nos pueden presentar.

Contenidos:

- Unidad 1: Descripción del problema de la seguridad en las comunicaciones y en la información. Tipos de ataques.
  - Introducción
  - Las preguntas que deben hacerse para definir el problema
  - Soluciones aparentemente perfectas y soluciones razonables
- Unidad 2: La seguridad en los elementos físicos existentes en la red.
  - Introducción
  - Los sistemas de cableado o inalámbricos
  - Repetidores, hubs y conmutadores
  - Encaminadores
  - Los servidores y otras máquinas.
- Unidad 3: La seguridad en los elementos software existentes en una red.
  - Introducción
  - Los sistemas operativos de estaciones y servidores
  - Los protocolos y aplicaciones IP
  - Mejoras de seguridad IPv6
  - Criterios de evaluación de seguridad
- Unidad 4: Métodos de ataque a equipos y redes.
  - Introducción
  - Taxonomía de los tipos de ataques
  - Ataques orientados a la obtención de información sobre el objetivo
  - Ataques orientados a la obtención no autorizda de información confidencial.

- Ataques de Denegación de servicios (DoS)
- Ataques "creativos"

- Unidad 5: Defensa básicas ante ataques.
  - Introducción
  - Controles de acceso físico a los sistemas
  - Controles de acceso lógico a los sistemas
  - Otros controles simles de acceso a la información

Módulo 2: *Prácticas recomendadas en la implantación de procesos de seguridad.*
Este módulo se centra en los administradores de procesos de seguridad. Se presentan prácticas recomendadas para la estimación, protección, detección y respuesta en un proceso de seguridad. A pesar que a lo largo de los otros módulos veremos recomendaciones, herramientas y técnicas a aplicar, en esta parte se ilustran apoyándose en casos prácticos que mejoran la comprensión de los contenidos teóricos.
Contenidos:

- Unidad 6: La política de seguridad como respuesta razonable a los problemas de seguridad en las comunicaciones y en la información.
  - ¿Qué es una política de seguridad?
  - Aspectos físicos de la política de seguridad
  - Aspectos lógicos de la política de seguridad
  - Aspectos humanos y organizativos de la política de seguridad
  - Aspectos legales de la política de seguridad
- Unidad 7: Métodos no criptográficos en la implantación de la política de seguridad.
  - Herramientas que implementen la política de seguridad
  - Otros elementos típicos a tener en cuenta.
- Unidad 8: Redes privadas virtuales.
  - Caracterización de las redes privadas virtuales
  - Ventajas e inconvenientes de las redes virtuales privadas
  - Arquitecturas de redes privadas virtuales
  - Diseño y planificación de redes privadas virtuales
  - Problemas de rendimiento, mantenimiento y seguridad.

Módulo 3: *Sistemas de gestión de la seguridad en redes.*
Dentro de este módulo se presentan los principales métodos utilizados para la implantación de diversas normas de seguridad. Por una parte, se analizar las técnicas de cortafuegos, desde las más sencillas, como los filtros de paquetes las más sofisticadas basadas en filtros dinámicos de conexión. Todos ellos se exponen en la primera parte del módulo incluyendo ejemplos ilustrativos.La segunda parte del módulo se concentra en los sistemas de detección de intrusos (IDS), que suelen implementar prácticamente todas las técnicas de monitorización reseñadas en el primer módulo del temario. Por lo tanto, debemos conocer qué requisitos deben satisfacer, las diferencias ente los IDS basados en máquinas y los basados en redes, así como las diferencias tecnológicas entre los que basan su trabajo en la detección de anomalías, de usos indebidos o de firmas de ataque.
Contenidos:

- *Parte 1: Protección de la red Cortafuegos*
  - Unidad 9: Los cortafuegos (firewalls) y sus aplicaciones como elementos básicos de una política de seguridad de redes
    - Los filtros de paquetes
    - Los gateways de aplicación o servidores proxy
    - ¿Qué se puede mejorar?
  - Unidad 10: Tecnología de última generación en cortafuegos.
    - Caso práctico: el modelo Cisco PIX Firewall
    - Caso práctico: el modelo Checkpoint Firewall-1
    - La confusión reinante
- *Parte 2: Sistemas de detección de intrusos (IDS)*
  - Unidad 11: Herramientas de detección de Intrusiones para la monitorización de la seguridad en las comunicaciones.
    - Introducción
    - Caso práctico: los sistemas Cisco Secure IDS
    - Caso práctico: los sistemas Red Secure de ISS
    - ¿Qué son los Honey Pots?

Módulo 4: *Análisis de Operaciones Intrusivas y herramientas disponibles.*
La monitorización de redes se basa en la captura y análisis de esta información para poder detectar y bloquear posibles intrusiones. Por ello es importante dedicar un espacio a presentar las herramientas disponibles en la actualidad así como la información que nos ofrecen y su interpretación. De esta forma nuestra política de seguridad tendrá mayores posibilidades de éxito.
Contenidos:

- Unidad 12: Herramientas de análisis de vulnerabilidades para la auditoría de la seguridad en las comunicaciones.
  - Introducción
  - Caso práctico: el modelo Cisco Secure Scanner
  - Caso práctico: los programas de Internet Security Systems.
- Unidad 13: Diseño seguro de redes. Concepto de alta disponibilidad y diseños redundante
  - Introducción
  - Diseño de soluciones de alta disponibilidad
  - Los problemas de infraestructura y soluciones
  - Los problemas en el nivel 2 de OSI y soluciones
  - Los problemas en el nivel 3 de OSI y soluciones
  - Consideraciones para el resto de los niveles OSI
  - Consideraciones para el almacenamiento en red: SAN (Storage Area Networks)
  - Consideraciones para los dispositivos de seguridad

6.EQUIPO DOCENTE

- ROBERTO HERNANDEZ BERLINCHES
- MARIA DE LOS LLANOS TOBARRA ABAD

7.METODOLOGÍA Y ACTIVIDADES DE APRENDIZAJE

La metodología de estudio utiliza la tecnología actual para la formación a distancia en aulas virtuales, con la participación del Equipo Docente, los Profesores Tutores y todos los alumnos matriculados. En este entorno se trabajaran los contenidos teórico- prácticos cuya herramienta fundamental de comunicación será el curso virtual, utilizando la bibliografía básica y el material complementario. Esta actividad del alumno en el aula virtual corresponde aproximadamente a un 10% del tiempo total asignado al estudio de la asignatura.
El trabajo autónomo de estudio, junto con las actividades de ejercicios y pruebas de autoevaluación disponibles, bajo la supervisión del tutor, con las herramientas y directrices preparadas por el equipo docente, completará aproximadamente un 70% del tiempo de preparación de la asignatura.
Por último esta asignatura tiene además programadas unas prácticas a distancia. Esta actividad formativa representa
aproximadamente el 20% del tiempo dedicado a la asignatura.

8.EVALUACIÓN

En esta asignatura se utilizan las siguientes modalidades de evaluación

- Evaluación continúa:
  - *Autoevaluación*, de carácter voluntario: En esta asignatura se plantea a los alumnos un proceso de autoevaluación, basado en la realización de pruebas de test. Estos ejercicios no serán evaluables. En el módulo de contenidos dentro del entorno virtual CiberUNED los alumnos podrán encontrar el apartado de “Autoevaluación” donde se alojarán tanto las pruebas como sus soluciones, con las que el alumno podrá autoevaluar sus conocimientos.
  - *Pruebas de evaluación a distancia*: En el módulo de contenidos dentro del entorno virtual CiberUNED los alumnos encontrarán el apartado de “Evaluación a distancia” donde se alojarán las pruebas (una por cada Unidad Didáctica) que serán evaluadas por los profesores tutores de los centros, con la ayuda del equipo docente. Consistirán en pequeños trabajos prácticos que permitirán comprobar la correcta asimilación de contenidos y la adquisición real de competencias relacionadas.
- Evaluación final de la asignatura que se llevará a cabo a partir de las siguientes pruebas:

- Realización de un *examen teórico/práctico,* que es indispensable aprobar para la superación de la asignatura y que contará como el 70% de la nota final.
- *Calificación de las prácticas obligatorias*, que es indispensable aprobar para la superación de la asignatura y que contarán, entre las tres, como el 30% de la nota final.

9.BIBLIOGRAFÍA BÁSICA

ISBN(13): 9788436249750
Título: SEGURIDAD EN LAS COMUNICACIONES Y EN LA INFORMACIÓN (1ª)
Autor/es: Castro Gil, Manuel Alonso ; Díaz Orueta, Gabriel ; Peire Arroba, Juan ; Mur Pérez, Francisco ;
Editorial: UNED

Buscarlo en Editorial UNED

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Comentarios y anexos:
Igualmente, el equipo docente ha desarrollado a medida un contenido que intentará actualizar constantemente el temario de la asignatura, que se distribuirá en el curso virtual de la asignatura en formato electrónico bajo licencia Creative Commons.
El texto de Díaz Orueta y otros comprende el 90% del desarrollo teórico de la asignatura. Contiene múltiples ejemplos y ejercicios resueltos, que ayudan mucho al estudio de la asignatura.

10.BIBLIOGRAFÍA COMPLEMENTARIA

LIBRO ACTUALMENTE NO PUBLICADO
ISBN(13):
Título: LA PROTECCIÓN DE DATOS PERSONALES, SOLUCIONES EN ENTORNOS MICROSOFT, VERSIÓN 2.0
Autor/es: Alonso J.M. Y Otros ;
Editorial: Disponible en la plataforma virtual

LIBRO ACTUALMENTE NO PUBLICADO
ISBN(13):
Título: SEGURIDAD EN UNIX Y REDES (http://es.tldp.org/Manuales-LuCAS/doc-unixsec/uni)
Autor/es: Antonio Villalón Huerta ;
Editorial: http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec.pdf

ISBN(13): 9780201634662
Título: FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER (2ND EDITION) (2º)
Autor/es: Steven M. Bellovin ; William Cheswick ;
Editorial: Addisson-Wesley

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

ISBN(13): 9788420541105
Título: COMUNICACIONES Y REDES DE COMPUTADORES (7ª)
Autor/es: Stallings, William ;
Editorial: PRENTICE-HALL

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

ISBN(13): 9788420546001
Título: EL TAO DE LA MONITORIZACIÓN DE SEGURIDAD EN REDES (2005)
Autor/es: R. Bejtlich ;
Editorial: PEARSON EDUCACIÓN

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

ISBN(13): 9789688805411
Título: REDES GLOBALES DE INFORMACIÓN CON INTERNET Y TCP/IP
Autor/es: D. E. Comer ;
Editorial: PEARSON-PRENTICE HALL

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

Comentarios y anexos:
Los libros de Stalling y Comer son un gran complemento para repasar toda una serie de conceptos, estándares y protocolos de comunicación (especialmente TCP/IP) necesarios como base para la adquisición correcta de conocimientos y capacidades asociadas con los contenidos de la asignatura.
El libro de Cheswick y otros es una muy buena aproximación a los conceptos e implementaciones más inteligentes de los cortafuegos, herramientas con poco más de 20 años de historia, pero que se han convertido en una herramienta imprescindible para la puesta en marcha de cualquier política de seguridad informática para cualquier tipo de organización.
Seguridad en Unix y Redes, aborda de manera global el tema de seguridad, no solo a nivel de las redes de comunicaciones, en entornos Linux/Unix. Abarca desde la securización de componentes hardware hasta el conchero de auditoria (y sus herramientas Unix/Linux asociadas). Se presentan diferentes sistemas operativos basados en Linux junto a sus premisas de seguridad. Dispone de una parte dedicada totalmente a las herramientas de seguridad de redes en entornos Unix, con especial detalle en los sistemas

de prevención (cortafuegos) y detección (IDS). Es una obra muy completa que cubre muchos conceptos globales de seguridad como la propia criptografía entre otras
El Tao de la monitorización de Seguridad en redes, aborda de una manera profunda los conceptos básicos sobre el modelo de seguridad de redes en todas sus fases: definición, diseño, implantación y evaluación. Se hace especial hincapié en las herramientas de monitorización de redes, en concreto las disponibles como Open Source, como piezas clave para la obtención de información sobre posibles ataques que permita detectar problemas en el modelo de seguridad. Se presentan casos prácticos desde el punto de vista de los administradores de la seguridad de red y sistemas para poder evaluar la seguridad desde el punto de vista de un atacante externo.
La primera parte (legal) del texto de Alonso y otros complementa con mucho detalle el apartado del libro básico sobre la LOPD (Ley Orgánica de Protección de Datos). Aunque no será objeto de evaluación, su segunda parte (técnica) es una muy buena presentación de cómo usar una tecnología concreta para implementar correctamente la LOPD.

11.RECURSOS DE APOYO

Como materiales adicionales para el estudio de la asignatura se ofrece en el curso virtual:

- Esta guía de estudio y la guía didáctica de estudio de la asignatura.
- Distintos libros electrónicos gratuitos, algunos interactivos.
- Material desarrollado exprofeso para el curso por el equipo docente
- Apartado de noticias y enlaces interesantes, relacionados con el desarrollo de la asignatura
- Pruebas prácticas de evaluación a distancia.
- Enunciados y soluciones de ejercicios teórico-prácticos que el alumno puede usar como ejercicios de autoevaluación.
- Lista de preguntas frecuentes.

12.TUTORIZACIÓN

La enseñanza a distancia utilizada para el seguimiento de esta asignatura, que garantiza la ayuda al alumno, dispone de los siguientes recursos:

1. Tutores en los centros asociados. Los tutores serán los encargados del seguimiento y control de las pruebas que constituyen la evaluación continua del alumno.
2. Tutorías presenciales o virtuales en el centro asociado correspondiente.
3. Entorno Virtual. A través de CiberUNED el equipo docente de la asignatura pondrá a disposición de los alumnos diverso material de apoyo al estudio, así como el enunciado del trabajo de prácticas. Se dispone además de foros donde los alumnos podrán plantear sus dudas para que sean respondidas por los tutores o por el propio equipo docente. Es el SOPORTE FUNDAMENTAL de la asignatura, y supone la principal herramienta de comunicación entre el equipo docente, los tutores y los alumnos, así como de los alumnos entre sí.
4. Tutor de Apoyo en Red (TAR). Se encarga de las siguientes tareas:

   - Elaborar una lista de preguntas frecuentes con las respuestas que dé el Equipo docente a las dudas de contenidos y dejarlas disponibles a través del entorno virtual.
   - Atender aquellas consultas que no tengan que ver con dudas de contenidos, y recopilar aquellas que traten sobre contenidos en el foro de alumnos, para que el equipo docente las responda y puedan ser publicadas en la lista de preguntas frecuentes.
   - Preparar resúmenes periódicos sobre la actividad que ha habido en los foros con el fin de que los alumnos puedan saber de qué se ha hablado o qué cuestiones se han tratado sin necesidad de leer todo para estar al corriente.
   - Mantener los foros ordenados en la medida de lo posible, recolocando aquellos mensajes que hayan sido dirigidos a foros que no corresponde.

5. Tutorías con el equipo docente: los lunes de 15:00 a 19:00 h para el periodo durante el que se desarrolla la asignatura, en el teléfono 913989566 o presencialmente. También en cualquier momento del curso por correo electrónico a roberto@scc.uned.es ó llanos@scc.uned.es o en el entorno CiberUNED.