

DATOS GENERALES DE LA ASIGNATURA

ASIGNATURA: Seguridad Informática y Criptografía

PLAN DE ESTUDIOS: Grado en Ingeniería Informática

GRUPO: 1718-M

CENTRO: Escuela Politécnica Superior

CARÁCTER DE LA ASIGNATURA: Obligatorio

ECTS: 6,0

CURSO: 3º

SEMESTRE: 2º Semestre

IDIOMA EN QUE SE IMPARTE:

Castellano, excepto las asignaturas de idiomas que se impartirán en el idioma correspondiente

DATOS DEL PROFESOR

NOMBRE Y APELLIDOS: Roberto Gutiérrez Fuente

EMAIL: roberto@uemc.es

TELÉFONO: 983 00 10 00

HORARIO DE TUTORÍAS: Jueves a las 17:00 horas

BREVE CV:

Licenciado en Ciencias Económicas y Empresariales por la Universidad de Valladolid.

Experiencia profesional:

- Docencia no reglada, en el ámbito de las redes de comunicaciones y sistemas microinformáticos.
- Docencia universitaria, en el ámbito de las redes de comunicaciones y seguridad informática.
- Dirección del Departamento de Administración de Sistemas Informáticos en la Universidad Europea Miguel de Cervantes.

Líneas de investigación:

- Perteneciente al grupo de investigación "GIE - Grupo de Innovación Educativa" UEMC.

DATOS ESPECÍFICOS DE LA ASIGNATURA

DESCRIPTOR DE LA ASIGNATURA:

Lograr un nivel de seguridad óptimo en el entorno informático (tanto en el ámbito personal como en el profesional o empresarial) se ha convertido en una de las metas de todos los usuarios. La implementación de la criptografía en estos ámbitos es cada día más importante por lo que los profesionales del sector deberán estar cualificados en el manejo de certificados digitales (y herramientas asociadas) para poder desempeñar su labor con garantías.

Por ello, desde el punto de vista del área de Sistemas Informáticos, la asignatura aporta pilares fundamentales para lograr la "higiene informática" requerida en cualquier entorno, mostrándose al estudiante los conceptos de seguridad imprescindibles a aplicar en modo personal o profesional (basados, casi siempre, en la criptografía).

De acuerdo con lo anterior, los contenidos se estructuran en los siguientes ejes:

- Tratamientos de la información.
- Criptografía y cifrado.
- Autenticación. Firmas y certificados.
- Seguridad en Internet. Comercio electrónico seguro.

- Técnicas de ataque y defensa en sistemas informáticos.

Es recomendable que el alumno haya cursado la asignatura Redes de Comunicaciones (o equivalente), en la que se introducen los conceptos fundamentales del networking. También es conveniente un manejo avanzado de sistemas operativos Microsoft y conocimientos básicos sobre aplicaciones de virtualización.

CONTENIDOS DE LA ASIGNATURA:

PROGRAMA DE TEORÍA.

Tema 1. Información y Seguridad.

Amenazas. Servicios y mecanismos de seguridad. Política de seguridad.

Tema 2. Criptografía y cifrado.

Criptosistemas. Tipos de cifrado: simétrico, asimétrico e híbrido.

Tema 3. Autenticación. Firmas y certificados.

Cifrado vs firma digital. Función Hash. Autenticación y firma digital. Certificados digitales y autoridades de certificación. Estructuras PKI. Aplicaciones criptográficas.

Tema 4. Comercio electrónico seguro. Seguridad en Internet.

Protocolos de pago. Métodos de pago basados en tarjeta de crédito. Dinero electrónico. Estafas 'phishing' y 'pharming'.

Tema 5. Técnicas de ataque y defensa en Sistemas Informáticos.

Sniffing. Spoofing. Troyanos. Rootkits.

PROGRAMA DE PRACTICAS.

La base práctica de la asignatura se fundamenta en:

- Manejo de certificados digitales.
- Gestión de correo electrónico seguro. Comercio electrónico seguro.
- Empleo de técnicas de monitorización de red. Prácticas de sniffing y ARP spoofing.

El alumno debe elaborar una Memoria de prácticas que documente todas las prácticas realizadas (en clase o como trabajo autónomo).

RECURSOS DE APRENDIZAJE:

Las actividades de trabajo presencial (clases presenciales, clases prácticas, laboratorio, etc.) se realizan en el aula o en el laboratorio. Para el desarrollo de las clases presenciales se utilizan diferentes herramientas (plataforma Moodle UEMC, pizarra, cañón, etc.). Durante el desarrollo de estas clases hay determinados tiempos, aplicados cuando sea pertinente, dedicados a la realización de ejercicios aclaratorios y ejemplos ilustrativos.

COMPETENCIAS Y RESULTADOS DE APRENDIZAJE A ADQUIRIR POR EL ALUMNO

COMPETENCIAS GENERALES:

- CG01. Capacidad de análisis y síntesis
- CG06. Capacidad de gestión de la información
- CG07. Resolución de problemas
- CG08. Toma de decisiones
- CG09. Trabajo en equipo
- CG14. Razonamiento crítico
- CG16. Aprendizaje autónomo
- CG17. Adaptación a nuevas situaciones
- CG22. Motivación por la calidad

- CG24. Orientación al resultado
- CG25. Orientación al cliente

COMPETENCIAS ESPECÍFICAS:

- CE18. Conocer los fundamentos y técnicas de seguridad aplicables a sistemas informáticos y redes, así como las principales técnicas criptográficas
- CE40. Aptitud para estudiar las necesidades de informatización de las organizaciones, diseñar y proponer soluciones de infraestructura informática, y participar en su implantación
- CE44. Aptitud para planificar, implantar y gestionar políticas de seguridad globales en las organizaciones, implantándolas a nivel de red, usuario y/o información, teniendo en cuenta los distintos sistemas de control de acceso, integridad de datos, etc.

RESULTADOS DE APRENDIZAJE:

El alumno será capaz de:

- Demostrar conocimiento de las principales técnicas de criptografía y su aplicación a los sistemas informáticos.
- Redactar informes de evaluaciones de los riesgos de los sistemas informáticos y elaboración de políticas de seguridad genéricas y especificadas para las distintas organizaciones.

BIBLIOGRAFÍA Y RECURSOS DE REFERENCIA GENERALES

BIBLIOGRAFÍA BÁSICA:

- Lucena López, Manuel José (2010). *Criptografía y Seguridad en Computadores*. (<http://criptografiayseguridad.blogspot.com.es/p/criptografia-y-seguridad-en.html>).
- Bradley, Tony (2009). *Manual práctico de protección del PC y seguridad en Internet*. Madrid: Anaya Multimedia.
- Stallings, William (2004). *Fundamentos de seguridad en redes. Aplicaciones y estándares*. Madrid: Pearson Educación.
- Gómez Vieites, Alvaro (2011). *Enciclopedia de la Seguridad Informática*. Madrid: Ra-Ma.
- ACISSI (2011). *Seguridad Informática. Ethical Hacking*. Ediciones ENI.
- Pérez Agudín, Justo (2005): *La biblia del hacker*. Madrid: Anaya Multimedia.
- Tanenbaum, Andrew S. (2003): *Redes de computadoras*. México: Pearson Educación.

BIBLIOGRAFÍA COMPLEMENTARIA:

- Molina Mateos, José María (2000). *Seguridad de la información*. Santa Fe: El Cid Editor.
- Ramos Alvarez, Benjamín; Ribagorda Gamacho, Arturo (2004). *Avances en criptología y seguridad de la información*. Madrid: Ediciones Díaz de Santos.

WEBS DE REFERENCIA:

Web / Descripción

<http://www.faqs.org/rfcs/>

Internet RFC Archives. Conjunto de documentos RFC (Requests For Comments) con las especificaciones técnicas de los protocolos aplicados en Internet.

<http://www.tcpipguide.com/free/index.htm>

Kozierok, Charles M. The TCP/IP Guide. Guía de referencia TCP/IP.

<http://technet.microsoft.com/en-us/library/bb742616.aspx>

Microsoft. Technet Library. Networking. Conjunto de recursos Microsoft sobre la orientación networking de sus sistemas operativos.

<http://criptografiayseguridad.blogspot.com.es/>

Blog Criptografía y Seguridad. Profesor Manuel J. Lucena López.

OTRAS FUENTES DE REFERENCIA:

e-campus UEMC. Curso de la asignatura.

PLANIFICACIÓN DEL PROCESO DE ENSEÑANZA-APRENDIZAJE DE LA ASIGNATURA

METODOLOGÍAS:

MÉTODO DIDÁCTICO:

Esta asignatura cuenta con una amplia carga teórica, lo que habilita la utilización del método didáctico o expositivo. Se basa en el concepto de clase magistral, en el que también se incluye la resolución en clase de ejercicios y problemas.

MÉTODO DIALÉCTICO:

En algunos componentes de la asignatura, como la presentación y la corrección (mediante el foro) de los trabajos en grupo, se utiliza el método dialéctico, que habilita una participación más activa de los alumnos.

MÉTODO HEURÍSTICO:

La realización de los trabajos propuestos, relacionados con diversos campos de la seguridad informática, requiere un trabajo autónomo a desarrollar por parte del alumno.

CONSIDERACIONES DE LA PLANIFICACIÓN:

La asignatura se planifica teniendo en cuenta las siguientes actividades formativas:

- *Clase presencial*. Se sucederán a lo largo de todo el curso. Se utilizará, principalmente, el método didáctico o expositivo. La mayor parte de estas clases se llevarán a cabo en *Laboratorio Informático*, por lo que tendrán un alto componente de *Clases prácticas*.
- *Presentación de trabajos*. Los alumnos deberán realizar (y entregar para su evaluación) una serie de trabajos sobre temáticas relacionadas con la asignatura. Dichos trabajos se presentarán en clase y se establecerá un foro de corrección común. Por otro lado, se deberá confeccionar una Memoria de Prácticas para documentar los ejercicios realizados en clase.
- *Tutorías grupales*. Las tutorías grupales se establecen (dentro de los horarios y ubicaciones oficiales de tutoría marcados para la asignatura) de forma previa a cada una de las actividades de evaluación y de recogida de trabajos y proyectos. El profesor informará, con la debida antelación, sobre cada una de estas sesiones.
- *Tutorías individuales*. Lado, las tutorías individuales se desarrollan en el despacho del profesor a la hora fija especificada. En el caso de requerir laboratorio para su desarrollo, el profesor se ocupa de tramitar una reserva con la debida antelación.

Estructura temporal de la asignatura:

- Bloque 1 de contenidos teóricos. Corresponde a los temas 1 y 2. Se desarrolla entre el comienzo de curso y la 4ª semana aproximadamente. Al final de dicho período se fija una sesión de tutoría grupal, justo antes de la actividad de evaluación asociada.
- Bloque 2 de contenidos teóricos. Corresponde a los temas 2 y 3. Se desarrolla entre la 5ª y la 10ª semanas de curso, aproximadamente. Al final de dicho período se fija una sesión de tutoría grupal, justo antes de la actividad de evaluación asociada.
- Bloque 3 de contenidos teóricos. Corresponde al tema 5. Se desarrolla entre la 11ª y la 15ª semanas de curso, aproximadamente. Al final de dicho período se fija una sesión de tutoría grupal, justo antes de la actividad de evaluación asociada.
- Trabajos en grupo. Durante las semanas 12ª y 13ª de curso se llevarán a cabo la entrega de trabajos, su presentación en clase y los posteriores comentarios de análisis y corrección a través de un foro especial vinculado a la asignatura.
- Prácticas. A lo largo del curso se realizarán prácticas de apoyo al contenido teórico. Dichas prácticas deberán documentarse por parte del alumno para confeccionar una Memoria de Prácticas, que se entregará al final del curso.

Esta planificación puede verse modificada por causas ajenas a la organización académica primeramente presentada. El profesor informará convenientemente a los alumnos de las modificaciones puntuales.

PROGRAMACIÓN DE ACTIVIDADES Y EVALUACIONES:

PROGRAMACIÓN DE ACTIVIDADES:

Actividad	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	¿Se evalúa?	EO	EE
1ª actividad de evaluación continua (temas 1 y 2)				X												X	X	
2ª actividad de evaluación continua (temas 3 y 4)										X						X	X	
3ª actividad de evaluación continua (tema 5)															X	X	X	
Presentación de trabajos en grupo												X				X	X	X
Foro de análisis y corrección de trabajos													X			X	X	X
Entrega de Memoria de Prácticas															X	X	X	X

CONSIDERACIONES DE LA EVALUACIÓN:

El conocimiento de los contenidos y la adquisición de las competencias relativos a esta asignatura se evalúan de forma continua, utilizando los sistemas que a continuación se detallan:

- Tanto las pruebas de evaluación parciales como las finales (en el caso de que fueran necesarias) constarán siempre de un conjunto de preguntas de tipo test y de otro de preguntas de respuesta corta. La información concreta sobre cada prueba (descripción, valoración, convocatoria, etc.) se publica en el *e-Campus* de la asignatura con la debida antelación.
- Descripción de las actividades de evaluación continua:
 - 1ª actividad de evaluación continua. Corresponde a los temas 1 y 2 (15% de la nota final). Se evalúa a través de: *Pruebas objetivas (verdadero/falso, elección múltiple, emparejamiento de elementos,...)* (10% de la nota final) y *Pruebas de respuesta corta* (5% de la nota final).
 - 2ª actividad de evaluación continua. Corresponde a los temas 3 y 4 (30% de la nota final). Se evalúa a través de: *Pruebas objetivas (verdadero/falso, elección múltiple, emparejamiento de elementos,...)* (20% de la nota final) y *Pruebas de respuesta corta* (10% de la nota final).
 - 3ª actividad de evaluación continua. Corresponde al tema 5 (25% de la nota final). Se evalúa a través de: *Pruebas objetivas (verdadero/falso, elección múltiple, emparejamiento de elementos,...)* (16,67% de la nota final) y *Pruebas de respuesta corta* (8,33% de la nota final).
 - Realización y presentación en clase de trabajos en grupo sobre temas relacionados con la asignatura (evaluados a través de *Trabajos y proyectos*). Esta actividad supone un 10% de la nota final. Tanto la herramienta de entrega como las instrucciones concretas con respecto a esta actividad se publican en el *e-Campus* de la asignatura con la debida antelación.
 - Foro de análisis y corrección de trabajos. Supone un 5% de la nota final. Se evalúa a través del sistema *Técnicas de observación (registros, listas de control,...)*. Tanto el foro como las instrucciones concretas con respecto a esta actividad se publican en el *e-Campus* de la asignatura con la debida antelación.
 - Memoria de prácticas. Esta actividad supone un 10% de la nota final. Tanto la herramienta de entrega como las instrucciones concretas con respecto a esta actividad se publican en el *e-Campus* de la asignatura con la debida antelación.
 - Algunas de las competencias de tipo genérico asociadas a la asignatura (capacidad de análisis y síntesis; organización; planificación; toma de decisiones; trabajo en equipo; creatividad; razonamiento crítico; etc.) incorporan a los sistemas de evaluación enunciados en este apartado un componente basado en *Técnicas de observación (registros, listas de control,...)* en cada una de las actividades realizadas a lo largo del curso (incluidas las tutorías). En global, este componente supone un 5% de la nota final para todos aquellos alumnos que utilicen las convocatorias ordinaria o extraordinaria. La nota no se mantiene para la convocatoria extraordinaria.

Normas sobre la evaluación en convocatoria ordinaria:

- Para superar la asignatura es necesario que el alumno obtenga una calificación global (media) mínima de 5 puntos sobre 10.
- Sólo se habilita un plazo para la presentación (y su análisis y corrección a través del foro) de trabajos en grupo y para la entrega de la memoria de prácticas, por lo que la calificación de dichas actividades (llevadas a cabo durante el curso, dentro del proceso de evaluación continua) es la definitiva

para la convocatoria ordinaria.

- Para superar la asignatura aplicando la evaluación continua sólo se permite un suspenso en cualquiera de las actividades propuestas, siempre que dicho suspenso no tenga una nota inferior a 3,5 puntos sobre 10 y que, evidentemente, la media global supere el 5. Dentro de este proceso, sólo se habilita una convocatoria por cada actividad.
- Los alumnos que no logren el aprobado mediante el sistema de evaluación continua deben superar una prueba final única y global sobre el contenido del Programa de Teoría de la asignatura. La nota final, en este caso, tiene en cuenta el resultado de este ejercicio (en vez de las citadas actividades de evaluación parciales).
- La nota final de la convocatoria ordinaria se compone de los siguientes elementos y porcentajes:
 - El resultado de las pruebas de evaluación sobre el Programa de Teoría -ya sean las actividades de evaluación sucesivas en período de evaluación continua o la prueba final única en el caso de no haber superado la evaluación continua-, cuyos porcentajes sobre la nota final son: 46,67% en Pruebas objetivas (verdadero/falso, elección múltiple, emparejamiento de elementos,...) y 23,33% en Pruebas de respuesta corta.
 - La calificación obtenida en el bloque de trabajos y memoria, es decir, los trabajos en grupo (Trabajos y proyectos, 10%), el foro de análisis y corrección (Técnicas de observación (registros, listas de control, ...), 5%) y la memoria de prácticas (Informes/memorias de prácticas, 10%).
 - La componente asociada a la adquisición de competencias de tipo genérico (Técnicas de observación (registros, listas de control,...), 5%).

Normas sobre la evaluación en convocatoria extraordinaria:

- Los alumnos que necesiten utilizar esta convocatoria realizarán una prueba única y global sobre el contenido del Programa de Teoría de la asignatura.
- En esta convocatoria se contempla una nueva presentación voluntaria de trabajos individuales o en grupo (pero nunca el foro de análisis y corrección asociado). También se puede optar, si fuera el caso, por mantener la nota del trabajo defendido en primera convocatoria (sólo el componente *Trabajos y proyectos*).
- Con respecto a la memoria de prácticas, por defecto se mantiene la nota de la memoria presentada en la convocatoria ordinaria, aunque existe la posibilidad de que el alumno presente una nueva memoria para alcanzar una mejor calificación.
- En la convocatoria extraordinaria no se aplicará el sistema de calificación Técnicas de observación (registros, listas de control,...) ya que el carácter extraordinario (no presencial para ciertas actividades) de dicha convocatoria no lo permite.

La nota final de la convocatoria extraordinaria, por tanto, se compone de los siguientes elementos y porcentajes:

- El resultado de la prueba única sobre el contenido del Programa de Teoría (53,34% Pruebas objetivas (verdadero/falso, elección múltiple, emparejamiento de elementos,...); 26,66% Pruebas de respuesta corta).
- El bloque de trabajos y memoria (20%), compuesto por los trabajos en grupo (Trabajos y proyectos, 10%) y la memoria de prácticas (Informes/memorias de prácticas, 10%).

Nota. La realización fraudulenta de cualquiera de las pruebas de evaluación, así como la extracción de información de las pruebas de evaluación, será sancionada según lo descrito en el Reglamento 7/2015, de 20 de noviembre, de Régimen Disciplinario de los estudiantes, Arts. 4, 5 y 7 y derivarán en la pérdida de la convocatoria correspondiente, así como en el reflejo de la falta y de su motivo en el expediente académico del alumno.

SISTEMAS DE EVALUACIÓN:

SISTEMA DE EVALUACIÓN	PORCENTAJE (%)
Pruebas de respuesta corta	23,33%
Trabajos y proyectos	10%
Técnicas de observación	10%
Pruebas objetivas	46,67%
Informes de prácticas	10%

EVALUACIÓN EXCEPCIONAL:

Los estudiantes que por razones excepcionales no puedan seguir los procedimientos habituales de evaluación continua exigidos por el profesor podrán solicitar no ser incluidos en la misma y optar por una «evaluación

excepcional». El estudiante podrá justificar la existencia de estas razones excepcionales mediante la cumplimentación y entrega del modelo de solicitud y documentación requerida para tal fin en la Secretaría de la Universidad Europea Miguel de Cervantes en los siguientes plazos: con carácter general, desde la formalización de la matrícula hasta el viernes de la segunda semana lectiva del curso académico para el caso de alumnos de la Universidad, y hasta el viernes de la cuarta semana lectiva del curso académico para el caso de alumnos de nuevo ingreso. En los siete días hábiles siguientes al momento en que surja esa situación excepcional si sobreviene con posterioridad a la finalización del plazo anterior.