DATOS GENERALES DE LA ASIGNATURA

ASIGNATURA: Fundamentos de Seguridad Informática y Criptografía

PLAN DE ESTUDIOS: Grado en Ingeniería Informática (PGR-INFORM)

GRUPO: 2425-M1

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: PABLO ABEL CRIADO LOZANO

EMAIL: pacriado@uemc.es

TELÉFONO: 983 00 10 00

HORARIO DE TUTORÍAS: Miércoles a las 10:00 horas

CV DOCENTE:

Desde el año 2019 al 2021 he impartido clase en la UEMC de las asignaturas:

- Redes de Comunicaciones
- Seguridad Informática y Criptografía

Desde el año 2021 he impartido clase en la UEMC de las asignaturas:

- Seguridad Informática y Criptografía
- Ataques a sistemas imformáticos

CV PROFESIONAL:

He formado parte de equipos tanto en el ámbito de sistemas como en el ámbito de desarrollo, asi como en equipos dedicados exclusivamente a ciberseguridad.

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 y conocimientos básicos sobre aplicaciones de virtualización.

CONTENIDOS DE LA ASIGNATURA:

1. **Bloque 1**
   1. Información y seguridad : Conceptos básicos. Servicios y mecanismos de seguridad.. Políticas de seguridad. Amenazas.
   2. Criptografía y cifrado : Tipos de cifrado: simétrico, asimétrico e híbrido.
2. **Bloque 2**
   1. Autenticación. Firmas y certificados. : Cifrado vs firma digital. Función Hash. Autenticación y firma digital. Certificados digitales y autoridades de certificación. Estructuras PKI. Aplicaciones criptográficas.
   2. Comercio electrónico seguro. Seguridad en Internet : Protocolos de pago. Métodos de pago basados en tarjeta de crédito. Dinero electrónico. Estafas ‘phishing’ y ‘pharming’.
3. **Bloque 3**
   1. Técnicas de ataque y defensa en Sistemas Informáticos. : Sniffing, spoofing ,hardening y otras técnicas para atacar y defender sistemas informáticos.

OBSERVACIONES CONTENIDO DE LA ASIGNATURA:

Se realizarán prácticas sobre los diferentes temas de teoría. Los alumnos deberán elaborar memorias de prácticas que documenten todas las prácticas realizadas y realizar presentaciones de algunas de ellas.

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:

- CG02. Capacidad y habilidad para la toma de decisiones en el ámbito tecnológico

COMPETENCIAS ESPECÍFICAS:

- CI1. Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente
- SI2. 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
- ICO6. Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos

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:

- Bradley, Tony (2009): Manual práctico de protección del PC y seguridad en Internet. Anaya Multimedia. ISBN: 9788441523074
- James F. Kurose y Keith W.Ross (2010): Redes de computadoras. Un enfoque descendente.. Pearson. ISBN: 978-84-7829-119-9
- Dafydd Stuttard y Marcus Pinto. (2011): The Web Application Hackers Handbook.. Wiley. ISBN: 978-1-118-02647-2

BIBLIOGRAFÍA COMPLEMENTARIA:

- Alfonso Muñoz Muñoz (2016): Privacidad y ocultación de información digital. Esteganografía. Protegiendo y atacando redes informáticas.. Ra-Ma. ISBN: 978-84-9964-644-2

WEBS DE REFERENCIA:

Web / Descripcion

http://www.faqs.org/rfcs/(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(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(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(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 de los trabajos, 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.
- **Presentación de trabajos.** Los alumnos deberán realizar (y entregar para su evaluación) una serie de

trabajos sobre temáticas relacionadas con la asignatura. Algunos de dichos trabajos se presentarán en clase.
- **Tutorías individuales.** Las tutorias individuales se desarrollaran en modalidad online en el horario especificado en la guia docente.
- **Evaluación.** La asignatura se evalúa -en su modo de evaluación continua- mediante una combinación de pruebas de evaluación parciales asociadas al Programa de Teoría de la misma y una serie de trabajos prácticos realizados y entregados por el alumno.

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.
- **Bloque 2 de contenidos teóricos.** Corresponde a los temas 3 y 4. Se desarrolla entre la 5ª y la 10ª semanas de curso, aproximadamente.
- **Bloque 3 de contenidos teóricos.** Corresponde al tema 5. Se desarrolla entre la 11ª y la 15ª semanas de curso, aproximadamente.
- **Ejercicios prácticos.** Se desarrollarán a lo largo de todo el curso, en paralelo a la teoría.

Esta planificación estimada podrá verse modificada por causas ajenas a la organización académica primeramente presentada. El profesor informará convenientemente a los alumnos de las nuevas 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?	CO	CE
1ª actividad de evaluación continua y entrega de trabajos				X												X	X	X
2ª actividad de evaluación continua										X						X	X	X
3ª actividad de evaluación continua															X	X	X	X

CONSIDERACIONES DE LA EVALUACIÓN EN LA CONVOCATORIA ORDINARIA:

El conocimiento de los contenidos y la adquisición de las competencias relativas 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 respuesta corta, desarrollo y/o tipo ejercicio. La información concreta sobre cada prueba se publica en el e-Campus de la asignatura con la debida antelación.

- 1ª actividad de evaluación continua. Corresponde a los temas 1 y 2 (20% de la nota final).
  - Pruebas escritas (100%)
- 2ª actividad de evaluación continua. Corresponde a los temas 3 y 4 (20% de la nota final).
  - Pruebas escritas (80%)
  - Ejecucion de prácticas (20%)
- 3ª actividad de evaluación continua. Corresponde al temas 5 (20% de la nota final).
  - Pruebas escritas (60%)
  - Ejecucion de prácticas (40%)

Los alumnos deberán realizar una serie de ejercicios prácticos que deberán ser entregados junto con un trabajo final. Estas actividades suponen un 35% de la nota final (Ejecucion de prácticas), ya que junto con los ejercicios, se deberá presentar una memoria sobre la realización de la actividad. 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.

Las competencias de tipo genérico (capacidad de análisis y síntesis; organización; planificación; toma de decisiones; trabajo en equipo; creatividad; razonamiento crítico; etc.) serán evaluadas mediante Técnicas de observación en cada una de las actividades realizadas a lo largo del curso (incluidas las tutorías). En global, estas competencias suponen un 5% de la nota final.

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 entrega de trabajos y prácticas, por lo que la calificación de esta primera entrega (llevada a cabo dentro del proceso de evaluación continua) es la definitiva para la convocatoria ordinaria.

Para superar la asignatura aplicando la evaluación continua sólo se permitirá un suspenso en cualquiera de las actividades propuestas (bien sea en las actividades de evaluación o en los ejercicios), siempre que ese suspenso no tenga una nota inferior a 4 puntos sobre 10 y que, evidentemente, la media global supere el 5.
Si la nota media no supera el 5, en el expediente aparecerá la nota media.
En caso de tener mas de una actividad suspensa y la media es superior a 5, en el expediente aparecerá una nota media de 4.
En caso de tener una actividad suspensa con una nota inferior a 4 y la media es superior a 5, en el expediente aparecerá una nota media de 4.

Los alumnos que no logren el aprobado mediante el sistema de evaluación continua deben superar de nuevo una prueba de evaluación correspondiente a la prueba de evaluación que tenían suspensa. Es decir, existirán 3 pruebas de evaluación que servirán para recuperar la nota de cada una de las pruebas suspensas. Cada una de estas pruebas tendrán un peso del 20%.

En cuanto al 35% correspondiente a la parte de actividades, será recuperable mediante un trabajo/proyecto que costará de varios tipos de ejercicios o problemáticas tratadas durante el desarrollo de la asignatura.

Se deberá obtener un mínimo de 5 puntos (teniendo en cuenta los porcentajes de puntuación antes citados para cada prueba de recuperación) para superar la asignatura. Siendo necesario aprobar ambas partes.

Esta planificación tiene un carácter meramente orientativo y podrá ser modificada a criterio del profesor, en función de circunstancias externas y de la evolución del grupo. El profesor informará convenientemente a los alumnos de dichas modificaciones. Los sistemas de evaluación descritos en esta guía docente son sensibles tanto a la evaluación de las competencias como de los contenidos de la asignatura. 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.

CONSIDERACIONES DE LA EVALUACIÓN EN LA CONVOCATORIA EXTRAORDINARIA:

El Programa de Teoría de la asignatura se evaluará mediante una prueba única y global sobre el contenido teórico.

En la convocatoria extraordinaria se habilitará una nueva opción para la entrega de los ejercicios y de la memoria de los mismos. Los alumnos que hubieran realizado la correspondiente entrega en la opción habilitada en convocatoria ordinaria pueden mantener su nota.

En la convocatoria extraordinaria no se aplicará el sistema de calificación Técnicas de observación ya que el carácter extraordinario (no presencial para ciertas actividades) de dicha convocatoria no lo permite.

La nota final, por lo tanto, tiene en cuenta el resultado de la prueba única sobre el Programa de Teoría (60%) y la calificación de Trabajos/proyectos (40%).

Esta planificación tiene un carácter meramente orientativo y podrá ser modificada a criterio del profesor, en función de circunstancias externas y de la evolución del grupo. El profesor informará convenientemente a los alumnos de dichas modificaciones. Los sistemas de evaluación descritos en esta guía docente son sensibles tanto a la evaluación de las competencias como de los contenidos de la asignatura. 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 (%)
Ejecución de prácticas	47%
Pruebas escritas	48%
Técnicas de observación	5%