DATOS GENERALES DE LA ASIGNATURA

ASIGNATURA: Defensa de Sistemas Informáticos
PLAN DE ESTUDIOS: Grado en Ingeniería Informática (PGR-INFORM)
GRUPO: 2425-T1
CENTRO: Escuela Politécnica Superior
CARÁCTER DE LA ASIGNATURA: Optativo
ECTS: 6,0
CURSO: 4º
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: CARMELO GONZÁLEZ GARCÍA
EMAIL: cgonzalezg@uemc.es
TELÉFONO: 983 00 10 00
HORARIO DE TUTORÍAS: Jueves a las 20:00 horas
CV DOCENTE:
Experto Docente del SEPE:

- IFCT0109 - Seguridad Informática (500 horas)
- IFCT120EXP - Ciberseguridad (100 horas)
- IFCT050PO - Gestión de la Seguridad Informática en la Empresa (100 horas)
- IFCT101PO - Planificación de la Seguridad Informática (100 horas)
- Planificación de la Seguridad Informática en la Empresa (80 horas)
- IFCT163PO - Inteligencia Artificial Aplicada a la Empresa (250 horas)
- IFCT127PO - Arquitectura Big Data (165 horas)
- IFCT107 - Responsable Experto de Data (240 horas)
- IFCT155PO - Introducción a la Inteligencia Artificial y los Algoritmos (180 horas)
- IFCT104 - Ciberseguridad para Microempresas (15 horas)
- IFCT083PO - Programación de Dispositivos Móviles (150 horas)

CV PROFESIONAL:
Auditor de Sistemas Informáticos:

- Gestión y configuración de la seguridad informática.
- Evaluación de riesgos y vulnerabilidades en sistemas y aplicaciones.
- Realización de auditorías de seguridad y cumplimiento normativo.
- Revisión y evaluación de políticas y procedimientos de TI.
- Monitoreo y seguimiento de acciones correctivas y mejoras en seguridad.

Analista de Sistemas Informáticos:

- Instalación de equipos informáticos en entornos Windows y Linux.
- Instalación de redes.
- Configuración y mantenimiento de Active Directory.
- Gestión y programación en bases de datos: SQL, MySQL, JSON.
- Administración y gestión de plataformas de virtualización VMWare.
- Programación de aplicaciones informáticas: Visual Basic, Java, Python, Gestión Middleware.

En las siguientes empresas:

- Bankinter
- Banco Popular
- Repsol
- UVa
- Microsoft
- Agrupo Sistemas
- Telefónica

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 administradores de sistemas. En muchas ocasiones, estos administradores deben enfrentarse a una auditoría de seguridad. Cada día es más importante lograr entender los informes resultantes de una auditoría de seguridad para solventar los problemas encontrados, aprovechando al máximo los recursos de una organización y sin desalinearse del negocio. Por ello, en esta asignatura se centrará en desarrollar los siguientes ejes:

- Seguridad Perimetral
- Puesta en producción segura
- Análisis Forense Informático

Es recomendable que el alumno haya cursado la asignatura Redes de Comunicaciones (o equivalente) y Fundamentos de Seguridad Informática y Criptografía (o equivalente), en la que se introducen los conceptos fundamentales para el desarrollo de esta asignatura. Haber cursado la asignatura de Sistemas Operativos Empresariales también es recomendable. Además, es conveniente un manejo avanzado de sistemas operativos y conocimientos básicos sobre aplicaciones de virtualización.

CONTENIDOS DE LA ASIGNATURA:

1. **Fortificación de sistemas** : Realiza medidas de seguridad de un sistema informático 1. Introducción a la fortificación de sistemas: Identifica técnicas para la protección y fortificación de Sistemas Operativos y Redes de Datos.
    1. Introducción a la fortificación de sistemas. : Identifica técnicas para la protección y fortificación de Sistemas Operativos y Redes de Datos
    2. Seguridad perimetral. : Establece medidas de protección que prevengan de ataques externos a la vez que identifica la actividad natural y esperada dentro de la propia red y filtra, protege y aísla actividad desconocida o fraudulenta. Casos prácticos.
2. **Despliegue Seguro de Aplicaciones** : Enfocado en el desarrollo y puesta enmarcha segura de software, con énfasis en aplicacionesweb y dispositivos móviles, y en la configuración segura de servidoresweb.
    1. Puesta en Producción Segura. : Desarrollo de un sistema de despliegue de software seguro en la capa de aplicación. El despliegue y análisis posteriorse realiza sobre aplicacionesweb y dispositivos móviles, así como en la configuración de servidoresweb. Casos de estudio prácticos.
3. **Forense Digital y Recuperación de Incidentes** : Este bloque se centra en el análisisforense de sistemas que han sufrido accesos no autorizados, y cómo garantizar la validez de las pruebasrecogidas para su posible uso en procesosjudiciales.
    1. Análisis Forense Informático : Análisis delsistema cuando, de forma previa, se ha accedido indebidamente. Se divide en una serie de etapas destinadas a asegurar las evidencias encontradas, de tal manera que se garantice su validez. Elresultado del análisis de la información puede ser prueba determinante en un proceso judicial. Casos de estudio prácticos

OBSERVACIONES CONTENIDO DE LA ASIGNATURA:

Se realizarán prácticassobre los diferentestemas de teoría. Los alumnos deberán elaborar memorias de prácticas

que documenten todaslas prácticasrealizadas 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 BÁSICAS:

- CB1. Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio 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
- CB2. Que los estudiantes sepan 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
- CB5. Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

COMPETENCIAS GENERALES:

- CG01. Capacidad de organización y planificación en el ámbito tecnológico
- CG02. Capacidad y habilidad para la toma de decisiones en el ámbito tecnológico

COMPETENCIAS ESPECÍFICAS:

- CI5. Conocimiento, administración y mantenimiento sistemas, servicios y aplicaciones informáticas.
- TI7. Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos
- CEN6. Capacidad para identificar posibles fallos de seguridad que se presenten o puedan presentar en un sistema y proponer soluciones para mitigar el riesgo.

RESULTADOS DE APRENDIZAJE:

El alumno será capaz de:

- Conocer cómo se lleva a cabo la fortificación de sistemas informáticos
- Entender los conceptos sobre seguridad perimetral
- Demostrar conocimientos sobre seguridad en la capa de aplicación

BIBLIOGRAFÍA Y RECURSOS DE REFERENCIA GENERALES

BIBLIOGRAFÍA BÁSICA:

- James F. Kurose y Keith W.Ross. (2010.): Redes de computadoras: un enfoque descendente.. Ra-Ma.. ISBN: 978-84-9964-644-2.

BIBLIOGRAFÍA COMPLEMENTARIA:

- White, Alan J.; Clark, Ben. (2017.): Blue TeamField Manual (BTFM) (RTFM).. CreateSpace Independent Publishing Platform.. ISBN: 978-1541016361.

WEBS DE REFERENCIA:

Web / Descripcion
VirusTotal(https://www.virustotal.com/gui/home/upload)

Analisis de malware en ficheros y URL
Pandora(https://alejandria.ddns.net/ciberseguridad/pandora.html) Encriptador y Desencriptador por el método César y Transposición realizado por el profesor Carmelo González.
Herramienta detección de Pegasus. (https://alejandria.ddns.net/ciberseguridad/pegasus.mp4) Se ve funcionar la herramienta de detención de Pegasus con la API de Virustotal. por el profesor Carmelo González
Blog de Criptografía y seguridad (http://criptografiayseguridad.blogspot.com/) Blog de Criptografía y seguridad del profesor Manuel J. Lucena López
Instituto Nacional de Ciberseguridad en España(https://www.incibe.es/) Instituto Nacional de Ciberseguridad en España
EuropeanUnionAgency for Cybersecurity(https://www.enisa.europa.eu/) Agencia de Ciberseguridad de la Unión Europea
CCN-CERT(https://www.ccn-cert.cni.es/) Centro Cripotológico Nacional de España

PLANIFICACIÓN DEL PROCESO DE ENSEÑANZA-APRENDIZAJE DE LA ASIGNATURA

METODOLOGÍAS:

MÉTODO DIDÁCTICO:

Esta asignatura cuenta con suficiente carga teórica como para utilizar el 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 tutorías individuales se desarrollarán en modalidad online en el horario especificado en la guía 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 y prácticos:** Corresponde al tema 1. Se desarrolla entre el comienzo de curso y la 5ª semana, aproximadamente.
- **Bloque 2 de contenidos teóricos y prácticos:** Corresponde al tema 2. Se desarrolla entre la 6ª y la 10ª semanas de curso, aproximadamente.
- **Bloque 3 de contenidos teóricos y prácticos:** Corresponde al tema 3. 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 y entrega de trabajos										X						X	X	X
3ª actividad de evaluación continua y entrega de trabajos															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:

1. **Primera actividad de evaluación continua:**
   - Ejecución del trabajo práctico: 40% de la nota final.
   - Prueba escrita: 40% de la nota final.
2. **Segunda actividad de evaluación continua:**
   - Ejecución del trabajo práctico: 40% de la nota final.
   - Prueba escrita: 40% de la nota final.
3. **Tercera actividad de evaluación continua:**
   - Ejecución del trabajo práctico: 40% de la nota final.
   - Prueba escrita: 40% de la nota final.

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.

Los alumnos deberán entregar una memoria de la ejecución de las prácticas al final de cada tema. 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. En global, estas competencias suponen un 20% de la nota final.

Para superar la asignatura es necesario que el alumno obtenga una calificación global (media) mínima de 5 puntos sobre 10. 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 más 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 tendrá el peso establecido anteriormente. En cuanto al 40% correspondiente a la parte de prácticas, será recuperable mediante un trabajo/proyecto que constará 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 teórico 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 por 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 escrita (50%) y la calificación de trabajos (50%).

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	40%
Pruebas escritas	40%
Técnicas de observación	20%