DATOS GENERALES DE LA ASIGNATURA

ASIGNATURA: Defensa de Sistemas Informáticos
PLAN DE ESTUDIOS: Grado en Ingeniería Informática (PGR-INFORM)
GRUPO: 2526-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: Viernes a las 13:00 horas

CV DOCENTE:

Docente especializado en informática, con una amplia experiencia en la enseñanza de disciplinas tecnológicas. Desde 2014 ha impartido más de 5.000 horas de formación presencial y online en áreas como ciberseguridad, inteligencia artificial, big data y sistemas informáticos, colaborando con instituciones publicas y plataformas de formación digital. Su sólida base científica, unida a su formación pedagógica, le permite abordar la enseñanza con un enfoque riguroso, práctico y adaptado a las necesidades del alumnado. Además, cuenta con formación en metodologías e-learning aplicadas a entornos como Moodle, lo que le capacita para diseñar experiencias de aprendizaje efectivas en formato digital. Su estilo docente se caracteriza por la claridad expositiva, el uso de recursos actualizados y la conexión constante entre teoría y práctica profesional. Como Físico aporta una visión analítica y estructurada al proceso de enseñanza, fomentando el pensamiento crítico y la comprensión profunda de los conceptos técnicos que conforman la base de las tecnologías emergentes.

CV PROFESIONAL:

Con una sólida trayectoria en el sector tecnológico y más de una década de experiencia profesional en entornos críticos. Ha trabajado como analista, desarrollador de software, gestor y coordinador de proyectos en sistemas informáticos y ciberseguridad, colaborando con entidades de alto nivel tanto a nivel financiero, energético, aeroespacial y de defensa. Su perfil técnico abarca desde la planificación y supervisión de infraestructuras tecnológicas hasta la administración de redes, plataformas de virtualización (VMware) y sistemas de seguridad informática. Está especializado en el análisis de riesgos, implementación de medidas de protección de datos y desarrollo de políticas de ciberseguridad. Además, posee experiencia en bases de datos (SQL, MongoDB), automatización y programación (Python, .NET, Java), así como en el tratamiento de imágenes geoespaciales. Como desarrollador de software, ha participado en el diseño y construcción de soluciones tecnológicas adaptadas a distintos entornos, integrando funcionalidades avanzadas y garantizando la calidad del código. Su enfoque combina rigor técnico, visión estratégica y capacidad para liderar equipos multidisciplinares en proyectos de transformación tecnológica, optimización de sistemas y mejora continua.

DATOS ESPECÍFICOS DE LA ASIGNATURA

DESCRIPTOR DE LA ASIGNATURA:

La asignatura *Defensa de Sistemas Informáticos* tiene como objetivo dotar al alumnado de los conocimientos, habilidades y criterios necesarios para proteger eficazmente entornos informáticos tanto personales como corporativos. En un contexto donde la seguridad informática es un factor estratégico, se abordarán de forma práctica y aplicada tres ejes fundamentales: la fortificación de sistemas operativos y redes, la seguridad en el despliegue de aplicaciones y el análisis forense digital. El estudiante aprenderá a identificar y mitigar vulnerabilidades, configurar infraestructuras seguras, y realizar análisis post-incidente con garantías jurídicas. El enfoque del curso es eminentemente técnico, con prácticas vinculadas a casos reales, orientadas a simular escenarios de ataque y defensa en sistemas TI. Se fomentará la comprensión de auditorías de seguridad, así como la capacidad para interpretar sus resultados y proponer medidas correctoras alineadas con los objetivos de negocio. Se recomienda haber cursado asignaturas como *Redes de Comunicaciones*, *Fundamentos de Seguridad Informática y Criptografía* y *Sistemas Operativos Empresariales*, así como poseer competencias previas en virtualización y administración de sistemas.

CONTENIDOS DE LA ASIGNATURA:

1. **Fortificación de sistemas**: En este bloque se abordan las técnicas y estrategias fundamentales para fortalecer la seguridad de sistemas operativos y redes. El alumnado aprenderá a identificar vulnerabilidades comunes y a aplicar configuraciones seguras que reduzcan la superficie de exposición de los sistemas frente a posibles amenazas.
    1. Fundamentos de fortificación de sistemas: Se introduce el concepto de fortificación o "hardening", abordando las medidas básicas para reducir vulnerabilidades en sistemas operativos. Se revisan configuraciones seguras, desactivación de servicios innecesarios, gestión de usuarios y políticas de contraseñas.
    2. Seguridad en redes y servicios de infraestructura: Se estudian técnicas para proteger servicios básicos de red (DNS, DHCP, FTP, SSH) y configurar entornos seguros en redes locales. Se incluye la segmentación de redes, control de acceso y principios de gestión segura de sistemas.
2. **Seguridad perimetral y despliegue seguro de aplicaciones**: Este bloque se centra en la protección del perímetro de red y en la implementación segura de servicios y aplicaciones. Se estudian mecanismos de control de tráfico, aislamiento de zonas críticas y buenas prácticas en la configuración de servidores, así como el despliegue seguro de aplicaciones web y móviles.
    1. Seguridad perimetral y control del tráfico: Se abordan mecanismos de defensa perimetral, como firewalls, IDS/IPS, configuración de routers y DMZ. El alumnado aprenderá a analizar tráfico de red, identificar comportamientos anómalos y establecer reglas de protección eficaces.
    2. Despliegue seguro de aplicaciones y servidores web: Estudio de las buenas prácticas en la puesta en producción de servicios web y móviles. Se abordarán aspectos como la configuración segura de servidores, la protección de datos en tránsito y la validación previa del entorno de ejecución.
3. **Análisis forense y respuesta a incidentes**: El último bloque introduce al análisis forense informático, orientado a la investigación de incidentes de seguridad. Se enseña cómo recolectar, preservar y analizar evidencias digitales de forma estructurada y legalmente válida, con el objetivo de detectar brechas, comprender su origen y documentarlas adecuadamente.
    1. Introducción al análisis forense digital: Estudio del proceso de análisis tras un incidente de seguridad. Se revisarán las fases de recolección, preservación y análisis de evidencias digitales, así como los principios legales asociados a su tratamiento.
    2. Monitorización y respuesta ante incidentes de seguridad: En este tema se abordarán los métodos de monitorización de sistemas y redes para la detección de comportamientos anómalos. El alumnado aprenderá a interpretar eventos de seguridad y a estructurar una respuesta técnica adecuada ante incidentes.

OBSERVACIONES CONTENIDO DE LA ASIGNATURA:

El contenido de la asignatura *Defensa de Sistemas Informáticos* se ha estructurado en tres bloques temáticos interrelacionados que permiten abordar la seguridad informática desde un enfoque integral y progresivo. Cada bloque combina teoría y práctica para facilitar la adquisición de competencias aplicables en entornos reales. A lo largo del curso, el alumnado desarrollará ejercicios y casos prácticos orientados a reforzar los conceptos clave de cada tema, aplicando herramientas profesionales y metodologías actuales. Se exigirá la elaboración de memorias técnicas que documenten todas las prácticas realizadas, algunas de las cuales deberán presentarse en clase. Estas

actividades fomentan la reflexión crítica, el trabajo autónomo y la capacidad de comunicación técnica. La asignatura requiere un nivel medio-avanzado en el manejo de sistemas operativos, redes y entornos de virtualización, siendo recomendable haber cursado asignaturas previas como *Redes de Comunicaciones*, *Fundamentos de Seguridad Informática* y *Sistemas Operativos Empresariales*.

RECURSOS DE APRENDIZAJE:

Las clases se desarrollarán combinando contenidos teóricos y prácticos en entornos presenciales y virtuales, utilizando para ello recursos específicos tanto en aula como en laboratorio. El objetivo es facilitar el aprendizaje aplicado y simulado de los principales conceptos de seguridad informática.

El alumnado dispondrá de los siguientes recursos:

- **Aula de informática y laboratorio de redes**, equipados con:
  - **Routers, switches gestionables y servidores en rack**, configurables para prácticas reales de segmentación de red, VLAN, firewalls y seguridad perimetral.
  - Estaciones de trabajo con herramientas de virtualización (VMware, VirtualBox) para la simulación de entornos atacados o comprometidos.
- **Plataforma Moodle UEMC**, para la gestión de contenidos, entrega de trabajos, comunicación docente y foros.
- **Proyector, pizarra digital y material audiovisual**, para clases magistrales y resolución interactiva de ejercicios.
- **Herramientas y utilidades técnicas**:
  - VirusTotal, sandbox de malware, herramientas de análisis forense.
  - Scripts desarrollados por el docente (como encriptadores y detectores de amenazas).
- **Bibliografía técnica y enlaces especializados**:
  - INCIBE, ENISA, CCN-CERT.
  - Blogs de ciberseguridad y criptografía, incluidos recursos propios del profesorado.

Estos recursos permiten trabajar en escenarios realistas de defensa de sistemas, análisis forense y seguridad perimetral, favoreciendo el aprendizaje activo, técnico y contextualizado.

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:

- Carmelo González García (2025): Defensa de Sistemas Informáticos. UEMC. ISBN: 978-84-126114-6-5

BIBLIOGRAFÍA COMPLEMENTARIA:

- White, Alan J.; Clark, Ben. (2017): Blue TeamField Manual (BTFM) (RTFM).. CreateSpace Independent. Publishing Platform.. ISBN: 98-1541016361

WEBS DE REFERENCIA:

Web / Descripcion
VirusTotal(https://www.virustotal.com/gui/home/upload) Análisis de malware en ficheros y URL
Codex(https://alejandria.ddns.net/codex/) Encriptador y Desencriptador por el método César y Transposición realizado por Javier Alonso y Carmelo González.
INCIBE(https://www.incibe.es/) Instituto Nacional de Ciberseguridad en España.
ENISA(https://www.enisa.europa.eu/) Agencia oficial de la Unión Europea que tiene como misión principal fortalecer la ciberseguridad en Europa
CCN-CERT(https://www.ccn-cert.cni.es/es/) Centro Criptológico Nacional de España.

PLANIFICACIÓN DEL PROCESO DE ENSEÑANZA-APRENDIZAJE DE LA ASIGNATURA

METODOLOGÍAS:

MÉTODO DIDÁCTICO:

El **método didáctico** se emplea principalmente en las sesiones expositivas, donde el docente presenta los contenidos teóricos mediante explicaciones estructuradas, apoyadas en ejemplos y resolución de ejercicios guiados.

MÉTODO DIALÉCTICO:

El **método dialéctico** se utiliza en la presentación, análisis y corrección de trabajos, promoviendo la participación activa del alumnado mediante el diálogo, la argumentación y el intercambio de ideas en un entorno crítico.

MÉTODO HEURÍSTICO:

El **método heurístico** se aplica en las actividades prácticas y proyectos, fomentando el aprendizaje autónomo, la investigación personal y la resolución de problemas reales, lo que permite al estudiante construir su propio conocimiento a partir de la experiencia.

CONSIDERACIONES DE LA PLANIFICACIÓN:

La asignatura se organiza en torno a diversas actividades formativas planificadas a lo largo del curso. Las **clases presenciales** se desarrollarán semanalmente y estarán orientadas, principalmente, mediante el **método didáctico o expositivo**, facilitando la comprensión de los contenidos teóricos a través de explicaciones estructuradas y ejemplos ilustrativos. El alumnado deberá realizar y entregar **trabajos prácticos** sobre temáticas específicas relacionadas con la asignatura, algunos de los cuales se presentarán en clase para su exposición y defensa, promoviendo así la participación activa y la argumentación técnica. Las **tutorías individuales** se llevarán a cabo en modalidad online, según el horario establecido en esta guía docente, con el fin de atender de forma personalizada las dudas o dificultades que puedan surgir. La **evaluación** de la asignatura se realizará mediante un sistema de evaluación continua, que combinará pruebas escritas parciales asociadas al programa teórico con la entrega de trabajos prácticos, garantizando así una valoración integral del aprendizaje adquirido.

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:

La asignatura se organiza mediante un sistema de evaluación continua, estructurado en tres bloques evaluables a lo largo del semestre. Cada bloque incluirá:

- **Una prueba escrita** (40% de la nota del bloque), compuesta por una parte teórica y una parte práctica, orientadas respectivamente a la comprensión conceptual y a la aplicación técnica de los contenidos. Para que esta prueba pueda computar en la media del bloque, será necesario obtener una calificación mínima de **4 puntos en ambas partes (teórica y práctica)**.
- **Un trabajo práctico** (40% de la nota del bloque), en el que el estudiante deberá desarrollar tareas aplicadas relacionadas con los contenidos trabajados en clase.
- **Una evaluación por observación continua** (20% de la nota global), basada en la asistencia y puntualidad, el respeto al profesorado, compañeros y recursos del aula, la participación activa, la actitud colaborativa y la capacidad de análisis y razonamiento crítico.

La calificación final de la asignatura se obtendrá como la media aritmética de las calificaciones obtenidas en los tres bloques evaluables, cada uno de los cuales representa un **33,3%** de la nota final, tanto en la evaluación continua como en la convocatoria ordinaria.

Para superar la asignatura, el estudiante deberá obtener una calificación mínima de **5 puntos en cada bloque**, tanto en la prueba escrita como en el trabajo práctico. Se permite suspender una de las dos partes (prueba o trabajo) siempre que la calificación no sea inferior a 4 puntos y la media final del bloque sea igual o superior a 5 puntos. En caso contrario, deberá recuperar la parte o partes suspensas en la convocatoria ordinaria.

Para aprobar la asignatura en la **convocatoria ordinaria**, todas las partes recuperadas deben obtener una calificación mínima de 5. En caso contrario, el estudiante pasará a la convocatoria **extraordinaria**. Se recuerda al alumnado que las pruebas teóricas y prácticas tienen una duración máxima de **dos horas (en su conjunto)**, por lo que es fundamental gestionar adecuadamente el tiempo, especialmente si se deben recuperar varias partes en la misma convocatoria. Por todo ello, se recomienda encarecidamente superar la asignatura mediante la evaluación continua.

La **Matrícula de Honor** únicamente podrá obtenerse a través del sistema de evaluación continua, y estará reservada a quienes logren una calificación final de **10 (sobresaliente)** en este régimen. No será posible obtenerla mediante pruebas de recuperación, convocatorias ordinarias o extraordinarias, ni mediante procedimientos de subida de nota.

CONSIDERACIONES DE LA EVALUACIÓN EN LA CONVOCATORIA EXTRAORDINARIA:

En la **convocatoria extraordinaria**, el estudiante deberá realizar una **prueba única y global** que evalúe de forma completa los contenidos teóricos de la asignatura. Esta prueba escrita representará el **50% de la calificación final**.

El **otro 50%** corresponderá a la **entrega de los trabajos prácticos** asociados a los bloques temáticos. Para ello, se habilitará un nuevo plazo de entrega específico.

En esta convocatoria no se aplicarán técnicas de observación continua, dado el carácter no presencial o excepcional de algunas de las actividades. Por tanto, la calificación final se obtendrá únicamente a partir de los resultados de la **prueba teórica (50%)** y la **evaluación de trabajos prácticos (50%)**.

Para superar la asignatura será necesario obtener una **calificación mínima de 5 puntos sobre 10**, habiendo alcanzado al menos una nota de **5 en cada una de las dos partes** (prueba escrita y trabajos prácticos), conforme a los criterios establecidos.

SISTEMAS DE EVALUACIÓN:

SISTEMA DE EVALUACIÓN	PORCENTAJE (%)
Ejecución de prácticas	40%
Pruebas escritas	40%
Técnicas de observación	20%