CENTRO UNIVERSITARIO DE TECNOLOGÍA Y ARTE DIGITAL

PLANIFICACIÓN DE LA DOCENCIA UNIVERSITARIA

GUÍA DOCENTE

Análisis Forense

1. DATOS DE IDENTIFICACIÓN DE LA ASIGNATURA.

Título:	Grado en Ingeniería del Software
Facultad:	Centro Universitario de Tecnología y Arte Digital (U-TAD)
Materia:	Ciberseguridad
Denominación de la asignatura:	Análisis Forense
Curso:	3
Cuatrimestre:	2
Carácter:	Obligatoria de mención
Créditos ECTS:	6
Modalidad/es de enseñanza:	Híbrido Presencial
Idioma:	Castellano
Profesor/a:	Roberto López Santoyo
E-mail:	roberto.santoyo@u-tad.com
Teléfono:	

2. DESCRIPCIÓN DE LA ASIGNATURA

2.1 Descripción de la materia

Esta materia se dedica al estudio de la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras.

2.2 Descripción de la asignatura

Esta asignatura pretender dar unos conocimientos y capacidades de análisis forense y respuesta ante incidentes. Para ello se va a ver la forma en la que se realiza la adquisición de evidencia y clonado de discos. A continuación, se verá la forma en la que analizar los sistemas operativos Windows y Linux. También se ahondará en los rastros forense en las redes, además del análisis de malware. Por último, se verán los procedimientos de respuesta ante incidentes.

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

3.1. COMPETENCIAS (Genéricas, específicas y transversales)

Competencias Básicas y Generales
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. CB3: Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética. CB4: Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. CB5: Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía CG1 - Capacidad para entender, planificar y resolver problemas a través del desarrollo de soluciones informáticas. CG2 - Desarrollo de soluciones informáticas respetuosas con el medio ambiente, los deberes sociales y los recursos naturales, además de cumplir con la legislación y la ética CG3 - Conocimiento de los fundamentos científicos aplicables a la resolución de problemas informáticos CG4 - Capacidad para simplificar y optimizar los sistemas informáticos atendiendo a la comprensión de su complejidad CG9 - Capacidad para aprender, modificar y producir nuevas tecnologías informáticas CG10 - Uso de técnicas creativas para la realización de proyectos informáticos CG11 - Capacidad de buscar, analizar y gestionar la información para poder extraer conocimiento de la misma
Competencias Específicas
CE10 - Capacidad para entnder un incident de seguridad y ser capaces de trazar un plan de acción para analizar y remediar
Competencias Transversales
CT1 - Conocimiento de la definición, el alcance y la puesta en práctica de los fundamentos de las metodologías de gestión de proyectos de desarrollo tecnológico CT2 - Conocimiento de los principales agentes del sector y del ciclo de vida completo de un proyecto de desarrollo y comercialización de contenidos digitales CT4 - Capacidad de actualización del conocimiento adquirido en el manejo de herramientas y tecnologías digitales en función del estado actual del sector y de las tecnologías empleadas CT5 - Desarrollo de las habilidades necesarias para el emprendimiento digital.

4. CONTENIDOS

4.1. Temario de la asignatura

1. **Tema 1. Adquisición de Evidencias**
    - 1.1. Adquisición
    - 1.2. Discos Duros
    - 1.3. Sistemas de Ficheros
    - 1.4. Adquisición
    - 1.5. Técnicas Anti Forense
2. **Tema 2. Windows**
    - 2.1. Información Volatil
    - 2.2. Adquisición de Memoria
    - 2.3. Identificación de Información no Volatil
    - 2.4. Registro de Windows
    - 2.5. Caché, Cookies e Historial
    - 2.6. Analisis de Ficheros Windows
    - 2.7. Metadatos
    - 2.8. Eventos de Windows
    - 2.9. Analisis de Memoria
3. **Tema 3. Linux**
    - 3.1. Comandos
    - 3.2. Logs
    - 3.3. Información Volatil
4. **Tema 4. Redes**
    - 4.1. Trafico de Red
    - 4.2. Analisis de Logs
5. **Tema 5. Malware**
    - 5.1. Analisis Manual
    - 5.2. Analisis Sandbox
6. **Tema 6. Respuesta ante Incidentes**
    - 6.1. Prcedimientos
    - 6.2. Herramientas

4.2. Desarrollo temporal

UNIDADES DIDACTICAS/TEMAS	PERIODO TEMPORAL
Tema 1: Adquisición de Evidencias	Semana 1, 2 y 3
Tema 2: Windows	Semana 4, 5, 6 y 7
Parcial 1	Semana 8
Tema 3: Linux	Semana 9
Tema 4: Redes	Semana 10 y 11
Tema 5: Malware	Semana 11 y 12
Tema 6: Respuesta ante Incidentes	Semanas 13
Parcial 2	Semana 14

5. ACTIVIDADES FORMATIVAS Y MODALIDADES DE ENSEÑANZAS

5.1. Modalidades de enseñanza

La asignatura se desarrollará a través de los siguientes métodos y técnicas generales, que se aplicarán diferencialmente según las características propias de la asignatura:

- **Método expositivo/Lección magistral:** el profesor desarrollará, mediante clases magistrales y dinámicas los contenidos recogidos en el temario.
- **Estudio de casos:** análisis de casos reales relacionados con la asignatura.
- **Resolución de ejercicios y problemas:** los estudiantes desarrollarán las soluciones adecuadas aplicando procedimientos de transformación de la información disponible y la interpretación de los resultados.
- **Aprendizaje basado en problemas:** utilización de problemas como punto de partida para la adquisición de conocimientos nuevos.
- **Aprendizaje orientado a proyectos:** se pide a los alumnos que, en pequeños grupos, planifiquen, creen y evalúen un proyecto que responda a las necesidades planteadas en una determinada situación.
- **Aprendizaje cooperativo:** Los estudiantes trabajan en grupo para realizar las tareas de manera colectiva.

5.2. Actividades formativas

Actividad Formativa	Horas	Presencialidad
AF1 Clases teóricas / Expositivas	30	100%
AF2 Clases Prácticas	24	100%
AF3 Tutorías	6	50%
AF4 Estudio independiente y trabajo autónomo del alumno	57,5	0%
AF5 Elaboración de trabajos (en grupo o individuales)	28,5	0%
AF6: Actividades de Evaluación	4	100%

6. SISTEMA DE EVALUACIÓN

ACTIVIDAD DE EVALUACIÓN	VALORACIÓN MÍNIMA RESPECTO A LA CALIFICACIÓN FINAL (%)	VALORACIÓN MÁXIMA RESPECTO A LA CALIFICACIÓN FINAL (%)
SE1 Evaluación de la participación en clase, en prácticas o en proyectos de la asignatura	10%	30%
SE2 Evaluación de trabajos, proyectos, informes, memorias	40%	80%
SE3 Exámenes intermedios o final (no continua)	10%	60%

6.1. Criterios de calificación

CRITERIOS DE EVALUACIÓN CONTINUA

ACTIVIDAD DE EVALUACIÓN	CRITERIO DE EVALUACIÓN	PESO SOBRE LA CALIFICACIÓN FINAL (%)
SE1 - Prácticas Parciales	Participación adecuada en el desarrollo de la práctica, compromiso y entrega en tiempo y forma. Entrega y demostración del resultado.	45% (Obligatoria aprobar esta parte por separado)
SE2 – Examenes Parciales	Evaluación del examen práctico realizado online	45% (Obligatoria aprobar esta parte por separado)
SE3 - Comportamiento, actitud y asistencia a clase	Evaluación por parte del profesor	10%

La nota final de la asignatura se calculará considerando las notas de las actividades SE1, SE2 y SE3 aplicándole los pesos correspondientes (que se han fijado dentro de los márgenes indicados en la tabla anterior). Por tanto, la regla a aplicar para calcular la nota final será:

Nota_Final = 45%*SE1 + 45%*SE2 + 10%*SE3

CRITERIOS DE EVALUACIÓN FINAL

ACTIVIDAD DE EVALUACIÓN	CRITERIO DE EVALUACIÓN	PESO SOBRE LA CALIFICACIÓN FINAL (%)
SE1 - Prácticas Parciales	Participación adecuada en el desarrollo de la práctica, compromiso y entrega en tiempo y forma. Entrega y demostración del resultado.	45% (Obligatoria aprobar esta parte por separado)
SE2 – Examen final	Evaluación del examen práctico realizado online	45% (Obligatoria aprobar esta parte por separado)
SE3 - Comportamiento, actitud y asistencia a clase	Evaluación por parte del profesor	10%

La nota final de la asignatura se calculará considerando las notas de las actividades SE1, SE2 y SE3 aplicándole los pesos correspondientes (que se han fijado dentro de los márgenes indicados en la tabla anterior). Por tanto, la regla a aplicar para calcular la nota final será:

Nota_Final = 45%*SE1 + 45%*SE2 + 10%*SE3

Condiciones Generales de Evaluación

Evaluación Continua

CONSIDERACIONES A TENER EN CUENTA:

- Para aprobar en la convocatoria ordinaria el alumno deberá tener una nota igual o superior a 5,00 en la media de todas las calificaciones, es decir, tiene que haber aprobado los dos examenes parciales y las prácticas.
- Para que pueda realizarse la media deberá tener al menos un 5,00 en cada una de las practicas y un 5,00 en los examenes parciales.
- Así mismo, será necesario haber realizado las entregas solictadas durante el curso en la fecha establecida por el profesor. En caso de que una entrga se realice fuera de plazo la nota tendrá un 15% de penalización, es decir, la nota máxima de dicha entrega podrá ser un 8,5.
- En el caso de que solo se apruebe uno de los dos parciales, en el examen final solo se haría la parte correspondiente al examen suspenso.

Evaluación Final

CONSIDERACIONES A TENER EN CUENTA:

- Para aprobar en la convocatoria ordinaria el alumno deberá tener una nota igual o superior a 5,00 en la media de todas las calificaciones.
- Para que pueda realizarse la media deberá tener al menos un 5,00 en cada una de las practicas y un 5,00 en el Examen Final.
- Así mismo, será necesario haber realizado las entregas solictadas durante el curso en la fecha establecida por el profesor. En caso de que una entrga se realice fuera de plazo la nota tendrá un 15% de penalización, es decir, la nota máxima de dicha entrega podrá ser un 8,5.

Los alumos que no consigan superar la evaluación ordinaria deberán realizar una evaluación extraoridnaria en los términos establecidos por el profesor.

Evaluación Extraordinaria

Los alumos que hayan suspendido alguna de las partes o tengan pendiente alguna entrega podrán optar a una evaluación extraordinaria.

CONSIDERACIONES A TENER EN CUENTA:

- Para los alumnos con la materia suspensa pero con todas las prácticas aprobadas: solo tendrá que realizarse el examen final.
- Para los alumnos con la materia suspensa por falta de alguna entrega de prácticas, el profesor establecerá la fecha de las nuevas entregas.
- Para los alumnos con al materia suspensa y falta de alguna entrega de prácticas, tendrá que realizar el examen final y la entrega de prácticas correspondiente.

7. BIBLIOGRAFÍA / WEBGRAFÍA

Bibliografía Básica:

- Incident Response & Computer Forensics. Jason T. Luttgens, Matthew Pepe and Kevin Mandia.
- Windows Forensic Analysis Toolkit. Harlan Carvey.
- Windows Registry Forensics. Windows Registry Forensics.
- The Art of Memory Forensics. Michael Hale Ligh, Jamie Levy, AAron Walters, Andrew Case.
- Practical Forensic Imaging: Securing Digital Evidence with Linux Tools. Bruce Nikkel.
- Linux Forensics. Philip Polstra.
- Hands-On Network Forensics. Nipun Jaswal.
    - Practica Malware Analysis. Michael Sikorski, Andrew Honig

Bibliografía Recomendada:

8. MATERIAL, SOFTWARE Y HERRAMIENTAS NECESARIAS

Materiales necesarios del alumno:

- Ordenador personal con Windows, Linux o OSX
- VirtualBox y VirtualBox Extension Pack