



| Guía docente | | | | |
|-----------------------|--|--------------------|---------------------------------|----------|
| Datos Identificativos | | | | 2020/21 |
| Asignatura (*) | Análisis Forense de Equipos | Código | 614530012 | |
| Titulación | Máster Universitario en Ciberseguridade | | | |
| Descriptorios | | | | |
| Ciclo | Periodo | Curso | Tipo | Créditos |
| Máster Oficial | 2º cuatrimestre | Primero | Optativa | 3 |
| Idioma | CastellanoGallego | | | |
| Modalidad docente | Presencial | | | |
| Prerrequisitos | | | | |
| Departamento | Ciencias da Computación e Tecnoloxías da InformaciónComputación | | | |
| Coordinador/a | | Correo electrónico | | |
| Profesorado | Vázquez Naya, José Manuel | Correo electrónico | jose.manuel.vazquez.naya@udc.es | |
| Web | faitic.uvigo.es | | | |
| Descripción general | <p>El análisis forense de equipos consiste en la aplicación de técnicas científicas y analíticas para identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.</p> <p>La materia "Análisis Forense de Equipos" tiene una fuerte componente práctica. Se comenzará con una introducción a este campo, explicando conceptos clave. A continuación, se estudiarán fundamentos y metodologías de análisis forense desde un punto de vista genérico y aplicable a nuevos casos, pero también se estudiarán ejemplos concretos basados en casos reales.</p> <p>En las prácticas de laboratorio el/la alumno/a aprenderá a manejar diferentes herramientas de análisis forense y realizará prácticas simulando problemas reales.</p> | | | |



Plan de contingencia

Plan de contingencia A: confinamiento total o parcial de estudiantes y/o profesores

1. Modificaciones en los contenidos

- No se realizarán cambios

2. Metodologías

*Metodologías docentes que se mantienen

- Se mantienen las metodologías docentes, con la excepción de que, en lugar de realizarse de manera presencial en el aula, se realizarán con la ayuda de herramientas TIC, como se explica a continuación.

*Metodologías docentes que se modifican

- Sesión magistral: se impartirá a través de videoconferencia.
- Prácticas de laboratorio: Tanto la docencia, como la defensa de las prácticas, cuando proceda, se realizarán a través de videoconferencia.
- Prueba objetiva: se realizará a través de Moodle (faitic), en combinación con videoconferencia.
- Examen de prácticas (segunda oportunidad y convocatoria extraordinaria): se realizará a través de videoconferencia.

3. Mecanismos de atención personalizada al alumnado

- Correo electrónico: Diariamente. De uso para hacer consultas, y solicitar encuentros virtuales para resolver dudas.
- Moodle (faitic): Diariamente. Según la necesidad del alumnado.
- Teams/Campusremoto: Durante las horas programadas de teoría y práctica. También bajo demanda, para resolución de dudas.

4. Modificaciones en la evaluación

- No se realizarán cambios

*Observaciones de evaluación:

Se mantienen las mismas que figuran en la guía docente. A mayores:

- En caso de que no puedan realizarse presencialmente, se llevarán a cabo según lo indicado en el apartado de "Metodologías".
- Si por algún motivo justificado el alumno no pudiera realizar el examen final (prueba objetiva) en el momento establecido, el examen pasará a realizarse la mayor brevedad posible, pasando a ser una prueba oral por videoconferencia.

5. Modificaciones de la bibliografía o webgrafía

Ninguna.

Plan de contingencia B: número de estudiantes exceda el aforo del aula

1. Modificaciones en los contenidos

- No se realizarán cambios

2. Metodologías

*Metodologías docentes que se mantienen

- Se mantienen las metodologías docentes, con la excepción de que además de realizarse de manera presencial, se realizarán con la ayuda de herramientas TIC, como se explica a continuación

*Metodologías docentes que se modifican

- Sesión magistral: se establecerán dos grupos, que asistirán presencialmente semanas alternas. Se empleará videoconferencia, para que puedan acceder a las sesiones los alumnos del grupo al que no le toca asistir presencialmente.
- Prácticas de laboratorio: se establecerán dos grupos, que asistirán presencialmente semanas alternas. Se empleará videoconferencia, para que puedan acceder a las sesiones los alumnos del grupo al que no le toca asistir presencialmente. Se establecerán turnos para la defensa de las prácticas, cuando proceda.
- Prueba objetiva: se buscará un aula alternativa, con aforo suficiente.
- Examen de prácticas (segunda oportunidad y convocatoria extraordinaria): se establecerán turnos para su realización.

3. Mecanismos de atención personalizada al alumnado

- Correo electrónico: Diariamente. De uso para hacer consultas, y solicitar encuentros virtuales para resolver dudas.
- Moodle (faiic): Diariamente. Según la necesidad del alumnado.
- Teams/Campusremoto: Durante las horas programadas de teoría y práctica. También bajo demanda, para resolución de dudas.

4. Modificaciones en la evaluación

- No se realizarán cambios

*Observaciones de evaluación:

Se mantienen las mismas que figuran en la guía docente. A mayores:

- En caso de que no puedan realizarse presencialmente, se llevarán a cabo según lo indicado en el apartado de "Metodologías".
- Si por algún motivo justificado el alumno no pudiera realizar el examen final (prueba objetiva) en el momento establecido, el examen pasará a realizarse la mayor brevedad posible, pasando a ser una prueba oral por videoconferencia.

5. Modificaciones de la bibliografía o webgrafía

Ninguna.



| Competencias / Resultados del título | |
|--------------------------------------|--|
| Código | Competencias / Resultados del título |
| A6 | CE6 - Desarrollar y aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad |
| B1 | CB1 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación |
| B2 | CB2 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio |
| B3 | CB3 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios |
| B7 | CG2 - Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones |
| C4 | CT4 - Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad |

| Resultados de aprendizaje | | | |
|---|--------------------------------------|------------|-----|
| Resultados de aprendizaje | Competencias / Resultados del título | | |
| Conocimiento de las metodologías adecuadas para la realización de trabajos forenses con validez legal | AP6 | BP1 | CP4 |
| Capacidad para la realización de análisis forense de los diferentes elementos que forman un sistema de información, en múltiples plataformas y sistemas operativos | AP6 | BP2 BP7 | CP4 |
| Capacidad para generar informes como resultado del análisis forense claros, concisos e inteligibles tanto por expertos como por personas ajenas al ámbito de la seguridad informática | AP6 | BP3 BP7 | CP4 |

| Contenidos | |
|--|--|
| Tema | Subtema |
| 1. Introducción al análisis forense | Introducción Fundamentos Normativa Clonado |
| 2. Análisis Forense en Windows | Artefactos Memoria Herramientas Aspectos avanzados de análisis forense en Windows |
| 3. Análisis Forense en Mac OS | Artefactos Memoria Herramientas Aspectos avanzados de análisis forense en Mac OS |
| 4. Análisis Forense en dispositivos móviles: Android | Artefactos Herramientas Aspectos avanzados de análisis forense en Android |
| 5. Análisis Forense en dispositivos móviles: iOS | Artefactos Herramientas Aspectos avanzados de análisis forense en iOS |

| Planificación | | | | |
|--------------------------|---------------------------|---|------------------------|---------------|
| Metodologías / pruebas | Competencias / Resultados | Horas lectivas (presenciales y virtuales) | Horas trabajo autónomo | Horas totales |
| Sesión magistral | A6 C4 | 11 | 22 | 33 |
| Prácticas de laboratorio | A6 B1 B2 B3 B7 C4 | 10 | 20 | 30 |



| | | | | |
|------------------------|-------------------|----|---|----|
| Prueba objetiva | A6 B1 B2 B3 B7 C4 | 2 | 0 | 2 |
| Atención personalizada | | 10 | 0 | 10 |

(*) Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos

| Metodologías | |
|--------------------------|---|
| Metodologías | Descripción |
| Sesión magistral | Clases expositivas de presentación de los conocimientos teóricos de cada uno de los temas. Se fomentará la participación del alumnado. |
| Prácticas de laboratorio | Sesiones prácticas en ordenador, en las que se deben resolver una serie de boletines de ejercicios prácticos propuestos por el profesor. Los ejercicios buscan consolidar los conocimientos presentados en las sesiones magistrales y también fomentar el aprendizaje autónomo del alumno. Una vez completado el boletín de ejercicios, el profesor evaluará el trabajo realizado por el alumno mediante una sesión de trabajo en ordenador. Los boletines de ejercicios se publicarán a través de la plataforma de formación del máster. Se impondrá una fecha máxima de defensa para cada boletín, con el objetivo de fomentar el estudio continuo. |
| Prueba objetiva | Prueba escrita mediante la que se valorarán los conocimientos y capacidades adquiridos por el alumno. |

| Atención personalizada | |
|--------------------------|----------------------|
| Metodologías | Descripción |
| Prácticas de laboratorio | Resolución de dudas. |

| Evaluación | | | |
|--------------------------|---------------------------|--|--------------|
| Metodologías | Competencias / Resultados | Descripción | Calificación |
| Prácticas de laboratorio | A6 B1 B2 B3 B7 C4 | Se propondrán varias prácticas a lo largo del curso, relacionadas con el análisis forense de equipos, en las que el/la alumno/a trabajará con distintas herramientas y deberá realizar procesos de clonado, de recuperación de información, redacción de informes, etc. Las prácticas tendrán carácter individual. En el enunciado de cada práctica se especificará la fecha límite para la realización de la misma, así como la metodología de evaluación, que puede ser a través de la entrega de una memoria, de la realización de una prueba en ordenador, o mediante ambas. | 60 |
| Prueba objetiva | A6 B1 B2 B3 B7 C4 | Examen final, tipo test, mediante el que se valorarán los conocimientos y capacidades adquiridos por el alumno, tanto en las sesiones de teoría como en las sesiones prácticas. | 40 |

| Observaciones evaluación |
|--------------------------|
|--------------------------|



1. PRIMERA OPORTUNIDAD

A lo largo del curso se realizarán una serie de "prácticas de laboratorio", con las características y peso indicados en el cuadro anterior.

Al finalizar el curso se realizará una "prueba objetiva", con las características y peso indicados en el cuadro anterior.

2. SEGUNDA OPORTUNIDAD

Se realizará una "prueba objetiva", con las características y peso indicados en el cuadro anterior.

Con respecto las "prácticas de laboratorio", el/la alumno/a podrá conservar la nota obtenida en la primera oportunidad. Caso de no haber presentado

las prácticas en la primera oportunidad, deberá someterse a un examen de prácticas.

3. CONVOCATORIA EXTRAORDINARIA

Se realizará una "prueba objetiva", con las características y peso indicados en el cuadro anterior.

Con respecto las "prácticas de laboratorio", el/la alumno/a podrá conservar la nota obtenida en en la primera oportunidad (si fuera el caso). Caso de no

haber presentado las prácticas en la primera oportunidad, deberá someterse la un examen de prácticas.

4. PLAGIO

Sí se detectara plagio en cualquiera de las pruebas de evaluación, la calificación final de la materia será de "suspense (0)", hecho que se comunicará a la coordinación del título para adoptar las medidas oportunas.

5. CONDICIÓN DE "NO PRESENTADO"

Se considerarán como "no presentados" a los alumnos que no realicen la prueba objetiva.

Fuentes de información

| | |
|-----------------------|--|
| Básica | Toda a documentación necesaria estará disponible a través de Moodle (fatic). |
| Complementaria | |

Recomendaciones

Asignaturas que se recomienda haber cursado previamente

Asignaturas que se recomienda cursar simultáneamente

Asignaturas que continúan el temario

Otros comentarios

(*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías