GUIA DOCENTE DEL CURSO
INFORMÁTICA FORENSE

AREA: DIGITAL BUSINESS
AUTOR: SPAIN BUSINESS SCHOOL

CÓDIGO: GD-731

IDENTIFICACIÓN DE LA ASIGNATURA

- Denominación: Informática forense
- Código: 731
- Curso: 1
- Cuatrimestre: 1
- Carácter: Optativa
- Nº de créditos (horas): 10 ECTS (250 horas)
- Idioma en que se imparte: Español

REQUISITOS PREVIOS

No tiene requisitos previos, pero conocimientos sobre las siguientes temáticas son recomendables:

- Fundamentos de Sistemas Operativos.
- Estructura de Sistemas Operativos.
- Garantía y Seguridad de la Información.

PROFESORES Y CONFERENCIANTES

Francisco Sanz Moya

- Categoría: Master
- Área funcional: Ciberseguridad
- Mail: francisco.sanz@sbs.edu.es
- Tutorías: pedir cita previa

David Gaona

- Categoría: Máster
- Área funcional: Ciberseguridad
- Mail: david.gaona@sbs.edu.es
- Tutorías: pedir cita previa

DESCRIPCIÓN Y OBJETIVOS

La ubicuidad de medios informáticos, combinada con el crecimiento imparable de Internet y las redes durante los últimos años, abre un escenario de oportunidades para actos ilícitos (fraude, espionaje empresarial, sabotaje, robo de datos, intrusiones no autorizadas en redes y sistemas y un largo etcétera) a los que es preciso hacer frente entendiendo las mismas tecnologías de las que se sirven los delincuentes informáticos, con el objeto de salirles al encuentro en el mismo campo de batalla. Parte vital en el combate contra el delito es una investigación de medios digitales basada en métodos profesionales y buenas prácticas al efecto de que los elementos de evidencia obtenidos mediante la misma puedan ser puestos a disposición de los tribunales.

Se debe hacer con las suficientes garantías en lo referente tanto al mantenimiento de la cadena de custodia y al cumplimiento de aspectos esenciales para el orden legal del estado de derecho, como al respeto a las leyes sobre privacidad y protección de datos y otras normativas de relevancia similar.

La Informática Forense es la disciplina que se encarga de la adquisición, el análisis y la valoración de elementos de evidencia digital hallados en ordenadores, soportes de datos e infraestructuras de red, y que pudieran aportar luz en el esclarecimiento de actividades ilegales perpetradas en relación con instalaciones de proceso de datos, independientemente de que dichas instalaciones sean el objetivo de la actividad delictiva o medios utilizados para cometerla.

La informática forense sirve para garantizar la efectividad de las políticas de seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de esa información; para ello se deberán investigar los sistemas informáticos con el fin de detectar evidencias de la vulneración de los sistemas. Cuando una empresa contrata servicios de informática forense puede perseguir objetivos preventivos, anticipándose al posible problema, u objetivos correctivos como solución una vez que la vulneración y las infracciones ya se han producido. Todo el procedimiento debe hacerse tenido en cuenta los requisitos legales para no vulnerar en ningún momento los derechos de terceros que puedan verse afectados, con el fin que, llegado el caso, las evidencias sean aceptadas por los tribunales y puedan constituir un elemento de prueba fundamental, si se plantea un litigio. En este bloque se estudiará la problemática de la informática forense así como sus bases legales, los distintos tipos de delitos informáticos (“cibercrimen”) que se pueden cometer y las actuaciones que se pueden llevar a cabo.

Los principales objetivos del curso son:

- Ser capaz de analizar un sistema cuando ha ocurrido un acceso no autorizado, un robo de información o un mal uso de los recursos en general.

- Conocer los aspectos legales que deben considerarse durante el análisis forense.
- Conocer y saber utilizar las técnicas y herramientas más útiles para la realización del análisis forense.
- Conocer las acciones legales que a emprender cuando ocurre un acceso no autorizado, robo o modificación de información, espionaje, etc

COMPETENCIAS

Competencias generales

- Capacidad de análisis y síntesis
- Capacidad de organizar y planificar
- Comunicación oral y escrita en la lengua propia
- Conocimiento de una segunda lengua (preferentemente inglés)
- Habilidades de gestión de la información
- Resolución de problemas
- Toma de decisiones
- Capacidad crítica y autocrítica
- Trabajo en equipo
- Responsabilidad y compromiso ético
- Liderazgo
- Capacidad de aplicar los conocimientos en la práctica
- Habilidades de investigación
- Capacidad de aprender
- Capacidad de adaptarse a nuevas situaciones
- Capacidad de generar nuevas ideas
- Habilidad para trabajar de forma autónoma

Competencias específicas

- Capacidad para seleccionar, diseñar, desplegar, integrar, evaluar, construir, gestionar, explotar y mantener las tecnologías de hardware, software y redes, dentro de los parámetros de coste y calidad adecuados.
- Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

Conocimientos

- Ser capaces de asumir la responsabilidad de su propio desarrollo profesional y de su especialización en uno o más campos de estudio.
- Haber adquirido conocimientos avanzados y demostrado, en un contexto de investigación científica y tecnológica o altamente especializado, una comprensión detallada y fundamentada de los aspectos teóricos y prácticos y de la metodología de trabajo en uno o más campos de estudio.
- Saber aplicar e integrar sus conocimientos, la comprensión de estos, su fundamentación científica y sus capacidades de resolución de problemas en entornos nuevos y definidos de forma imprecisa, incluyendo contextos de carácter multidisciplinar tanto investigadores como profesionales altamente especializados.
- Ser capaces de predecir y controlar la evolución de situaciones complejas mediante el desarrollo de nuevas e innovadoras metodologías de trabajo adaptadas al ámbito científico/investigador, tecnológico o profesional concreto, en general multidisciplinar, en el que se desarrolle su actividad.

- Haber desarrollado la autonomía suficiente para participar en proyectos de investigación y colaboraciones científicas o tecnológicas dentro su ámbito temático, en contextos interdisciplinares y, en su caso, con una alta componente de transferencia del conocimiento

Destrezas

- Conoce los elementos vulnerables en el desarrollo de planes de ciberseguridad.
- Demuestra que conoce y utiliza las Tecnologías de la Información y la Comunicación aplicadas a la Seguridad Informática.
- Conoce y aplica las herramientas para la búsqueda activa de empleo y el desarrollo de proyectos de emprendimiento.
- Demuestra habilidades para el trabajo cooperativo, la participación en equipos y la negociación, incorporando los valores de cooperación, esfuerzo, respecto y compromiso con la búsqueda de la calidad como signo de identidad.

TEMARIO / PROGRAMA ACADÉMICO

- Informática forense. Principios y entorno de trabajo
  - Introducción
  - Creación de laboratorios en Windows
  - Creación de laboratorios en Linux
- Recolección de evidencias
  - Asegurar la escena
  - Identificar las evidencias
  - Preservar las evidencia (cadena de custodia)
- Captura y análisis de evidencias en Windows
  - FTK imager (clonación y análisis de la evidencia)
  - Volatility
  - Etiquetado
  - Captura Ram en ejecución
  - Captura servicios ejecución
  - Captura de procesos en ejecución
  - Captura de usuarios
  - Estado de la red
  - Evidencias no volátiles
    - Hardware
    - Logs
    - Papelera de reciclaje
    - Ficheros y directorios
    - Variables y tareas
    - Historiales
    - Contraseñas
    - Evidencias de registro
- Captura y análisis de evidencias en Linux
  - Estructura de directorios
  - Sistemas de archivos
  - Particiones
  - Antivirus
  - Detección de Rootkits
  - Ficheros ocultos
  - Análisis de directorios
  - Logs
  - Reputación de ficheros

- Análisis de correos electrónicos
    - Sistema de análisis
    - Trazabilidad
    - Probabilidad de origen
- El informe pericial
    - Identificación
    - Juramento
    - razón de ciencia
    - Objeto del peritaje
    - Antecedentes
    - Desarrollo del dictamen
    - Conclusiones
    - Materiales complementarios
    - Firmas
- Captura y análisis de evidencias en Móviles
    - Dispositivos Android
        - Depuración USB-ADB
        - Root-unroot
        - Aplicaciones instaladas
        - Contactos, historial y mensajes
        - Conexiones mwifi
        - Whatsapp y oras RRSS
    - Dispositivos IOS
        - Decifrado del patrón de bloqueo
        - Jailbreak
        - Iphone data protector
        - Imazing
        - Análisis de directorio y aplicaciones sospechosas
        - Contactos, historial y mensajes
        - Conexiones mwifi
        - Whatsapp y oras RRSS
- Ciberseguridad de defensa

RESULTADO DEL APRENDIZAJE

<<Los resultados de aprendizaje son declaraciones de lo que se espera que un estudiante conozca, comprenda y/o sea capaz de hacer al final de un proceso de formación y aprendizaje (ANECA 2022).
Se concretan en:

- *Conocimientos o contenidos que han sido comprendidos, mediante la asimilación de teorías, información, datos, etc.*
- *Habilidades o destrezas, actitudes y valores para aplicar conocimientos y utilizar técnicas a fin de completar tareas y resolver problemas.*
- *Capacidades demostradas para utilizar conocimientos, destrezas y habilidades personales, sociales y metodológicas en situaciones de trabajo o estudio y en el desarrollo profesional y personal. >>*

- Conocer los aspectos legales que deben considerarse durante el análisis forense.
- Conocer las acciones legales que a emprender cuando ocurre un acceso no autorizado, robo o modificación de información, espionaje, etc.

ACTIVIDADES FORMATIVAS

<< Las actividades formativas que se realizarán en cada módulo/materia/asignatura (lo que corresponda). Para cada una de ellas se establecerá las horas de dedicación, porcentaje de presencialidad de dichas horas, y qué porcentaje de la actividad formativa implica interacción estudiantado/profesorado. Tal y como se indica en el Documento de REACU de 15 de enero de 2020 "Las actividades formativas desarrolladas a través de Internet, de modo sincrónico e interactivo, podrán equipararse a las actividades de tipo presencial de modo síncrono con las actividades formativas de tipo presencial.">>

En la asignatura se seguirán las actividades siguientes:

- Clases presenciales teóricas
- Prácticas con ordenador
- Seminarios
- Trabajos dirigidos
- Tutorías personalizadas
- Estudio y trabajo personal
- Pruebas presenciales (en directo) de evaluación

ACTIVIDADES PRESENCIALES	HORAS
Clases teóricas y prácticas en aula	50
Trabajos (trabajos con asesoramiento y presentación)	13
Tutorías presenciales (individuales o grupales) (5%)	18
Actividades de evaluación	8
	89 (35%)

Los alumnos de metodología virtual desarrollan las actividades presenciales en online síncrono.

METODOLOGÍA Y PLAN DE TRABAJO

La Universidad trabaja con 3 metodologías de enseñanza de clases en directo:

1) Presencial.
2) Semipresencial.
3) Online.

Además, cuenta con una cuarta metodología virtual o a distancia con clases asincronías y recursos de enseñanza (grabados), en la cual el alumno no asiste en directo a clases.

La definición de la presencialidad viene definida según se recoge en la guía de calidad universitaria descrita por ANECA (acreditadora oficial de la calidad universitaria en España) donde:

Presencial:

La metodología presencial se define como aquella que tiene presencia en directo del profesor docente, ya sea en aula o de manera virtual síncrona y siempre que supere un 34% de las horas correspondientes a los ECTS (1 ECTS son 25 horas de trabajo total).
En cada guía docente de la asignatura tendrá una definición concreta de la distribución de actividades presenciales y no presenciales, así como las horas de actividad formativa presencial por actividad concreta.

Definición en base a la guía de apoyo ANECA (Memoria de verificación de títulos 2023, ANECA Verifica). “Enseñanza presencial, aquella en la que la mayor parte de las actividades formativas se desarrollan preferentemente de forma presencial, es decir, interactuando el profesorado y el alumnado en el mismo espacio físico, sea éste el aula, laboratorios, espacios académicos especializados, etc. (presencia física y síncrona).” Y lo establecido en el RD 822/2021 en su artículo 14.7

Según definición de RD 1125/2003. Y define los siguientes tipos de actividades:

- Actividades presenciales. Son aquellas en las que el profesor o profesora está presente:

  - Actividades presenciales convencionales. Se refieren a las clases de teoría y/o problemas y a las prácticas de laboratorio o aula de informática. Suelen ser actividades sistemáticas y estar recogidas dentro del horario académico del centro.
  - Actividades presenciales no convencionales. El profesorado está presente, pero no están recogidas dentro del horario del centro: tutorías, pruebas de evaluación, seminarios, visitas, exposición de trabajos, etc.
- Actividades no presenciales. El profesor o profesora no está presente en ningún momento: estudio personal, preparación de trabajos e informes individuales o en grupo, etc.

Semipresencial:

SBS mezcla la metodología virtual con actividades síncronas y asíncronas. Las actividades síncronas obligatorias para el alumno son las pertenecientes a la evaluación de cada asignatura.

Definición en base a la guía de apoyo ANECA (Memoria de verificación de títulos 2023, ANECA Verifica). "Enseñanza semipresencial, aquella en que la gran mayoría de las actividades formativas previstas en el plan de estudios no requieren la presencia física del estudiantado y profesorado en el centro de impartición del título. Tal y como especifica el RD 822/2021 un título podrá definirse como semipresencial o híbrida si al menos el 40% -80% de los créditos que lo configuran se imparten en dicha modalidad."

Virtual:

SBS mezcla la metodología virtual con actividades síncronas y asíncronas. Las actividades síncronas obligatorias para el alumno son las pertenecientes a la evaluación de cada asignatura.

Definición en base a la guía de apoyo ANECA (Memoria de verificación de títulos 2023, ANECA Verifica). "Enseñanza virtual, aquella en que la gran mayoría de las actividades formativas previstas en el plan de estudios no requieren la presencia física del estudiantado y profesorado en el centro de impartición del título. Tal y como especifica el RD 822/2021 un título podrá definirse como virtual si al menos el 80% de los créditos que lo configuran se imparten en dicha modalidad."

Cabe destacar que la metodología de la Universidad es enriquecida dado que complementa los directos con recursos adicionales en el campus (cursos de la materia post-producidos, notas técnicas, casos prácticos, referencias adicionales, exámenes, etc.)

Sobre la definición anterior de las metodologías SBS, ¿cómo se trabajan a nivel educativo?

1) Presencial

   El alumno asiste presencialmente en aula entre 2-5 días por semana lo que confiere entre 8-20 horas de asistencia en aula semanales. El alumno debe complementar la enseñanza del aula con el estudio del campus virtual.
   Cada asignatura se configura en un número de ECTS. Cada ECTS son 25 horas totales y siguiendo la norma ANECA de estudios superiores, al menos el 34% de estas horas deben ser en acciones directas con el profesor (8,5). SBS, siguiendo la norma, realiza la siguiente distribución:
   - Al menos 5 horas de clase presencial en aula
   - 1-1,5 horas de evaluación (examen)
   - 1-1,5 horas de tutoría
   - 1-1,5 horas de trabajo práctico guiado por el profesor

   Cada asignatura cuenta con una guía docente donde queda definido particularmente el funcionamiento en el apartado de Actividades formativas.

2) Semipresencial

   El alumno asiste en directo entre 2-5 días por semana lo que confiere entre 8-20 horas de asistencia semanales (bien en presencial física en el aula u online directo

de la emisión). El alumno debe complementar la enseñanza del aula con el estudio del campus virtual.

Existe una variación a la metodología en la edición de febrero/marzo. El alumno asiste regularmente en aula los viernes sin limitación a que pudieran establecerse otros días presenciales en aula. Además, tiene entre semana días de clase online directo en una periodicidad entre 1 y 4 que complementa la acción presencial según recoge la guía. En esta variación el número de horas del alumno en directo (presencial aula o virtual) será de 6-14 h semanales.

3) Online

El alumno asiste de manera virtual a las clases, sin limitación a que pueda ser invitado por la escuela a algún periodo presencial en aula o bootcamp intensivo. Atendiendo a la definición del punto anterior, el alumno tendrá clases en directo de entre 8-20 horas semanales para la edición de septiembre/octubre y 6-14 horas para la edición de febrero/marzo.

Igualmente, el alumno debe complementar la enseñanza del aula con el estudio del campus virtual.

Es importante destacar que, con independencia de la metodología, los exámenes se realizan en directo, bien en aula o virtual con identificación y cámara para garantizar la veracidad del alumno. La parte práctica docente utiliza además de metodologías más tradicionales otras metodologías innovadoras basadas en:

- Aprendizaje basado en proyecto
- Estudios, análisis y exposiciones de métodos del caso
- Aprendizaje cooperativo y colaborativo
- Trabajo por ámbitos
- Gamificación educativa

SISTEMA DE EVALUACIÓN

La evaluación se llevará a cabo a través de las distintas pruebas de la asignatura:

- 100%. Examen final y pruebas prácticas de desarrollo sobre la materia.

Si hay casos prácticos se evalúan atendiendo a

1. Entrega de la memoria del caso
2. Exposición en público de este (en caso de ser un caso que requiera exponer, a decisión del profesor)

El examen tipo test es un examen de solución única en la que los fallos no restan. Se realiza en el campus online, en directo y siguiendo las instrucciones del profesor que puede ser presencial u online. Una vez se inicia el examen se genera uno específico para el alumno (distinto a otro pero de igual dificultad) que deberá realizarlo en ese momento. No puede salirse o dar para atrás en el navegador una vez visualizada la primera pregunta. Si sucediera alguna incidencia (corte de luz, internet, cierre inesperado, etc…) el examen se bloquea. Dicha incidencia debe ser reportada a la escuela quien analizar el comportamiento de uso anterior a la incidencia. Si es una incidencia se retomará un nuevo intento. Si hay algún indicio de fraude o engaño, el examen queda suspenso con la nota obtenida hasta el momento del corte o incidencia. No es alarmante, pero la escuela cuenta con un sistema antifraude.

Las fechas de examen, concretas a la edición, serán informados por el tutor principal de la asignatura.

BIBLIOGRAFÍAS

- Notas técnicas propias SBS
- C. Altheide y H. Carvey, Digital Forensics with Open Source Tools. Syngress. ISBN: 978-1597495868
- H. Carvey, Windows Forensic Analysis Toolkit. Syngress. ISBN: 978-1597497275
- E. Casey, Handbook of Digital Forensics and Investigation. Academic Press. ISBN: 978-0123742674
- B. Nelson, Guide to Computer Forensics and Investigations. Cengage Learning. ISBN: 978-1435498839