GUIA DOCENTE DEL CURSO
INTRODUCCIÓN A LA CIBERSEGURIDAD

AREA: DIGITAL BUSINESS
AUTOR: SPAIN BUSINESS SCHOOL

CÓDIGO: GD-732

IDENTIFICACIÓN DE LA ASIGNATURA

- Denominación: Introducción a la Ciberseguridad
- Código: 732
- Curso: 1
- Cuatrimestre: 1
- Carácter: Optativa
- Nº de créditos (horas): 1 ECTS (25 horas)
- Idioma en que se imparte: Español

REQUISITOS PREVIOS

No tiene requisitos previos.

PROFESORES Y CONFERENCIANTES

Gustavo Vallejo

Soy un profesional con 20 años de experiencia, 12 de los cuales en Seguridad de la Información. Realicé responsabilidades de consultor senior, especialista técnico, arquitecto de soluciones, líder del equipo y director del proyecto.

Gerente de servicios de seguridad en Open-Sec. Anteriormente responsable de seguridad en Telefónica ingeniería de Seguridad en Perú.

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

Francisco Sanz Moya

Ingeniero informático por la universidad Autónoma de Madrid. Licenciado en marketing y gestión comercial por ESIC. Varias certificaciones CISCO

Fundador, Co-CEO, CTO de TSS Ciberseguridad

- Categoría: Master

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

DESCRIPCIÓN Y OBJETIVOS

La ciberseguridad es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales. Las organizaciones tienen la responsabilidad de proteger los datos para mantener la confianza del cliente y cumplir la normativa. Utilizan medidas y herramientas de ciberseguridad para proteger los datos confidenciales del acceso no autorizado, así como para evitar interrupciones en las operaciones empresariales debido a una actividad de red no deseada. Las organizaciones implementan la ciberseguridad al optimizar la defensa digital entre las personas, los procesos y las tecnologías.

En los negocios de varios sectores, como la energía, el transporte, el comercio al detalle y la fabricación, use sistemas digitales y conectividad de alta velocidad para proporcionar un servicio eficiente al cliente y ejecutar operaciones empresariales rentables. Igual que protegen los recursos físicos, deben proteger también los recursos digitales y los sistemas frente al acceso no intencionado. El evento no intencionado de incumplimiento y acceso no autorizado a un sistema informático, una red o recursos conectados se denomina ciberataque. El éxito de un ciberataque produce la exposición, sustracción, eliminación o alteración de datos confidenciales. Las medidas de ciberseguridad defienden frente a ciberataques y proporcionan los siguientes beneficios.

COMPETENCIAS

Competencias generales

- Trabajar en equipos interdisciplinares (Competencias Interpersonales)
- Analizar sintetizar y organizar información masiva de grandes volúmenes de datos (Competencias Instrumentales)

Competencias específicas

- Desarrollar la implementación y puesta en marcha de proyectos en el ámbito de la gestión de la ciberseguridad.
- Identificar, conocer y comprender los marcos regulatorios, organizaciones de referencia, estándares y recomendaciones existentes en el ámbito de las redes digitales y de la ciberseguridad.
- Desarrollar e implementar políticas, procedimientos, normas y guías de seguridad de la información en organizaciones sectoriales, garantizando la disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad de los recursos valiosos de un sistema de información.

Conocimientos

- Aplicar los conocimientos de protección de datos y seguridad de la información en distintos niveles.
- Ejecutar técnicas de desarrollo y prenetración analizando las mejoras técnicas, soluciones y buenas prácticas.
- Realizar desarrollos seguros y aplicar contramedidas a nivel de código.
- Identificar los fundamentos teóricos y arquitecturas de los SSOO.
- Conocer la nube, su seguridad y sus aplicaciones

Destrezas

- Trabajar en grupo transmitiendo conocimientos y habilidades adquiridos.
- Desarrollar habilidades para el análisis, la elaboración y la colaboración en proyectos, partiendo de las necesidades propias del mercado.
- Ser capaz de trabajar con información técnica en inglés, tanto a nivel de consulta como de su elaboración.
-

TEMARIO / PROGRAMA ACADÉMICO

Gobierno del dato e información

a. Tipo de datos e identidad de la información
b. Ciclo de vida de la información
c. Seguridad de la información

¿Qué aprenderemos?

- Conocer los distintos tipos de datos digitales que existen y sus distintos tránsitos en medios digitales. Incluye la descripción de la identidad de la información digital.
- Describir cada una de las fases del ciclo de vida de la información en medios digitales.
- Conocer los requisitos del estándar ISO/IEC 27001:2013 - Sistema de Gestión de Seguridad de la Información como medio para realizar la protección de la información.
- Elaboración de un plan de gestión de datos e información.

Introducción a la ciberseguridad

- Introducción
  - Certificado (Validez, ventajas)
  - Objetivo
  - Metodología
  - Materiales didácticos
  - Oportunidades laborales
  - Definición de hacker
  - Hackers conocidos
  - Hacking ético, profesión
  - Perfil del Hacker ético
  - Tipos de auditorías
- Arquitectura de redes
  - Introducción
  - Modelo OSI
  - NAT vs Bridge

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. >>*

- Diseñar e implementar proyectos en Gestión de la Ciberseguridad.
- Elaborar planes y políticas, normas y procedimientos Gestión de la Ciberseguridad.

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	5
Trabajos (trabajos con asesoramiento y presentación)	1
Tutorías presenciales (individuales o grupales) (5%)	2
Actividades de evaluación	1
	9 (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
- Adam Shostack. Threat modeling designing of security.
- Michael Sikorski and Andrew Honig. Practical Malware Analysis.
- Simon Singh. The code book.
- Cristopher Hadnagy. Social Engineering,

Otros Recursos de Aprendizaje Recomendados

- https://www.nist.gov/
- https://www.shodan.io/
- https://www.wireshark.org/download.html
- https://www.first.org/cvss/
- https://attack.mitre.org/
- https://www.cisecurity.org/