GUIA DOCENTE DEL CURSO
DIRECCIÓN DE LA CIBERSEGURIDAD

AREA: DIGITAL BUSINESS
AUTOR: SPAIN BUSINESS SCHOOL

CÓDIGO: GD-655

IDENTIFICACIÓN DE LA ASIGNATURA

- Denominación: Dirección de la Ciberseguridad
- Código: 655
- 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 básicos técnicos y de Linux sin recomendables. Es recomendable haber cursado primero el curso de Introducción a la Ciberseguridad.

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

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.

Es por lo tanto que el curso intenta cumplir los objetivos:

- Prevención o reducción del costo de las brechas
  Las organizaciones que implementan estrategias de ciberseguridad minimizan las consecuencias no deseadas de ciberataques que pueden afectar a la reputación empresarial, las capacidades financieras, las operaciones empresariales y la confianza del cliente. Por ejemplo, las compañías activan planes de recuperación de desastres para contener las posibles intrusiones y minimizar las interrupciones en las operaciones empresariales.

- Mantenimiento de la conformidad normativa
  Las empresas de sectores y regiones específicos deben cumplir con los requisitos normativos para proteger los datos confidenciales frente a posibles riesgos cibernéticos. Por ejemplo, las empresas que operan en Europa deben cumplir el Reglamento General de Protección de Datos (GDPR), que espera que las organizaciones adopten las medidas de ciberseguridad adecuadas para garantizar la privacidad de los datos.

- Mitigación de las ciberamenazas en desarrollo
  Los ciberataques evolucionan a la par que las tecnologías cambiantes. Los delincuentes utilizan nuevas herramientas y elaboran nuevas estrategias para el acceso no autorizado al sistema. Las organizaciones emplean y actualizan las medidas de ciberseguridad para mantenerse al día de estas tecnologías y herramientas de ataque digital nuevas y en desarrollo.

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

- 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

1. Gestión del riesgo operacional
    a. Gestión de procesos y activos
    b. Gestión de vulnerabilidades
    c. Gestión del riesgo

    ¿Qué aprenderemos?
    - Entender la estructura y organización de los procesos que soportan al negocio y la relación de los activos (recursos) que se necesitan proteger.
    - Conocer las fuentes de declaración, scoring de vulnerabilidades, incluyendo los procesos y tecnologías necesarias para identificarlos dentro de los activos.
    - Conocer los procesos de gestión de riesgos basado en el estándar ISO 31000:2018 - Gestión del Riesgo.
    - Elaboración de un plan de gestión de riesgo operacional.

2. Leyes y regulaciones en el entorno de los datos
    a. Protección de datos personales
    b. Delitos informáticos y convenios internacionales
    c. Protección de evidencias informáticas

    ¿Qué aprenderemos?
    - Identificar las leyes entorno a la protección de datos personales y su relación con la seguridad de la información.
    - Identificar las leyes entorno a delitos informáticos y convenios internacionales en materia de delitos informáticos.
    - Conocer las técnicas, procedimientos y regulaciones entorno a las evidencias informáticas que serán utilizadas para análisis forense.
    - Elaboración un procedimiento de evidencias informáticas.

3. Ofrecimiento de servicios en la nube
    a. Tipos y características de servicios en nube
    b. Marco normativo de servicio en nube
    c. Servicios de seguridad en la nube

    ¿Qué aprenderemos?
    - Entender los tipos y características de los servicios en nube que soportan la arquitectura empresarial.
    - Identificar los estándares y buenas prácticas entorno a la seguridad de la información en servicios en nube.
    - Conocer la descripción de los servicios de seguridad que ofrecen los servicios en la nube.
    - Elaboración de modelo de autenticación a servicios en nube.

4. Gestión de defensa y respuesta a incidentes
    a. Amenazas avanzadas
    b. Detección de eventos
    c. Respuesta de incidentes

    ¿Qué aprenderemos?
    - Identificar las prácticas entorno a la identificación de amenazas avanzadas, usando técnicas de ciber-inteligencia.
    - Conocer los procesos y tecnologías que permiten automatizar la detección de eventos de seguridad.
    - Conocer los procesos y tecnologías que permiten automatizar la respuesta ante incidentes de seguridad.
    - Elaboración de plan de respuesta ante incidentes.

5. Arquitectura de seguridad
    a. Arquitectura empresarial
    b. Marco de ciberseguridad
    c. Modelos de arquitectura de seguridad

¿Qué aprenderemos?

- Conocer el modelo de organización de servicios digitales dentro de la tecnología de la información basada en el modelo de TOGAF.
- Entender de las funciones del marco de ciberseguridad basada en NIST CyberSeguridad y su alineación a estándares y buenas prácticas en seguridad.
- Identificar los modelos de arquitectura de seguridad que existen para brindar seguridad a la arquitectura empresarial.
- Elaboración de diseño de arquitectura de seguridad.

6. MLSec. Machine Learning para la Cibersegruidad
    a. Machine Learning & NLP
    b. Deep Learning, Reinforcement Learning y GANs
    c. ML para la Ciberseguridad (MLSec)

¿Qué aprenderemos?

- Entender el Machine Learning a través de una exploración de los algoritmos más importantes supervisados y no supervisados. Incluye exploración de técnicas para manejo de lenguaje (NLP).
- Entender el Deep Learning y sus variantes más importantes como CNN o RNN. Adicionalmente entender el aprendizaje reforzado (reinforcement learning) y GANs (redes generativas antagónicas).
- Presentación de diversos casos de uso de ML aplicado a la Ciberseguridad (MLSec) tomando en cuenta tanto un enfoque defensivo como ofensivo.
- 2 laboratorios en donde se implementan aplicaciones de MLSec usando técnicas de ML y Deep Learning respectivamente. Uso de Python y Open Source.

7. Seguridad en las operaciones
    a. Gestión de servicio TI
    b. Seguridad en desarrollo de software
    c. Seguridad física

¿Qué aprenderemos?

- Identificar los servicios TI que soportan la arquitectura empresarial y que deben ser protegidos por la arquitectura de seguridad.
- Identificar los componentes de desarrollo de software que necesitan de seguridad para entregar aplicaciones seguras.
- Reconocer los ambientes físicos en donde se realizan procesamiento o tránsito de la información para brindarles seguridad.
- Elaboración de plan de protección de servicio de TI y desarrollo.

8. Evaluación de postura de seguridad
    a. Ejercicio de ataque y respuesta
    b. Monitoreo y evaluación de controles
    c. Auditoría interna

¿Qué aprenderemos?

- Identificar los modelos para realizar ejercicios de ataque y respuesta a la arquitectura de seguridad.
- Definir los modelos de monitoreo y evaluación de los controles implementados dentro de la arquitectura de seguridad.

- Realizar la auditoría interna bajo el estándar ISO 19011 para revisar el correcto funcionamiento de los controles implementados.
- Elaboración de plan de verificación de postura de seguridad

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	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
- Gómez Fernández, Luis. Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad /
- Gómez Fernández, Luis. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes[recurso electrónico] / 2a ed. Madrid :AENOR,2012.