Guía Docente

DATOS DE IDENTIFICACIÓN

Titulación:	Grado en Análisis de Negocios/Business Analytics
Rama de Conocimiento:	Ciencias Sociales y Jurídicas
Facultad/Escuela:	Derecho, Empresa y Gobierno
Asignatura:	Seguridad de la Información y de los Sistemas
Tipo:	Obligatoria
Créditos ECTS:	3
Curso:	4
Código:	5337
Periodo docente:	Séptimo semestre
Materia:	Informática Aplicada al Análisis de Negocios / IT applied to Business Analytics
Módulo:	Formación Disciplinar
Tipo de enseñanza:	Presencial
Idioma:	Castellano
Total de horas de dedicación del alumno:	75

Equipo Docente	Correo Electrónico
Enrique de Miguel Ambite	enrique.demiguel@ufv.es

DESCRIPCIÓN DE LA ASIGNATURA

La Seguridad de los Sistemas de Información es una faceta esencial y estratégica en la gestión de las empresas y organizaciones. La disponibilidad y continuidad de los negocios depende significativamente de los Sistemas donde se gestionan los datos, la información y el conocimiento. La Seguridad de los Sistemas de Información ha trascendido, de ser exclusivamente una materia del campo de la tecnología, los sistemas y las redes, a situarse en el centro de las organizaciónes y empresas, alrededor de la cuál se construyen, desde una perspectiva segura, el resto de las unidades y áreas (la Seguridad en el interior del Diseño de las Organizaciones).

OBJETIVO

Aprender signficativamente el carácter y la naturaleza holística de la Seguridad de la Información y los Sistemas en las organizaciones, identificando las estrategias, áreas, metodologías y técnologías idóneas para la detección, análisis, gestión y remediación de los riesgos, amenazas y vulnerabilidades en los procesos que garanticen la disponibilidad y continuidad del negocio.

CONOCIMIENTOS PREVIOS

Los propios de los estudios en los cursos académicos anteriores.

CONTENIDOS

1. Fundamentos y términos clave en Seguridad de la Información y los Sistemas. Ciberseguridad.
2. Tipos de ataques y amenazas. Categorias y clasificaciones.
3. Fundamentos de las Tecnologías básicas utilizadas para proteger los activos de una organización. Principios de la Detección y Prevención en los Sistemas.
4. Diseño de Redes de Seguridad Corporativa. Analizadores de redes y tráfico. Estrategias para Identificar y Remediar en activos de la organización. Evaluación y Detección de Vulnerabilidades. Herramientas software
5. Seguridad en Sistemas y Redes DAO (Decentralized Autonomous Organization). Smart Contracts y Blockchain.
6. Gestión de la Seguridad Corporativa. Estrategia y Gestión de un Programa Director de Seguridad. Politicas, Procesos y Procedimientos de Seguridad. Identificación de riesgos y áreas. Identificación de componentes sistémicos y eslabones más débiles. Concienciación de los usuarios y responsables de la organización.

ACTIVIDADES FORMATIVAS

La metodología seguida en esta asignatura está dirigida a conseguir un aprendizaje significativo por parte del alumno de los conceptos y técnicas fundamentales de la materia. Por ese motivo se combinan sesiones de carácter expositivo e interactivas con los alumnos, con sesiones de carácter práctico y presentaciones de resultados/conclusiones de los mismos, tanto a nivel individual como grupal. De este modo, se logra la participación del alumno y la interacción alumno-profesor y alumno-alumno como vía para fomentar el aprendizaje colaborativo y la capacidad de autoaprendizaje. En algunos casos, el alumno tendrá que realizar en clase la exposición de las principales conclusiones de su estudio o trabajo, lo que permitirá el intercambio de conocimientos y experiencias entre alumnos. Se priorizarán las técnicas pedagógicas de Aprendizaje Basado en Problemas (ABP) y "Flipped-Learning".
El trabajo presencial se completará con trabajo autónomo por parte del alumno, en algunos casos desarrollados en grupo, de manera que se fomente el aprendizaje cooperativo.
Finalmente, con el fin de facilitar al alumno el acceso a los materiales y la planificación de su trabajo, así como la comunicación con el profesor y el resto de alumnos, se empleará plataformo LMS: Aula Virtual (CANVAS), que es una plataforma de aprendizaje que ofrece diferentes recursos electrónicos para complementar, de forma muy significativa, el aprendizaje del alumno.
Todo el estudio y trabajo realizado por el alumno será supervisado y guiado por el profesor mediante tutorías, individuales o en grupo.

DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO

ACTIVIDAD PRESENCIAL	TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL
30 horas	45 horas
Lección expositiva 11h Clases prácticas 11h Pruebas/Prácticas/Trabajos 8h	Estudio y trabajo individual 30h Trabajo en grupo 15h

COMPETENCIAS

Competencias básicas

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

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

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

Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado

Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

Competencias generales

Compromiso ético en la sociedad de la información

Capacidad de diseñar e implementar proyectos e informes, utilizando con naturalidad los canales digitales

Capacidad de liderazgo y de trabajar en equipo en la sociedad de la información

Capacidad de pensamiento crítico, autocrítico, analítico y reflexivo

Capacidad de aprendizaje autónomo en la sociedad de la información

Competencias específicas

Conocer y comprender los fundamentos de la planificación estratégica y la dirección de proyectos y aplicarlos a la realidad

Conocer, comprender y aplicar los fundamentos y las herramientas de la programación para el uso y explotación de la información, garantizando su seguridad e integridad

Ser capaz de conocer los fundamentos, paradigmas y técnicas propias de los sistemas inteligentes y analizar, diseñar y construir sistemas, servicios y aplicaciones informáticas que utilicen dichas técnicas en el ámbito del big data

RESULTADOS DE APRENDIZAJE

Evaluar las repercusiones técnicas y de negocio de los requisitos de seguridad en el diseño, desarrollo, implantación y mantenimiento de los sistemas de información; así como de la necesidad de construir estos sistemas mediante proyectos cuya gestión se realice teniendo en cuenta criterios de seguridad de la información tratada.

Aplicar metodologías y marcos de actuación que permitan analizar los riesgos de seguridad y evaluar diferentes escenarios, independientemente de los entornos tecnológicos y de negocio que los caractericen.

Analizar las vulnerabilidades más relevantes de los sistemas, aplicaciones y bases de datos comerciales utilizadas actualmente en las organizaciones.

SISTEMA DE EVALUACIÓN DEL APRENDIZAJE

El sistema de evaluación continua contempla cuatro tipos de pruebas:
Examen final (50%) + Resolución Ejercicios (20%) + Tareas Individuales/Grupales (20%) + Participación en clase (10%)

•[1] Examen escrito teórico- práctico final: presenta un peso del 50% en la nota final. El formato del mismo podrá contener preguntas cortas, preguntas de desarrollo, resolución de supuestos prácticos y/o preguntas tipo de test de diferente tipología: respuesta múltiple, respuesta única, Verdadero/Falso, etc
•[2,3] Pruebas en clase, prácticas, resolución de casos prácticos y otros trabajos relacionados con la asignatura tanto individuales como grupales: presenta un peso del 40% en la nota final (distribuido del siguiente modo: resolución de ejercicios (20%); preparación, resolución de tareas y casos prácticos ABP individuales y grupales y presentaciones (20%)
•[4] Participación en clase, interacción en foros, actitud de aprendizaje cooperativo e implicación en el aprendizaje (Flipped-Learning): presenta un peso del 10% en la nota final.
La nota ponderada de la evaluación continua será un valor entre 0 y 10 y se calculará como sigue: 0,5*[1]+ 0,2*[2]+ 0,2*[3]+ 0,1*[4] .
En las tres primeras pruebas [1],[2],[3] es necesario obtener un mínimo de 5 puntos sobre 10 para poder aprobar la asignatura.

Los alumnos que no cursen la evaluación continua de la asignatura y aquellos alumnos que estén exentos de la obligación de asistir a clase, bien por segunda matrícula en la asignatura o sucesivas, bien por contar con autorización expresa de la Dirección del Grado, serán evaluados por el cómputo de: un examen teórico-práctico (70%) que aúne la totalidad de contenidos y habilidades descritas en la presente guía didáctica. El formato de dicha prueba será similar al explicitado anteriormente como [1]; y por un Trabajo Individual (30%).

Recuperación en convocatoria extraordinaria: Los alumnos que no hayan alcanzado la nota mínima en la evaluación ordinaria podrán presentarse a la convocatoria extraordinaria, evaluándose la totalidad de los contenidos y habilidades como las descritas en el apartado de evaluación continua ordinaria.

La condición de No Presentado en la convocatoria ordinaria/extraordinaria se corresponderá con la no presentación por parte del alumno/a a las pruebas teorico-prácticas de la asignatura.

Los alumnos están obligados a observar las reglas elementales y básicas sobre autenticidad y originalidad en toda actividad formativa o prueba de evaluación. Cuando un alumno disponga o se valga de medios ilegítimos en la celebración de una prueba de evaluación, incurra en plagio, o se atribuya indebidamente la autoría de trabajos académicos requeridos para la evaluación será sancionado conforme a lo establecido en la Normativa de Evaluación y Convivencia de la universidad

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Peter H. Gregory. Página CISM Certified Information Security Manager Bundle

Victor Ruiz Lara. Ciberseguridad Ahora: Conceptos clave para gestionar el riesgo y asegurar los activos empresariales.

Aranzadi. Guía práctica de Ciberseguridad.