Universidad Francisco de Vitoria UFV Madrid

Guía Docente

DATOS DE IDENTIFICACIÓN

Titulación:	Integral Leadership Program (Título propio asociado a ADE+DER)
Rama de Conocimiento:	Ciencias Sociales y Jurídicas
Facultad/Escuela:	Derecho, Empresa y Gobierno
Asignatura:	Digital Lab II: Ciberseguridad
Tipo:	Propia Obligatoria
Créditos ECTS:	2
Curso:	3
Código:	72620
Periodo docente:	Quinto-Sexto semestre
Tipo de enseñanza:	Presencial
Idioma:	Castellano
Total de horas de dedicación del alumno:	50

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

DESCRIPCIÓN DE LA ASIGNATURA

La Ciberseguridad es una faceta esencial y estratégica en la gestión de las empresas y organizaciones. La disponibilidad, reputación y continuidad de los negocios depende significativamente del conocimiento, concienciación, tecnologías y procedimientos para garantizar la protección, detección y remediación de los ataques cibernéticos. 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 estratégica y significativamente el carácter integrador de la Seguridad Cibernética en las empresas y organizaciones que afectan tanto a Tecnologías, Procedimientos y Personas, garantizando la disponibilidad, reputación organizacional y continuidad de los negocios.

CONOCIMIENTOS PREVIOS

No se requieren conocimientos previos.

CONTENIDOS

1. Fundamentos y términos clave en Ciberseguridad.
2. Tipos de ataques y amenazas. Categorias y clasificaciones.
3. Fundamentos de las Tecnologías básicas utilizadas para securizar los activos de una organización.
4. Estrategias para Proteger, Identificar y Remediar en activos de la organización.
5. 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.
LAS ACTIVIDADES FORMATIVAS, ASÍ COMO LA DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO, PUEDEN VERSE MODIFICADAS Y ADAPTADAS EN FUNCIÓN DE LOS DISTINTOS ESCENARIOS ESTABLECIDOS SIGUIENDO LAS INDICACIONES DE LAS AUTORIDADES SANITARIAS.

DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO

ACTIVIDAD PRESENCIAL	TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL

20 horas	30 horas
Lección expositiva 7h Clases prácticas 7h Pruebas/Prácticas/Trabajos 6h	Estudio y Trabajo individual 20h Trabajo en grupo 10h

COMPETENCIAS

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

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

CG10 - 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

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 tres tipos de pruebas:

•[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] 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 (15%); elaboración de wikis-colaborativas (5%); preparación, resolución de casos

prácticos ABP y presentaciones (20%)
•[3] 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]+ 0,4*[2]+ 0,1*[3] .
En las dos primeras pruebas [1],[2] 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 anterior.

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 finales.

TODAS LAS PRUEBAS SUSCEPTIBLES DE EVALUACIÓN ESTARÁN SUPEDITADAS A LO ESTABLECIDO EN LA NORMATIVA DE EVALUACIÓN DE LA UNIVERSIDAD FRANCISCO DE VITORIA.
LAS CONDUCTAS QUE DEFRAUDEN EL SISTEMA DE COMPROBACIÓN DEL RENDIMIENTO ACADÉMICO, TALES COMO PLAGIO DE TRABAJOS O COPIA EN EXÁMENES SON CONSIDERADAS FALTAS GRAVES SEGÚN EL ARTÍCULO 7 DE LA NORMATIVA DE CONVIVENCIA DE LA UFV Y SERÁN APLICADAS LAS SANCIONES OPORTUNAS COMO RECOGE EL ARTÍCULO 9 DEL MISMO DOCUMENTO.
EN EL CASO DE QUE LAS RECOMENDACIONES SANITARIAS NOS OBLIGUEN A VOLVER A UN ESCENARIO DONDE LA DOCENCIA HAYA QUE IMPARTIRLA EXCLUSIVAMENTE EN REMOTO, LOS PARÁMETROS Y PESOS DEL SISTEMA DE EVALUACIÓN DESCRITOS SE MANTIENEN, ÚNICAMENTE ADAPTANDO O MODIFICANDO LA PRESENCIALIDAD CON LAS METODOLOGÍAS REMOTAS e-learning DE LA PLATAFORMA LMS (CANVAS).
LOS EXÁMENES SE REALIZARÁN DE MANERA PRESENCIAL SIEMPRE Y CUANDO LA SITUACIÓN SANITARIA LO PERMITA, PUDIENDO SER MODIFICADOS CON EL OBJETIVO DE CUMPLIR LAS INDICACIONES DADAS POR LAS AUTORIDADES.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

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

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

Guía práctica de Ciberseguridad. Aranzadi.

Complementaria

María Angeles Caballero Velasco, Diego Cilleros Serrano, Abtin Shamsaifar. El Libro Del Hacker (2014). Editorial Anaya Multimedia