21-22

MÁSTER UNIVERSITARIO EN
CIBERSEGURIDAD

GUÍA DE ESTUDIO PÚBLICA



GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD

CÓDIGO 31109082

UNED

21-22

GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD

CÓDIGO 31109082

ÍNDICE

PRESENTACIÓN Y CONTEXTUALIZACIÓN

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

EQUIPO DOCENTE

HORARIO DE ATENCIÓN AL ESTUDIANTE

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

RESULTADOS DE APRENDIZAJE

CONTENIDOS

METODOLOGÍA

SISTEMA DE EVALUACIÓN

BIBLIOGRAFÍA BÁSICA

BIBLIOGRAFÍA COMPLEMENTARIA

RECURSOS DE APOYO Y WEBGRAFÍA

Nombre de la asignatura	GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD
Código	31109082
Curso académico	2021/2022
Título en que se imparte	MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD
Tipo	CONTENIDOS
Nº ETCS	6
Horas	150.0
Periodo	SEMESTRE 2
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

La notificación temprana de los incidentes de ciberseguridad es uno de los factores más importantes para una adecuada actuación y respuesta efectiva. El objetivo de la asignatura es la adquisición de capacidades para el triage y la respuesta adecuada a los ciberincidentes en el contexto de un responsable del centro de operaciones de ciberseguridad.
Esta asignatura expone la clasificación de los riesgos, el marco estratégico y regulatorio para la gestión y notificación de ciberincidentes y se describen las infraestructuras y servicios que hacen posible la notificación y la clasificación de incidentes con objeto de hacer frente adecuadamente a los ciberataques. También complementa otras asiganturas como "Auditoría y Monitorización de la Seguridad" y en menor medida "Ciberdelitos" en la administración de los activos TIC.
La asignatura permite completar el perfil profesional del responsable de ciberseguridad con las habilidades necesarias para organizar los activos, ponderar su importancia y estructurar un plan de respuesta a incidentes en función de la afectación del incidente de ciberseguridad.

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

Esta asignatura no requiere para su aprovechamiento de otras asignaturas del Máster.

EQUIPO DOCENTE

Nombre y Apellidos	MIGUEL RODRIGUEZ ARTACHO (Coordinador de asignatura)
Correo Electrónico	miguel@lsi.uned.es
Teléfono	91398-7924
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	LENGUAJES Y SISTEMAS INFORMÁTICOS

Nombre y Apellidos	ROBERTO HERNANDEZ BERLINCHES
Correo Electrónico	roberto@scc.uned.es
Teléfono	91398-7196
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	JUAN CARLOS LAZARO OBENSA
Correo Electrónico	jclo@scc.uned.es
Teléfono	91398-7163
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

HORARIO DE ATENCIÓN AL ESTUDIANTE

El profesor Miguel Rodríguez Artacho atenderá las guardias acedémicas los Jueves de 11h a 13h y de 14h a 16h.
Mail de contacto: miguel@lsi.uned.es
Teléfono: +34 913 987 924
Dirección postal:
16 Juan del Rosal
28040 Madrid

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

COMPETENCIAS BÁSICAS
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
COMPETENCIAS GENERALES
CG1 - Analizar métodos y técnicas de ciberataques.
CG3 - Conocer la normativa y la legislación en materia de ciberseguridad, sus implicaciones en el diseño y puesta en marcha de sistemas informáticos.
COMPETENCIAS TRANSVERSALES
CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.
CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).
COMPETENCIAS ESPECÍFICAS
CE2 - Diseñar mecanismos de prevención de amenazas a la seguridad, así como de

reconocer y resolver incidentes de seguridad en los sistemas críticos.
CE6 - Conocer las tendencias actuales en técnicas de ciberataque, los mecanismos de defensa mediante aprendizaje automático y especialmente dirigido a casos reales.

RESULTADOS DE APRENDIZAJE

Los resultados más relevantes que se pretenden alcanzar con el estudio de esta asignatura son los siguientes:

•Organizar y mantener un esquema de riesgos
•Conocer la estructura de un ciberataque
•Tipificar los Ciberincidentes y clasificar su peligrosidad ·Clasificar los grupos o niveles de un ciberataque
•Conocer la metodología de notificación al CERT
•Conocer los elementos para diseñar un plan de respuesta de Ciberincidentes

CONTENIDOS

1.- Metodología para el análisis de riesgos: Activos, Agentes y Escenarios de riesgo (ER)

1.1.- Análisis de riesgos
1.2.- Gestión de riesgos
1.3.- Proyectos y planes de seguridad

2.- Catalogación de elementos y activos TIC y de ciberseguridad

2.1.- Tipos de activos
2.2.- Dimensiones de valoración
2.3.- Criterios de valoración
2.4.- Amenazas y Salvaguardas

3.- La gestión de incidentes de Ciberseguridad: Organismos, estrategias, organización y servicios

3.1.- Esquema Nacional de Seguridad
3.2.- Estrategia Nacional de Ciberseguridad (2019)
3.3.- Elementos para la notificación de Ciberincidentes

3.4.- Organismos para la gestión de Ciberincidentes

4.- Normativa y estándares para la notificación de ciberincidentes

4.1.- Organismos de normalización en ciberseguridad

4.2.- Normativa ISO IEC/JTC1 27035

4.3.- Otras normas nacionales e internacionales

METODOLOGÍA

Esta asignatura se impartirá conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, pero asistido por el profesor y articulado a través de diversos sistemas de comunicación docente-discente. Dentro de estos sistemas, cabe destacar que esta asignatura se imparte con apoyo en una plataforma virtual interactiva de la UNED donde el estudiante encuentra tanto materiales didácticos básicos como materiales didácticos complementarios, informaciones, noticias, ejercicios y también permite la evaluación correspondiente a las diferentes materias.
Las actividades formativas para el estudio de la asignatura son las siguientes:

•Estudios de cotenidos (60 horas)

•Tutorías (15 horas)

•Actividades en la plataforma (15 horas)

•Prácticas informáticas (20 horas)

•Otros trabajos (40 horas)

SISTEMA DE EVALUACIÓN

TIPO DE PRUEBA PRESENCIAL

Tipo de examen	Examen de desarrollo
Preguntas desarrollo	
Duración del examen	90 (minutos)
Material permitido en el examen	

Ninguno

Criterios de evaluación

El examen teórico viene a comprobar el grado de asimilamiento de los contenidos referentes a la catalogación (Tema 1) el conocimiento de los marcos legales y estratégicos de seguridad y ciberseguridad (Tema 2) y las normas estandarizadas existentes (Tema 3).

% del examen sobre la nota final	60
Nota del examen para aprobar sin PEC	
Nota máxima que aporta el examen a la calificación final sin PEC	

Nota mínima en el examen para sumar la PEC

Comentarios y observaciones

CARACTERÍSTICAS DE LA PRUEBA PRESENCIAL Y/O LOS TRABAJOS

Requiere Presencialidad: No

Descripción

Se realizará al menos un trabajo y una prueba presencial.

Criterios de evaluación

Ambas pruebas (trabajo y examen) deberán aprobarse por separado, pero se podrá compensar nota entre ambos en algunos casos que se indicarán a comienzo del Curso.

Ponderación de la prueba presencial y/o los trabajos en la nota final: La Prueba Presencial valdrá un 60%, y el trabajo un 40% de la nota total.

Fecha aproximada de entrega: Antes de las pruebas presenciales del cuatrimestre correspondiente

Comentarios y observaciones

PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC?: No

Descripción

Criterios de evaluación

Ponderación de la PEC en la nota final

Fecha aproximada de entrega

Comentarios y observaciones

OTRAS ACTIVIDADES EVALUABLES

¿Hay otra/s actividad/es evaluable/s?: Si,no presencial

Descripción

Se elaborará un trabajo de análisis y síntesis de un caso práctico relacionado con los conceptos de la asignatura acompañado de recopilación y estudio de bibliografía en diferentes fuentes. Se proporcionará el enunciado completo a comienzo del curso.

El trabajo podrá realizarse en grupos si así lo indica el Equipo Docente.

Criterios de evaluación

La valoración dependerá de la profundidad, estructura, redacción y adecuación del trabajo al estado del arte.

Ponderación en la nota final: El trabajo supone un 40% de la nota de la asignatura.

Fecha aproximada de entrega

Comentarios y observaciones

¿CÓMO SE OBTIENE LA NOTA FINAL?

La asignatura se evalúa mediante el examen (prueba presencial) y el trabajo.
Ambos son obligatorios para aprobar la asignatura.
La nota del trabajo se guarda de junio a septiembre. La nota del examen no se guarda de una convocatoria para otra.
El cálculo de la nota de la asignatura será el siguiente: Nota del Examen * 0,6 + Nota del Trabajo * 0,4

BIBLIOGRAFÍA BÁSICA

La asignatura se basará en apuntes, presentaciones y material de clase que se ofrecerá desde la plataforma virtual.

BIBLIOGRAFÍA COMPLEMENTARIA

ISBN(13):9781484238707
Título:CYBERSECURITY INCIDENT RESPONSE
Autor/es:Eric C. Thompson ;
Editorial:APRESS

RECURSOS DE APOYO Y WEBGRAFÍA

Se proporcionará acceso a los documentos públicos del CCN disponibles para el estudio de algunos temas de la asignatura.

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.