MATERIALES DOCENTES DE LA ASIGNATURA INTRODUCCIÓN A LA CIBERSEGURIDAD

BLOQUES 1 Y 2: GUÍA DOCENTE DE LA ASIGNATURA GUÍAS DE ESTUDIO

CURSO ACADÉMICO 2022-2023

GRADO EN INGENIERÍA DE LA CIBERSEGURIDAD

Universidad Rey Juan Carlos

Marta Beltrán Pardo

Universidad Rey Juan Carlos

Grado en Ingeniería de la Ciberseguridad

Introducción a la Ciberseguridad

1. GUÍA DOCENTE DE LA ASIGNATURA

GUÍA DOCENTE

INTRODUCCION A LA CIBERSEGURIDAD

GRADO EN INGENIERÍA DE LA CIBERSEGURIDAD

CURSO 2022-23

Fecha de publicación: 10-07-2022

I.-Identificación de la Asignatura	
Tipo	OBLIGATORIA
Período de impartición	1 curso, 1Q semestre
Nº de créditos	6
Idioma en el que se imparte	Castellano

II.-Presentación

En esta asignatura trataremos la importancia de la ciberseguridad en la actualidad y el contexto en el que se trabaja en este campo en diferentes sectores, escenarios y dominios de aplicación. Para ello, realizaremos una introducción a la Informática que nos permita comprender los aspectos básicos de cualquier sistema informático actual (desde la representación de la información hasta el desarrollo de aplicaciones, pasando por conceptos básicos de estructura y arquitectura de computadores, sistemas operativos, compiladores, redes o Internet).
Una vez adquiridos estos conocimientos básicos ya podremos comprender la importancia de la confidencialidad, la integridad, la disponibilidad, el control de acceso y el no repudio así como conocer los conceptos de riesgo, amenaza y vulnerabilidad. Y analizar los más comunes en la actualidad para poder estudiar los distintos tipos de contramedidas, protecciones, controles o salvaguardas que se pueden diseñar y desplegar. Todo esto se estudiará en mucha mayor profundidad en las diferentes asignaturas que componen el plan de estudios del Grado, pero al finalizar el cuatrimestre los estudiantes tendrán una visión global de este campo y habrán adquirido las bases sobre las que se asentarán todas estas asignaturas en el futuro.

III.-Competencias

Competencias Generales

CG4. Capacidad para dirigir y liderar las actividades objeto de los proyectos del ámbito de la informática y la ciberseguridad comprendiendo los criterios de calidad que rigen dichas actividades investigadora y profesional.
CG7. Capacidad para evaluar y asegurar la confidencialidad, integridad y disponibilidad de los activos tecnológicos.
CG8. Capacidad para definir, evaluar y seleccionar contramedidas para la protección de los activos tecnológicos, entendiendo las peculiaridades de los distintos contextos en los que deben desplegarse.
CG15. Capacidad para aplicar conocimientos a su trabajo o vocación de una forma profesional. Capacidad para elaborar y defender argumentos y resolver problemas dentro de su aérea de estudio.
CG16. 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.
CG17. Capacidad para transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.
CG18. Capacidad para aplicar las habilidades de aprendizaje adquiridas necesarias para emprender estudios posteriores con un alto grado de autonomía.

Competencias Específicas

CE03. Conocer el concepto, marco institucional y jurídico, organización y gestión de la empresa, y en especial de aquellas que operan en el sector de la ciberseguridad.
CE13. Comprender y analizar las implicaciones que para la seguridad tiene desarrollar, desplegar y utilizar aplicaciones y servicios basados en tecnologías de red, incluyendo: Internet, web, comercio electrónico, multimedia, servicios interactivos, redes sociales, computación móvil, Internet de las cosas.
CE16. Conocer el concepto de ciberseguridad y sus pilares fundamentales e implicaciones en un contexto globalizado, tecnológico y conectado como el actual.
CE19. Comprender los algoritmos criptográficos de clave pública y de clave privada más importantes y conocer sus aplicaciones en ciberseguridad.

IV.-Contenido

IV.A.-Temario de la asignatura

Bloque	Unidad didáctica	Contenidos
I- Los fundamentos de la Informática y de la Seguridad	1. Bits y bytes	Representación de la información. Código binario, hexadecimal y ASCII. Imágenes y gráficos. ¿Qué es la criptografía? Esteganografía.
	2. La arquitectura de un computador	Tipos de computador. Modelo Von Neumann. Procesador, memoria y sistema de E/S. Lenguaje ensamblador.
	3. ¿Qué es la ciberseguridad?	Los pilares de la ciberseguridad: confidencialiad, integridad y disponibilidad. Conceptos de riesgo, amenaza y vulnerabilidad. Arquitecturas y principios de ciberseguridad. Contexto actual y escenarios**.**
II- Sistemas, aplicaciones y personas	4. El sistema operativo	Servicios del sistema operativo. Sistemas operativos actuales y evolución. Virtualización. Protección proporcionada por el sistema operativo. Control de accesos y autenticación.
	5. Compiladores y lenguajes de programación	El compilador. Necesidad de lenguajes de alto nivel y tipos. Instrucciones y datos. Algoritmos. Desarrollo de aplicaciones.
	6. El factor humano y el económico en ciberseguridad	Amenazas internas. Ingeniería social. Políticas y procedimientos. Modelos de negocio. Marco regulatorio.
III- Redes e Internet	7. Redes de comunicaciones e Internet	Modelos en capas. Pila de protocolos. Tipos de red. Redes de área local e Internet. La arquitectura cliente/servidor. El navegador.
	8. Bases de datos y repositorios de información	Sistemas de información. Sistema de ficheros vs bases de datos. Tipos de bases de datos. ¿Qué es SQL?
	9. Amenazas, ciberataques y protecciones	Principales amenazas en la actualidad. Tipos de atacante. Anatomía de un ataque. Incidentes y gestión de incidentes. Protecciones, contramedidas y salvaguardas.

	10. Privacidad y anonimato	Concepto de privacidad. Relación de la privacidad con la seguridad. Privacidad desde el diseño y en el despliegue. Técnicas de anonimato.

IV.B.-Actividades formativas	
Tipo	**Descripción**
Prácticas / Resolución de ejercicios	Práctica 1 - Bloque I de la asignatura
Prácticas / Resolución de ejercicios	Práctica 2 - Bloque II de la asignatura
Prácticas / Resolución de ejercicios	Práctica 3 - Bloque III de la asignatura
Otras	Evaluación continua- resolución de casos prácticos y pruebas

V.-Tiempo de Trabajo	
Clases teóricas	20
Clases prácticas de resolución de problemas, casos, etc.	18
Prácticas en laboratorios tecnológicos, clínicos, etc.	18
Realización de pruebas	4
Tutorías académicas	10
Actividades relacionadas: jornadas, seminarios, etc.	8
Preparación de clases teóricas	30
Preparación de clases prácticas/problemas/casos	32
Preparación de pruebas	40
Total de horas de trabajo del estudiante	180

VI.-Metodología y plan de trabajo

Tipo	Periodo	Contenido
Lecturas	Semana 1 a Semana 15	Apoyo en las clases teóricas y prácticas (noticias de actualidad, documentación introductoria, manuales, etc.)
Prácticas	Semana 4 a Semana 7	Práctica 2 - En grupo, asistencia obligatoria
Prácticas	Semana 8 a Semana 14	Práctica 3 - En grupo, asistencia obligatoria
Tutorías académicas	Semana 1 a Semana 15	Tutorías individuales/grupales acerca de todo el temario de la asignatura
Seminarios	Semana 1 a Semana 15	Jornadas o seminarios de interés para la asignatura
Clases Teóricas	Semana 1 a Semana 14	Contenidos teóricos de las unidades didácticas del programa de la asignatura
Prácticas	Semana 1 a Semana 3	Práctica 1 - En grupo, asistencia obligatoria
Pruebas	Semana 1 a Semana 15	Evaluación continua (resolución de casos prácticos y pruebas según se vaya avanzando en las unidades didácticas)

VII.-Métodos de evaluación

VII.A.-Ponderación para la evaluación

Evaluación ordinaria continua:
La distribución y características de las pruebas de evaluación son las que se describen a continuación. Solo en casos excepcionales y especialmente motivados, el profesor podrá incorporar adaptaciones en la Guía. Dichos cambios requerirán, previa consulta al Responsable de la Asignatura, la autorización previa y expresa del Coordinador de Grado, quien notificará al Vicerrectorado con competencias en materia de Ordenación Académica la modificación realizada. En todo caso, las modificaciones que se propongan deberán atender a lo establecido en la memoria verificada. Para que tales cambios sean efectivos, deberán ser debidamente comunicados a comienzo de curso a los estudiantes a través del Aula Virtual.
La suma de las actividades no revaluables no podrá superar el 50% de la nota de la asignatura y, en general, no podrán tener nota mínima (salvo en el caso de las prácticas de laboratorio o prácticas clínicas, cuando esté debidamente justificado), evitando incorporar pruebas que superen el 60% de la ponderación de la asignatura.
Evaluación extraordinaria: Los estudiantes que no consigan superar la evaluación ordinaria, o no se hayan presentado, serán objeto de la realización de una evaluación extraordinaria para verificar la adquisición de las competencias establecidas en la guía, únicamente de las actividades de evaluación revaluables.

Descripción de las pruebas de evaluación y su ponderación

Actividad de evaluación continua	Re-evaluable (podrá evaluarse en la convocatoria extraordinaria)	Ponderación	Pruebas	Nota mínima	Contenidos	Fecha
Pruebas escritas: Cuestiones de respuesta abierta	Sí, mediante una prueba con el mismo formato	40%	1	5	Todo el temario de la asignatura	Periodo de exámenes de la ETSII según calendario académico
Resolución de casos prácticos	Sí, mediante la entrega de los mismos casos	20% (cada caso un 10%)	2	4	Caso 1: Ética Caso 2: Factor humano	Semana 6 Semana 10
Prácticas con ordenador: Tests/informes y entrega/discusión de resultados	Sí, mediante la realización de las mismas prácticas	40% (un 10% las prácticas 1 y 2, el 20% restante la práctica 3)	3	4	Práctica 1: Bloque I del temario Práctica 2: Bloque II del temario Práctica 3: Bloque III del temario	Semanas 1-3 Semanas 4-7 Semanas 8-14
TOTAL		100%				

Se exigirá la nota mínima indicada en cada una de las partes para hacer media y poder aprobar la asignatura (nota media igual o superior a 5).

Las entregas de soluciones de casos y memorias de prácticas se realizará siempre a través de Aula Virtual, el resto de pruebas serán siempre presenciales. Las fechas concretas se anunciarán en el calendario de Aula Virtual con antelación suficiente.

Nota sobre las actividades

Si el estudiante debe presentarse a la convocatoria extraordinaria para re-evaluar alguna de las actividades de la tabla anterior (para llegar a las notas mínimas), se le guardará la nota de las que ya la hayan superado. No es posible presentarse a "subir nota" en ningún caso.

Normativa aplicable a la realización de las pruebas

En todas las pruebas de evaluación será necesario que el estudiante disponga de documentación identificativa (DNI, pasaporte, permiso de conducir o carnet de estudiante de la URJC) que le podrá ser requerida en cualquier momento. El estudiante se compromete a entregar siempre una solución propia y original así como a incluir, cuando se estime necesario, las referencias bibliográficas y las fuentes consultadas. El plagio total o parcial de las soluciones, o cualquier otro tipo de fraude académico, se penalizará aplicando la normativa de la URJC y se notificará a la ETSII.

VII.B.-Evaluación de estudiantes con dispensa académica de asistencia a clase

Para que un alumno pueda optar a esta evaluación, tendrá que obtener la 'Dispensa Académica de asistencia a clase' para la asignatura, que habrá solicitado al Decano/a o Director/a del Centro que imparte su titulación. La Dispensa Académica se podrá conceder siempre y cuando las peculiaridades propias de la asignatura lo permitan. Una vez que se haya notificado la concesión de la Dispensa Académica, el docente deberá informar al estudiante a través del Aula Virtual acerca del plan de evaluación establecido en cada caso.

Asignatura con posibilidad de dispensa: Si

VII.C.-Revisión de las pruebas de evaluación

Conforme a la normativa de reclamación de exámenes de la Universidad Rey Juan Carlos.

VII.D.-Estudiantes con discapacidad o necesidades educativas especiales

Las adaptaciones curriculares para estudiantes con discapacidad o con necesidades educativas especiales, a fin de garantizar la igualdad de oportunidades, no discriminación, la accesibilidad universal y la mayor garantía de éxito académico serán pautadas por la Unidad de Atención a Personas con Discapacidad en virtud de la Normativa que regula el servicio de Atención a Estudiantes con Discapacidad, aprobada por Consejo de Gobierno de la Universidad Rey Juan Carlos.
Será requisito para ello la emisión de un informe de adaptaciones curriculares por parte de dicha Unidad, por lo que los estudiantes con discapacidad o necesidades educativas especiales deberán contactar con ella, a fin de analizar conjuntamente las distintas alternativas.

VII.E.-Conducta Académica, integridad y honestidad académica

La Universidad Rey Juan Carlos está plenamente comprometida con los más altos estándares de integridad y honestidad académica, por lo que estudiar en la URJC supone asumir y suscribir los valores de integridad y la honestidad académica recogidos en el Código Ético de la Universidad (https://www.urjc.es/codigoetico). Para acompañar este proceso, la Universidad dispone de la Normativa sobre conducta académica de la Universidad Rey Juan Carlos (https://urjc.es/images/Universidad/Presentacion/normativa/Normativa_conducta_academica_URJC.pdf) y de diferentes herramientas (antiplagio, supervisión) que ofrecen una garantía colectiva para el completo desarrollo de estos valores esenciales.

VIII.-Recursos y materiales didácticos
Bibliografía
"Computing". Yoshihide Igarashi; Tom Altman; Mariko Funada; Barbara Kamiyama, Chapman and Hall/CRC (2014). ISBN: 978-1-4822-2741-3. Disponible en la plataforma de O'Reilly.
"Computer Security Fundamentals, Third Edition". Chuck Easttom. Pearson Certification (2016). ISBN: 978-0-13-447062-7. Disponible en la plataforma de O'Reilly.
"Computer &Internet Security: A Hands-on Approach, 3rd Edition". Wenliang Du (2019). ISBN: 978-17330039-4-0.
Bibliografía de consulta
Se proporcionarán enlaces a blogs, noticias, artículos, estándares, manuales y otros documentos de interés para las diferentes actividades que se realicen en la asignatura. Todo estará disponible a través del Aula Virtual.

IX.-Profesorado	
Nombre y apellidos	MARTA BELTRAN PARDO
Correo electrónico	marta.beltran@urjc.es
Departamento	Ciencias de la Computación, Arquitectura de Computadores, Lenguajes y Sistemas Informáticos y Estadística e Investigación Operativa
Categoría	Titular de Universidad
Titulación académica	Doctor
Responsable Asignatura	Si
Horario de Tutorías	Para consultar las tutorias póngase en contacto con el/la profesor/-a a través de correo electrónico
Nº de Quinquenios	4
Nº de Sexenios	2
Nº de Sexenios de transferencia	0
Tramo Docentia	5
Nombre y apellidos	MIGUEL CALVO MATALOBOS
Correo electrónico	miguel.calvo@urjc.es
Categoría	Profesional
Responsable Asignatura	No
Horario de Tutorías	Para consultar las tutorias póngase en contacto con el/la profesor/-a a través de correo electrónico

Nº de Quinquenios	0
Nº de Sexenios	0
Nº de Sexenios de transferencia	0
Tramo Docentia	0

2. GUÍA DE ESTUDIO DE LA ASIGNATURA

GUÍA DE ESTUDIO DE LA UNIDAD 1

Bits y bytes

Tiempo estimado de estudio fuera del aula: 4 horas

Material obligatorio de estudio para esta semana

1. Diapositivas de la Unidad 1.
2. Vídeos de la Unidad 1.
3. Píldora de Introducción a la Criptografía (MOOC): https://www.youtube.com/watch?v=AKFEWeKynd0
4. Guión de la Práctica 1.

Material complementario/optativo

Sistema binario – Truco de magia clásico:
https://lacienciaparatodos.wordpress.com/2010/01/02/experimento-truco-de-magia/
Clase de Introducción a la Esteganografía – Lección de Class4crypt:
https://www.youtube.com/watch?v=_5pwzv-0w5k

Autoevaluación (conceptos que deberían quedar claros tras esta semana de estudio)

1. ¿Qué tienen en común hoy en día un teléfono móvil, una lavadora, un coche y un robot de producción?
2. ¿Qué cuatro funciones esenciales realiza un sistema considerado "informático"?
3. ¿Qué es el hardware? ¿Qué es el software?
4. ¿Qué es un bit? ¿Qué es un byte?
5. ¿Cómo representas el número 275 (en base 10) en sistema binario? ¿Qué número es, en base 10, el número binario 101010111?
6. ¿Cómo representas este último número binario en sistema hexadecimal?
7. ¿Qué formatos estándar conoces para representar, en binario, un número entero o un número real en un computador?
8. ¿Qué formatos estándar conoces para representar, en binario, un carácter alfanumérico e un computador?
9. ¿Qué diferencias hay entre el formato ASCII y el Unicode?
10. ¿Cómo se representa el carácter 'Z' en código ASCII?
11. ¿Qué dos tipos de imágenes suelen distinguirse en función de cómo se representan en un computador? ¿En qué se diferencian?
12. ¿Qué es la criptografía y para qué se utiliza? Menciona al menos tres ejemplos de aplicaciones actuales.
13. ¿Qué características debe tener un buen criptosistema?
14. ¿Qué es la esteganografía y para qué se utiliza? Menciona al menos tres ejemplos de aplicaciones actuales.
15. ¿Qué características tiene un buen estego-medio?

GUÍA DE ESTUDIO DE LA UNIDAD 2

La arquitectura de un computador

Tiempo estimado de estudio fuera del aula: 4 horas

Material obligatorio de estudio para esta semana

1. Diapositivas de la Unidad 2.
2. Vídeos de la unidad 2.
3. Guión de la Práctica 1.

Material complementario/optativo

Lectura History of computing:
https://www.britannica.com/technology/computer/History-of-computing
Vídeo How Intel Makes Chips:
https://www.youtube.com/watch?v=4oQoZF_KRCc

Autoevaluación (conceptos que deberían quedar claros tras esta semana de estudio)

1. Resume brevemente la historia de los computadores resaltando los hitos que te parezcan más importantes.
2. ¿Atendiendo a qué criterios se te ocurre que se pueden clasificar los computadores actuales?
3. Dibuja el esquema de una placa base actual de un PC e identifica los componentes más importantes.
4. ¿Cuál es la estructura de un computador según el modelo Von Neumann? ¿Se sigue cumpliendo este modelo o ha evolucionado? Si es así, ¿en qué aspectos?
5. ¿Qué es el repertorio de instrucciones de un computador? ¿Qué tres tipos de instrucciones debe incluir?
6. ¿Debe un programador conocer estos repertorios de instrucciones a bajo nivel? Es más, ¿debe conocer la microarquitectura del procesador para el que programa? ¿Y un especialista en ciberseguridad, qué opinas?
7. ¿Qué diferencia hay entre los repertorios CISC y los RISC? ¿Cómo son las arquitecturas x86 actuales de Intel y AMD, CISC ó RISC?
8. ¿Qué pasos se siguen para ejecutar una instrucción en un núcleo de procesador RISC sencillo? Intenta recordar las cinco fases de ejecución con todas las tareas importantes que se realizan en cada una de ellas.
9. ¿Qué recursos hardware incluye la ruta de datos de un procesador RISC para poder ejecutar cada una de estas tareas?

GUÍA DE ESTUDIO DE LA UNIDAD 3

¿Qué es la ciberseguridad?

Tiempo estimado de estudio fuera del aula: 4 horas

Material obligatorio de estudio para esta semana

1. Diapositivas de la Unidad 3.
2. Vídeos de la Unidad 3.
3. Píldora Principios de la ciberseguridad en el contexto actual (MOOC) https://www.youtube.com/watch?v=LZkZZi7eR-0&t=1s
4. Píldora Enfoque actual para la ciberseguridad y su ciclo continuo (MOOC) https://www.youtube.com/watch?v=peY12L2qxos

Material complementario/optativo

En estos enlaces podéis encontrar material muy interesante para toda la asignatura:

https://www.enisa.europa.eu/
https://www.dhs.gov/topic/cybersecurity
https://www.incibe.es/
https://www.ccn.cni.es
https://csrc.nist.gov/
https://securityintelligence.com/
https://www.elladodelmal.com/
https://www.darkreading.com/
https://threatpost.com/
https://www.blackhat.com/ (conferencias)
https://www.defcon.org/ (conferencias)

Autoevaluación (conceptos que deberían quedar claros tras esta semana de estudio)

1. ¿Qué tres aspectos debe garantizar la Seguridad Informática? ¿Qué dos adicionales se pueden considerar también?
2. ¿Cuáles son las diferencias entre los conceptos de riesgo, amenaza y vulnerabilidad? Define primero cada uno de ellos, identifica las relaciones entre ellos e intenta poner ejemplos para que estas diferencias queden claras.
3. ¿Cuáles son las típicas causas de una vulnerabilidad?
4. ¿Qué es el CVE-ID de una vulnerabilidad?
5. ¿Qué proceso se sigue desde que una vulnerabilidad se descubre hasta que se resuelve?
6. ¿En qué consiste un ataque de zero-day?
7. ¿Qué es un exploit?
8. ¿Qué es el CVSS?
9. ¿Qué es un Bug Bounty?
10. ¿Qué es un CSIRT y cuáles son sus principales tareas?
11. Explica los conceptos de evento de seguridad, ataque e incidente; haciendo hincapié en la relación entre ellos.
12. ¿En qué principios se basa la Seguridad Informática actual y qué implica cada uno de ellos?

GUÍA DE ESTUDIO DE LA UNIDAD 4

El sistema operativo

Tiempo estimado de estudio fuera del aula: 4 horas

Material obligatorio de estudio para esta semana

1. Diapositivas de la Unidad 4.
2. Vídeos de la Unidad 4.
3. Guión de la Práctica 2.

Material complementario/optativo

En este link tenéis una serie de vídeoclases de Introducción a la Informática que Alberto Prieto y Beatriz Prieto, de la Universidad de Granada, han publicado generosamente: **https://atc.ugr.es/informacion/directorio-personal/alberto-prieto-espinosa/web/videoclases/fundamentos-informatica**

Tratan casi todos los temas básicos de Informática que veremos en esta asignatura, pero en concreto, os permiten profundizar algo más en este tema de sistemas operativos si queréis ir avanzando.

Autoevaluación (conceptos que deberían quedar claros tras esta semana de estudio)

1. ¿Qué servicios fundamentales proporciona el sistema operativo a las aplicaciones y a los usuarios en la actualidad?
2. ¿Todos los sistemas operativos siguen una misma estructura, existe una metodología estándar de diseño? ¿Cómo afecta esto al trabajo de los ingenieros en ciberseguridad sea cual sea su función/perfil?
3. ¿Cómo se implementan los sistemas operativos actuales, en ensamblador o en lenguajes de alto nivel? De nuevo ¿qué implicaciones tiene esto en la seguridad de los sistemas operativos?
4. ¿Qué es el kernel de un sistema operativo?
5. Explica la evolución que se ha seguido en cuanto al diseño de los sistemas operativos, incidiendo en el tipo de diseño que se utiliza para los sistemas de Microsoft, los UNIX/Linux y los de Apple.
6. ¿Qué son las llamadas al sistema y para qué sirven? ¿Por qué se suelen relacionar con APIs?
7. ¿Qué tipos de interfaz de usuario suelen incorporar los sistemas operativos actuales?
8. ¿Qué es la virtualización, para qué sirve y qué tipos conoces?
9. ¿Qué es un hipervisor y cuál es su función principal en la virtualización de máquina?
10. ¿En qué se diferencian un hipervisor de tipo I y uno de tipo II?

GUÍA DE ESTUDIO DE LA UNIDAD 5

Protección vs Seguridad

Tiempo estimado de estudio fuera del aula: 4 horas

Material obligatorio de estudio para esta semana

1. Diapositivas de la Unidad 5.
2. Píldora Sistemas Operativos de Confianza (MOOC)
   https://www.youtube.com/watch?v=MlVw9cgOJcE
3. Guión de la Práctica 2.

Material complementario/optativo

Lectura "Easy Ways to Build a Better P@$5w0rd" (NIST)
https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd

Autoevaluación (conceptos que deberían quedar claros tras esta semana de estudio)

1. Intenta explicar los conceptos de protección y seguridad, diferenciándolos claramente y relacionándolos con los sistemas operativos.
2. ¿Qué cuatro tipos de separación se suelen emplear en los sistemas operativos actuales para garantizar la protección?
3. ¿Qué tipo de recursos tiene que proteger el sistema operativo? ¿Qué grados de separación/compartición se pueden utilizar para ello?
4. ¿Qué diferencia hay entre el control de acceso MAC y el DAC?
5. ¿Qué mecanismos de control de acceso son más habituales? Explica cómo funcionan y sus ventajas e inconvenientes.
6. ¿En qué consiste el RBAC o Role Based Access Control?
7. ¿En qué consiste el proceso de autenticación de un usuario por parte de un sistema operativo? ¿Por qué es necesario?
8. ¿Qué alternativas tenemos para construir estos procesos de autenticación?
9. ¿Qué normas son básicas para la construcción/mantenimiento de una contraseña segura?
10. ¿Qué es un sistema operativo de confianza? ¿Conoces alguno? ¿Con qué nivel de seguridad?

GUÍA DE ESTUDIO DE LA UNIDAD 6

Compiladores y lenguajes de programación

Tiempo estimado de estudio fuera del aula: 1.5 horas

Material obligatorio de estudio para esta semana

1. Diapositivas de la Unidad 6.

Material complementario/optativo

Vídeo "Machine Code and High level Languages Using Interpreters and Compilers"
https://www.youtube.com/watch?v=1OukpDfsuXE

Autoevaluación (conceptos que deberían quedar claros tras esta semana de estudio)

1. ¿Qué diferencias hay entre los lenguajes de bajo nivel de tipo ensamblador y los de alto nivel?
2. ¿Qué diferencias hay entre un lenguaje compilado y uno interpretado?
3. ¿Qué es un compilador y cómo funciona?
4. ¿Cuáles son las causas más habituales de los bugs o vulnerabilidades de código? Menciona algunas mejores prácticas que podrían ayudar a reducir su número.
5. ¿Qué tipos de análisis de código conoces y en qué se diferencian?

GUÍA DE ESTUDIO DE LA UNIDAD 7

El factor humano en la ciberseguridad

Tiempo estimado de estudio fuera del aula: 4 horas

Material obligatorio de estudio para esta semana

1. Diapositivas de la Unidad 7.
2. Vídeo de concienciación (MOOC, Premio al mejor vídeo educativo en el Día de Internet) https://www.youtube.com/watch?v=kvbYbsGoofo&t=4s
3. Material para el Caso 1.

Material complementario/optativo

Lectura sobre ingeniería social
https://www.sba-research.org/wp-content/uploads/publications/jisa_revised.pdf
Lectura sobre cibercrimen (Internet Organised Crime Threat Assessment, IOCTA)
https://www.europol.europa.eu/publications-events/main-reports/iocta-report

Autoevaluación (conceptos que deberían quedar claros tras esta semana de estudio)

1. ¿Por qué solemos decir que las personas somos el eslabón más débil en ciberseguridad? ¿A qué nos referimos cuando decimos que la seguridad por oscuridad no funciona?
2. ¿Qué es un Insider Threat? ¿Cómo pretende lidiar con esta amenaza un ITP?
3. ¿En qué consiste la ingeniería social? ¿Cuáles suelen ser sus objetivos? Menciona las técnicas de ingeniería social que conozcas.
4. ¿Cómo combatirías este tipo de técnicas?
5. ¿Qué es el phishing y qué pretende? ¿Qué tipos específicos de phishing conoces?
6. ¿Qué es un CIO o CISO y cuáles son sus principales responsabilidades?
7. ¿Qué es un Plan Director de Seguridad y cómo se define?
8. ¿Qué es una política de seguridad y para qué sirve? Explica qué partes la componen y menciona alguna típica que suelan tener definida casi todas las organizaciones.
9. ¿Qué tipo de cibercriminales conoces según la tarea que realizan? ¿Qué tipos de modelos de negocio?
10. ¿En qué consiste el cibercrimen como servicio y por qué está de actualidad?
11. ¿Qué es un delito informático?
12. ¿Cuál es el marco regulatorio de la ciberseguridad en España? Menciona las principales leyes o normas que aplican en la actualidad y su ámbito.

GUÍA DE ESTUDIO DE LA UNIDAD 8

Redes de comunicaciones e Internet

Tiempo estimado de estudio fuera del aula: 6 horas

Material obligatorio de estudio para esta semana

1. Diapositivas de la Unidad 8.
2. Guión de la Práctica 3.

Material complementario/optativo

Lectura sobre el funcionamiento, en profundidad, de un navegador web:
https://www.html5rocks.com/en/tutorials/internals/howbrowserswork/#The_rendering_engine
Tutorial de HTML:
https://www.w3schools.com/html/default.asp
Tutorial de PHP:
https://www.w3schools.com/php/default.asp

Autoevaluación (conceptos que deberían quedar claros tras esta semana de estudio)

1. ¿Por qué se habla de una pila de protocolos? ¿Qué ventajas tienen los modelos por capas que utilizamos, por ejemplo, para organizar los protocolos en los que se basa el funcionamiento de Internet? ¿Qué capas propone distinguen los protocolos TCP/IP? ¿De qué se encarga cada una de ellas?
2. ¿En qué capas están los protocolos SMTP, TCP, UDP, IP y ARP?
3. ¿Qué es un puerto y para qué sirve?
4. ¿Qué nombres, identificadores o direcciones se utilizan en TCP/IP y a qué nivel está cada uno de ellos?
5. ¿Qué distingue a una red de área local de una de área extensa como Internet?
6. ¿En qué consiste la arquitectura cliente/servidor que da soporte a Internet?
7. ¿Qué es HTTP y para qué sirve? ¿Cómo funciona?
8. ¿Qué son las cookies y para qué se usan?
9. Intenta resumir los pasos que se siguen desde que tecleas una dirección en la barra de herramientas de tu navegador hasta que se te muestran los contenidos de esa página web (desde el punto de vista de las redes y los protocolos de comunicaciones).
10. ¿Qué es un navegador web y para qué sirve? ¿Por qué necesitamos este tipo de aplicación? ¿Qué módulos los componen?
11. ¿Qué es HTML y para qué sirve?
12. Intenta explicar en una frase o dos cada uno de los siguientes paradigmas: NFV, Cloud Computing, Internet of Things.¿Qué es un sistema de información y para qué sirve? ¿Qué tipo de actividades suele realizar?

GUÍA DE ESTUDIO DE LA UNIDAD 9

Bases de datos y repositorios de información.

Tiempo estimado de estudio fuera del aula: 4 horas

Material obligatorio de estudio para esta semana

1. Diapositivas de la Unidad 9.
2. Guión de la Práctica 3.

Material complementario/optativo

Tutorial de SQL
https://www.w3schools.com/sql/
Píldora Inyección SQL (MOOC)
https://www.youtube.com/watch?v=qSzU2RW882I

Autoevaluación (conceptos que deberían quedar claros tras esta semana de estudio)

1. ¿Qué es un ERP? ¿Y un CRM?
2. ¿Dónde se almacena el sistema de ficheros y qué software se encarga de gestionarlo?
3. ¿Qué es un directorio dentro de un sistema de ficheros y cómo se gestiona y organiza?
4. ¿Cuándo se utiliza un sistema de ficheros para almacenar la información y cuándo es mejor recurrir a una base de datos?
5. ¿Qué es una base de datos? ¿Y un SGBD?
6. ¿Cómo es el modelo de base de datos relacional, por qué se caracteriza?
7. ¿Qué es SQL y para qué sirve?
8. ¿A qué nos referimos cuando utilizamos el término Big Data?
9. ¿Qué tipo de repositorios para almacenamiento de información se utilizan en entornos Big Data?

GUÍA DE ESTUDIO DE LA UNIDAD 10

Amenazas y ciberataques

Tiempo estimado de estudio fuera del aula: 6 horas

Material obligatorio de estudio para esta semana

1. Diapositivas de la Unidad 10.
2. ENISA ETL (última versión publicada).
3. OWASP Top 10.
4. MITRE ATT&CK
5. Material para el Caso 2.

Material complementario/optativo

Para completar el tema de recogida de información podéis:

- Ver este vídeo (alrededor de 40 minutos en inglés): https://www.youtube.com/watch?v=d7x-Bn_bqt0
- Leer esta entrada del blog de Incibe: https://www.incibe-cert.es/blog/osint-la-informacion-es-poder
- Investigar en el framework que hemos visto en clase: http://osintframework.com/

Autoevaluación (conceptos que deberían quedar claros tras esta semana de estudio)

1. ¿Qué amenazas de seguridad preocupan más en la actualidad?
2. Explica brevemente qué es el malware, qué tipos de malware hay y qué mecanismos distinguen a unos de otros.
3. ¿Qué significa el acrónimo APT? ¿Qué tipo de amenaza es y qué la caracteriza?
4. ¿A qué pilar de la seguridad amenaza una brecha de datos? ¿Y una denegación de servicio?
5. ¿Qué es STRIDE y para qué sirve? Explica este modelo brevemente.
6. ¿Qué tipos de atacantes o adversarios se distinguen en la actualidad?
7. ¿Por qué fases atraviesa un ataque a la seguridad? Explica brevemente cada una de ellas.
8. ¿Qué diferencia hay entre el footprinting y el fingerprinting?
9. ¿Cuáles son las principales técnicas de footprinting? ¿Y de fingerprinting?
10. ¿Qué es Shodan y para qué se utiliza?
11. ¿Por qué los atacantes suelen buscar el anonimato? ¿Qué tipo de técnicas utilizan?
12. ¿Cómo se consigue el anonimato mediante el uso de un proxy?
13. ¿Qué son Tor, FreeNet y I2P?
14. ¿Qué tipos de ataque puedes distinguir en función de su acción/objetivo?
15. ¿En qué base de datos puedes encontrar los patrones de ataque conocidos en la actualidad clasificados por mecanismo de ataque o por dominio?

GUÍA DE ESTUDIO DE LA UNIDAD 11

Privacidad

Tiempo estimado de estudio fuera del aula: 2 horas

Material obligatorio de estudio para esta semana

1. Diapositivas de la Unidad 11.

Material complementario/optativo

Todos los recursos en la página web de la Agencia Española de Protección de datos pueden ser interesantes para completar:

https://www.aepd.es/es

Lecturas sobre casos o contextos concretos:

https://theconversation.com/por-que-nos-preocupa-solo-pegasus-si-estamos-constantemente-vigilados-184872

https://theconversation.com/edificios-y-coches-inteligentes-el-reto-de-la-privacidad-172529

https://theconversation.com/el-precio-que-pagamos-por-iniciar-sesion-con-facebook-o-google-en-las-aplicaciones-141851

https://theconversation.com/clases-por-internet-garantizan-la-privacidad-de-los-menores-138040

Autoevaluación (conceptos que deberían quedar claros tras esta semana de estudio)

1. ¿Qué es la privacidad? ¿es lo mismo que la intimidad?
2. ¿Qué son los datos personales? ¿Y a qué se refiere el acrónimo PII?
3. ¿Qué tipo de impactos puede tener una amenaza a la privacidad en las personas?
4. ¿Cómo se relacionan los conceptos de privacidad, protección de datos y seguridad?
5. ¿Qué estrategias de privacidad desde el diseño conoces?
6. ¿Y de privacidad en el despliegue?
7. ¿Qué otras estrategias, más relacionadas con la ciberseguridad, se deben tener en cuenta para evitar que se materialicen amenazas para la privacidad?
8. ¿Crees que los riesgos para la privacidad se analizan y gestionan igual que los riesgos para la seguridad, siguiendo los mismos métodos y aplicando las mismas herramientas?