GUÍA DOCENTE 2023/24

Centro	363 - Escuela de Ingeniería de Bilbao	**Ciclo**	Indiferente
Plan	GIIGSI30 - Grado en Ingeniería Informática de Gestión y Sistemas de Informa	**Curso**	3er curso

ASIGNATURA

26025 - Sistemas de Gestión de Seguridad de Sistemas de Información — **Créditos ECTS :** 6

DESCRIPCIÓN Y CONTEXTUALIZACIÓN DE LA ASIGNATURA

Los Sistemas de Información, entre los cuales podemos incluir los equipos informáticos, las redes y los soportes de datos, son los encargados de trabajar con la información sensible de cualquier organización. Estos Sistemas de Información se ven amenazados por riesgos y amenazas que pueden tener distintos orígenes. Podemos encontrar riesgos físicos como los daños causados por una catástrofe natural, o por un acceso no autorizado a la información; y riesgos lógicos generados por un ataque informático como un virus, ataques de denegación de servicios, etc.

En esta asignatura se estudiarán los distintos riesgos a los que se puede ver sometida la información y los sistemas que la contienen, para conocerlos en profundidad y de este modo poder llegar a controlarlos y minimizar su impacto.

COMPETENCIAS / RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA

Capacidad para integrar soluciones de tecnologías de la información y comunicaciones y procesos empresariales para satisfacer las necesidades de información de las organizaciones, permitiéndoles alcanzar sus objetivos de forma efectiva y eficiente, dándoles así ventajas competitivas.

Capacidad para determinar los requisitos de los sistemas de información y comunicación de una organización atendiendo a aspectos de seguridad y cumplimiento de la normativa y la legislación vigente.

Capacidad para participar activamente en la especificación, diseño, implementación y mantenimiento de los sistemas de información y comunicación.

Capacidad para comprender y aplicar los principios de la evaluación de riesgos y aplicarlos correctamente en la elaboración y ejecución de planes de actuación.

CONTENIDOS TEÓRICO-PRÁCTICOS

TEMA 1.- Introducción
En este tema se analizarán los riesgos de seguridad a los que se enfrenta una organización y se estudiará la forma de evaluar y estimar el impacto que dichos riesgos pueden tener.

BLOQUE I - Cifrado

TEMA 2.- Introducción al cifrado
El principal objetivo del cifrado de la información es su protección. En este tema se abordarán las ideas básicas sobre cifrado, así como su historia.

TEMA 3.- Cifrado simétrico
Algoritmos más comunes y sus aplicaciones.

TEMA 4.- Cifrado asimétrico
Algoritmos más comunes y sus aplicaciones.

TEMA 5.- Comunicaciones seguras
Aplicación de cifrado en comunicaciones seguras: certificados, conexiones SSH, etc.

TEMA 6.- Bitcoin
Bitcoin es una aplicación interesante del cifrado, así como de otros conceptos como las bases de datos distribuidas. Se ofrecerá una introducción técnica básica a Bitcoin y su Blockchain.

BLOQUE II - Sistemas

TEMA 7.- Backups
Las copias de seguridad aseguran la completitud de la información y su usabilidad en caso de pérdida de la información original. En este tema se estudiarán distintas formas y sistemas de realizar copias de seguridad.

TEMA 8.- Seguridad física
De nada sirve tener un sistema de información protegido contra todo tipo de riesgos lógicos, si cualquiera puede acceder físicamente a él y manipularlo. La seguridad física de los sistemas de información y de los datos es imprescindible.

TEMA 9.- Seguridad en redes
La información pocas veces está aislada en una máquina sin conexión a ninguna red. La toma de medidas de seguridad para la protección de las redes de comunicación es un paso imprescindible para asegurar la información.

TEMA 10.- Seguridad en Sistemas Web
Cada día más y más datos se encuentran en sistemas conectados a la Web a los cuales se puede tener acceso desde cualquier punto del planeta. Hay muchos aspectos de la seguridad que se deben tener en cuenta en la propia implementación de dichos sistemas para evitar los accesos no deseados.

BLOQUE III - Sociedad

TEMA 11.- El factor humano
A lo largo de este tema se estudiará la ingeniería social y distintas formas de proteger la información de las personas, ya que muchas veces son el eslabón más débil de la cadena de protección de la información.

TEMA 12.- Malware
¿Qué es el código malicioso (malware)? ¿Cómo se puede detectar y evitar? En este tema se verán las principales formas de protegerse del software malicioso y de sus efectos. Para ello se estudiará qué tipos de malware existen, las características de cada uno de ellos y sus efectos en los sistemas de información.

TEMA 13.- Legislación
En el campo de la seguridad informática es imprescindible conocer la legislación vigente en dicho área. En este tema se analizarán las leyes más importantes que se encuentren en vigor y sus efectos sobre los sistemas de información.

TEMA 14.- Informática forense
En este tema se estudiarán los procedimientos para la autopsia de un equipo informático.

TEMA 15.- Charlas (A definir)
Charlas sobre Bitcoin, Pentest, etc. por expertos de la industria

METODOLOGÍA

Las clases magistrales (M) se emplearán principalmente para la exposición de los conceptos teóricos asociados a la seguridad informática y a la resolución de dudas que planteen los alumnos. Sin embargo, en algunas clases magistrales y en algunas de Prácticas de Ordenador (PO) se reforzarán dichos conceptos mediante la resolución de ejercicios, bien individualmente o en grupos reducidos. Se recomienda el uso del ordenador portátil en clase, especialmente con un sistema operativo GNU/Linux.

Las clases de tipo PO que no se utilicen para la resolución de ejercicios, se emplearán para aplicar la metodología activa de Aprendizaje Basado en Problemas. Cada cierto tiempo se les proporcionará a los alumnos una serie de ejercicios que podrán trabajar de manera individual o grupal.

TIPOS DE DOCENCIA

Tipo de Docencia	M	S	GA	GL	GO	GCL	TA	TI	GCA
Horas de Docencia Presencial	45				15				
Horas de Actividad No Presencial del Alumno/a	67,5				22,5				

Leyenda:
M: Magistral — S: Seminario — GA: P. de Aula
GL: P. Laboratorio — GO: P. Ordenador — GCL: P. Clínicas
TA: Taller — TI: Taller Ind. — GCA: P. de Campo

SISTEMAS DE EVALUACIÓN

- Sistema de evaluación continua
- Sistema de evaluación final

HERRAMIENTAS Y PORCENTAJES DE CALIFICACIÓN

- Prueba escrita a desarrollar 10%
- Prueba tipo test 20%
- Realización de prácticas (ejercicios, casos o problemas) 30%
- Trabajos en equipo (resolución de problemas, diseño de proyectos) 40%

CONVOCATORIA ORDINARIA: ORIENTACIONES Y RENUNCIA

En la convocatoria ordinaria, por defecto, el alumnado está acogido al sistema de evaluación continua, aunque existe la opción de acogerse a la evaluación final indicándolo por email en cualquier momento, con el límite de dos semanas antes de la fecha último parcial.

En el sistema de evaluación continua la evaluación se dividirá en tres partes, cada una de ellas con un examen teórico y otro práctico, cuyas calificaciones harán media. Cada examen tratará sobre la materia vista en clase y los informes de laboratorio realizados hasta esa fecha y desde el examen anterior.

Además, a lo largo del cuatrimestre se realizarán una serie de trabajos que influirán en la calificación final de la asignatura en distinta medida.

En el sistema de evaluación final habrá un único examen teórico y otro práctico que se corresponderán con todo el temario de la asignatura. La calificación final de la asignatura se calculará mediante la media aritmética de ambos exámenes.

EVALUACIÓN DE TRABAJOS:

La detección de un plagio en cualquier parte de un trabajo supondrá una nota de 0 en dicho trabajo.
Los trabajos tienen que estar escritos correctamente, por lo que en el momento que se detecte la tercera falta ortográfica grave se dejará de corregir dicho trabajo y su nota será la correspondiente a la parte del mismo que ha sido evaluada.

CASOS DE COPIA:

Si se detecta una copia entre trabajos de dos grupos distintos, ambos trabajos serán evaluados con 0. En el caso de los exámenes se aplicará el artículo 11.3 de la Normativa reguladora de la Evaluación del Alumnado en las titulaciones oficiales de Grado.

RENUNCIA A LA CONVOCATORIA:

Para renunciar a la convocatoria y figurar como "No Presentado" en el modo de evaluación continua basta con no presentarse al último parcial. En el modo de evaluación final, es suficiente con no presentarse al examen final.

CONVOCATORIA EXTRAORDINARIA: ORIENTACIONES Y RENUNCIA

El alumnado que no superen la asignatura en su convocatoria ordinaria tendrá que realizar un examen teórico y otro práctico en la convocatoria extraordinaria sobre el temario completo de la asignatura. El alumnado que hubiera seguido el sistema de evaluación continua tendrá la posibilidad de indicar en el propio examen si desea que la calificación final de la asignatura se calcule usando únicamente las calificaciones de los exámenes o si quiere que se tenga en cuenta la nota de los trabajos realizados a lo largo del cuatrimestre.

RENUNCIA A LA CONVOCATORIA:

En caso de no realizar el examen teórico o el práctico se obtendrá una valoración de "No Presentado".

MATERIALES DE USO OBLIGATORIO

Notas de clase, material de soporte a la docencia en aula y laboratorios.

BIBLIOGRAFÍA

Bibliografía básica

Enciclopedia de la Seguridad Informática 2ª edición, Álvaro Gómez Vieites, RAMA 2011

Bibliografía de profundización

The governance of privacy. C.J. Bennett y C.D. Raab, Massachussets Institute of Technology Press 2006
Beyond Fear. B. Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World; 2006; Springer
Vigilancia permanente. Edward Snowden. Planeta, 2019
Social Engineering: The Science of Human Hacking. Christopher Hadnagy, Wiley 2018
El pequeño libro rojo del activista en la red. Marta Peirano, Roca 2015
Grokking Bitcoin. Kalle Rosenbaum, Manning 2019

Revistas

Auditoría + Seguridad informática
IEEE Security & Privacy

Direcciones de internet de interés

Blog de Bruce Schneier sobre seguridad (Accedido el 12/05/2022)

https://www.schneier.com/

Agencia Española de Protección de Datos (Accedido el 12/05/2022)
http://www.agpd.es

Red temática de criptografía y seguridad de la información (Accedido el 12/05/2022)
http://www.criptored.upm.es

Equipo de seguridad de rediris (Accedido el 12/05/2022)
http://www.rediris.es/cert/

Instituto nacional de ciberseguridad (Accedido el 12/05/2022)
https://www.incibe.es/

Blog sobre seguridad (Accedido el 12/05/2022)
https://krebsonsecurity.com

Malware scanner (Accedido el 12/05/2022)
https://www.virustotal.com

OBSERVACIONES

Si un trabajo es calificado con un 0 por razones de plagio, la asignatura será suspendida en su convocatoria ordinaria.