Seguridad de la información y gestión de riesgos tecnológicos empresariales

Curso Académico: (2020 / 2021) **Fecha de revisión: 23-06-2020**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: GONZALEZ MANZANO, LORENA

Tipo: Optativa Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 2

MATERIAS QUE SE RECOMIENDA HABER SUPERADO

Ninguna

RESULTADOS DEL APRENDIZAJE Y COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE.

Se definen los siguientes objetivos en términos de resultados de aprendizaje, acorde al nivel de Máster definido en el RD 1027/2011, de 15 de julio.

Por lo que se refiere a los CONOCIMIENTOS, al finalizar el curso el estudiante será capaz de:
1a. Conocer y comprender los objetivos de la seguridad de la información.
1b. Conocer y comprender las amenazas que sufre la información y las vulnerabilidades de los sistemas que la tratan.
1c. Conocer y comprender cómo las técnicas de análisis de datos masivos pueden servir para protegerse frente a las citadas amenazas y vulnerabilidades
1d. Conocer y comprender cómo aplicar las técnicas de análisis de datos masivos para evaluar el nivel de riesgo dinámico de un sistema basado en tecnologías de la información.

Por lo que atañe a las COMPETENCIAS adquiridas, el alumno será capaz de:
2a. Identificar las vulnerabilidades y amenazas que sufren los sistemas de información digital.
2b. Investigar las principales amenazas y vulnerabilidades de la información almacenada o procesada en un sistema en cierto entorno concreto.
2c. Encontrar y seleccionar las técnicas de análisis de datos masivos para proteger un sistema de información, considerando también el marco legal aplicable.
2d. Aplicar técnicas de análisis de datos masivos para determinar el nivel de riesgo de un sistema basado en TIC.
2e. Investigar y elaborar documentos técnicos sobre los aspectos de seguridad en entornos nuevos y objeto de estudio.
2f. Asumir la responsabilidad en el ámbito profesional de tareas de investigación, evaluación e implantación de medidas y mecanismos de análisis de datos masivos con fines de aseguramiento y evaluación de nivel de riesgo.

En cuanto a las ACTITUDES, el alumno tras cursar el curso debería tener:
3a. Una actitud crítica respecto de la aplicación de técnicas de análisis de datos masivos para la seguridad
3b. Una actitud de colaboración y de conocimiento que le permita obtener de otros profesionales la documentación y los datos necesarios para analizar y evaluar los riesgos de los sistemas de información.
3c. Una actitud favorable al trabajo en equipo que permita coordinar los distintos puntos de vista (legales, operativos, procedimentales) de los actores implicados en la protección de los sistemas TIC.

El objetivo principal es que el estudiante aprenda cómo aplicar los mecanismos de análisis de datos masivos con fines de seguridad y privacidad. Subordinado a este objetivo global, el estudiante deberá ser capaz de elegir la técnica más adecuada teniendo en cuenta la meta a alcanzar (e.g. proteger un sistema, reaccionar frente a un incidente, evaluar el nivel de riesgo) y las restricciones existentes (e.g. datos disponibles, aspectos legales u organizacionales).

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

El programa se divide en cinco grandes bloques:

1. Conceptos básicos de la seguridad de la información
Se realiza una introducción a la seguridad informática, exponiendo conceptos necesarios para el

aseguramiento de la información en el ámbito del Big Data y los sistemas corporativos.

2. Fuentes de datos en seguridad
Se introducirán las herramientas y técnicas la obtención de datos de seguridad y su posterior procesamiento. Así, será posible monitorizar el estado de seguridad de una red empresarial y detectar posibles amenazas.

3. Análisis de datos aplicados a seguridad
Se presentarán a los SIEM como herramienta para la gestión de eventos de seguridad a gran escala, a la vez que se vinculará su uso con las fuentes de información aprendidas anteriormente. Asimismo, se introducirá la importancia de la gestión de logs en los sistemas como método de análisis y mejora de la seguridad de los mismos.

4. Visualización de datos en seguridad
Se presentarán las técnicas y herramientas que permiten visualizar de forma eficaz el estado de seguridad y los riesgos existentes en una red corporativa de grandes dimensiones.

5. Privacidad y aspectos legales.
Se presentarán las principales técnicas para la protección de la privacidad en las fases de análisis de datos, sanitización y recuperación de información. Asimismo, se abordarán las principales directrices legales que afectan al tratamiento de datos masivos, con énfasis en las disposiciones que afectan a su realización en entornos corporativos

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

La metodología docente incluirá:
(1) Sesiones teóricas y material docente, donde se presentarán los conocimientos que los alumnos deben adquirir. Para facilitar su desarrollo los alumnos recibirán las notas de clase y diversos documentos en la herramienta web oportuna y tendrán textos básicos de referencia que les permitan completar y profundizar en aquellos temas en los cuales estén más interesados. (1.5 ECTS)
(2) Planteamiento, resolución por los alumnos y discusión posterior de casos reales de procesos y prácticas de seguridad de la información que servirán para ilustrar lo expuesto en las clases teóricas. (1.5 ECTS)
Las sesiones teóricas están orientadas fundamentalmente a la consecución de los objetivos de conocimiento, mientras que las prácticas y resolución de problemas tratan de desarrollar las competencias actitudinales y destrezas generales.

SISTEMA DE EVALUACIÓN

El alumno será evaluado atendiendo a la relación de descriptores (1a-1d) definidos como objetivos en la adquisición de conocimientos de esta asignatura, así como a la relación de descriptores (2a-2f) definidos como objetivos de competencias adquiridas y descriptores (3a-3c) relativos a las actitudes.

Se establece el siguiente sistema de evaluación:
1. Convocatoria ordinaria - evaluación continua

Examen final (40% de la nota final)
- La nota mínima será de 5.0 para superar la asignatura

Trabajos periódicos (60% de la nota final)
- De carácter individual o por grupos, según se anuncie al comienzo de la asignatura. Deberán entregarse todos los trabajos. En caso contrario, se aplicará lo dispuesto para la evaluación no continua.

2. Convocatoria ordinaria - evaluación no continua
Examen final (100% de la nota final)
- La calificación máxima obtenible será de 6 puntos
- Será necesario obtener 5 puntos para superar la asignatura.
- El examen contendrá ejercicios específicos para comprobar la adquisición de competencias relativas a los trabajos.

3. Convocatoria extraordinaria
La calificación de los estudiantes en la convocatoria extraordinaria se ajustará a las siguientes reglas:

a. Si el estudiante siguió el proceso de evaluación continua, el examen tendrá el mismo valor porcentual que en la convocatoria ordinaria, y la calificación final de la asignatura tendrá en cuenta la nota de la evaluación

continua y la nota obtenida en el examen final.
b. Si el estudiante no siguió el proceso de evaluación continua, tendrá derecho a realizar un examen en la convocatoria extraordinaria con un valor del 100 % de la calificación total de la asignatura. No obstante lo anterior, cuando las características de los ejercicios de la evaluación continua lo permitan, el profesor podrá autorizar al estudiante su entrega en la convocatoria extraordinaria, evaluándose en tal caso la asignatura del mismo modo que en la convocatoria ordinaria.
c. Aunque el estudiante hubiera seguido el proceso de evaluación continua, tendrá derecho a ser calificado en la convocatoria extraordinaria teniendo en cuenta únicamente la nota obtenida en el examen final cuando le resulte más favorable.

Peso porcentual del Examen Final:	40
Peso porcentual del resto de la evaluación:	60

BIBLIOGRAFÍA BÁSICA

- James R. Kalyvas; Michael R. Overly Big Data, CRC Press, 2015
- Matt Bishop Computer Security: Art and Science, Addison-Weley, 2003
- Petra Saskia Bayerl; Andrew Staniforth; Richard Hill; Hamid R. Arabnia; Gregory B. Saathoff; Babak Akhgar Application of Big Data for National Security, Butterworth-Heinemann, 2010
- Terence Craig; Mary E. Ludloff Privacy and Big Data, O'Reilly Media, 2011
- Xu, L., Jiang, C., Wang, J., Yuan, J., & Ren, Y. Information security in big data: privacy and data mining, IEEE Access, 2014

BIBLIOGRAFÍA COMPLEMENTARIA

- Mark Talabis; Robert McPherson; I Miyamoto; Jason Martin Information Security Analytics, Syngress, 2013
- Mark Van Rijmenam Think Bigger, AMACOM, 2014
- Mohamed Gaber; Sherif Sakr Large Scale and Big Data, CRC Press, 2013

RECURSOS ELECTRÓNICOS BÁSICOS

- VVAA . Big data analysis, how to turn big data into big money, Ch. 7: https://www.safaribooksonline.com/library/view/big-data-analytics/9781118239049/xhtml/Chapter07.html