Guía de Asignatura

ASIGNATURA: MONITORIZACIÓN Y DATA MINING

Título: *MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD*
Materia: *Gobierno y gestión de la tecnologías de la información*
Créditos: *6 ECTS*
Código: *03MCYB*

Índice

1. Organización general

1.1. Datos de la asignatura

TITULACIÓN	*MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD*
ASIGNATURA	*MONITORIZACIÓN Y DATA MINING*
CÓDIGO - NOMBRE ASIGNATURA	*03MCYB_MONITORIZACION_Y_DATA_MINING*
Carácter	Obligatorio
Cuatrimestre	Primero
Idioma en que se imparte	Castellano
Requisitos previos	No existen
Dedicación al estudio por ECTS	**25 horas**

1.2. Introducción a la asignatura

Detrás de cada infraestructura de TI, detrás de los sistemas que ejecutan su negocio, se están generando masivamente flujos de datos generados por las máquinas. Las principales organizaciones se dan cuenta de que estos datos pueden ser increíblemente valiosos para mejorar la eficiencia no solo de TI, sino también de otras partes del negocio. El análisis de dichos datos es una parte importante a la hora de gestionar la seguridad en sistemas. Tanto como para descubrir amenazas y fallos, así como para transmitir de forma inteligible la información forense adquirida.

El análisis de datos en seguridad requiere el uso de las herramientas y métodos adecuados para tratar grandes volúmenes de datos, así como de su correcta visualización. El objetivo de este curso consiste en presentar el estado del arte en procesado de datos, los métodos de minería de datos, el lenguaje de programación R para datos y estadística, las herramientas gráficas de R, y herramientas para importar datos, exportar resultados, y reproducir experimentación.

El profesor que imparte esta primera parte es experto en minería de datos, aprendizaje y detección de patrones, y a nivel de formación tiene amplia experiencia en cursos de aprendizaje automático (machine learning) e inteligencia artificial.

En la segunda parte del curso se abordará la monitorización y las técnicas SIEM (Security Information and Event Management) que permiten detectar cualquier comportamiento anómalo de nuestra infraestructura para resolverlo lo más rápido y de lo forma más eficaz posible. Encontrar señales de comportamiento del adversario es asimismo la base fundamental para identificar los Indicadores de Compromiso (IOC), es decir, toda aquella información relevante

que describe cualquier incidente de ciberseguridad, actividad y/o artefacto malicioso, mediante el análisis de sus patrones de comportamiento.

La búsqueda y monitorización de eventos, de signos de cómo el adversario interactuó con plataformas específicas y aplicaciones para encontrar una cadena de anomalías o comportamientos sospechosos centrará la segunda parte de nuestra asignatura. Aprenderemos los procedimientos y herramientas necesarias para procesar y monitorizar una cantidad enorme de datos tanto de hardware, software como fuentes de seguridad, dejando constancia de posibles fallos de seguridad que encuentra a su paso y también de dichas actividades sospechosas.
De esta manera podremos ayudar a las organizaciones a cumplir la normativa de seguridad y a la vez conseguir la garantía de que su red es segura ya que previene ataques y frena posibles incursiones no deseadas, a la vez que detecta debilidades en la misma. Profundizaremos en el recurso a normas y estándares, incluyendo las normas ISO, las guías STIC y, de modo adicional, veremos los requerimientos de monitorización de red en sistemas de control propios de organizaciones industriales.

1.3. Competencias y resultados de aprendizaje

COMPETENCIAS GENERALES

CG.1-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.

CG.2 -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.

CG.3-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.

CG.4-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.

CG.5-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 ESPECÍFICAS DE LA ASIGNATURA

CE.2 - Diseñar el despliegue de sistemas de vigilancia, análisis y protección de sistemas complejos de tratamiento, almacenamiento y transmisión de datos.

CE.3 - Implementar soluciones de análisis de información relevante para la ciberseguridad basados en tecnologías emergentes de tratamiento de datos.

CE.4 - Identificar las vulnerabilidades, amenazas, y software malicioso a los que estén expuestos los diferentes activos de una organización.

CE.5 - Comprender la interacción entre negocio, activos y ciberseguridad en una organización

CE.6 - Elaborar estrategias de alineamiento entre soluciones de ciberseguridad y objetivos de negocio.

CE.7 - Conocer las tendencias actuales en ciberataques, técnicas de ocultación y principales vectores utilizados.

CE.8 - Crear informes de carácter ejecutivo y de carácter científico-técnico que respondan a las necesidades de comunicación en términos de ciberseguridad dentro de una organización.
CE.9 - Conocer la normativa que regula la certificación de seguridad en sistemas de la información y su implementación dentro de una organización.

CE.13 - Aplicar metodologías que implementen soluciones de ciberseguridad en sistemas complejos de la información, servicios, software y aplicaciones.

2. Contenidos/temario

Bloques temáticos:

- Registros propios del sistema: peculiaridades de Windows y Linux.
- Monitorización del tráfico y seguridad en redes: tipos de protocolos, puertos y backdoors.
- Sistemas de detección y monitorización, automatización del proceso.
- Fuentes heterogéneas de datos y correlación de logs.
- Data Science: Principios de Cloud Computing & Big Data. Data Science.
- Minería de Datos y R como herramientas de ciberseguridad.

El docente facilitará un temario más desarrollado.

3. Metodología

La modalidad de enseñanza propuesta para el presente título guarda consonancia con la Metodología General de la Universidad Internacional de Valencia, aprobada por el Consejo de Gobierno Académico de la Universidad y de aplicación en todos sus títulos.

Este modelo, que vertebra el conjunto de procesos de enseñanza y aprendizaje de la institución, combina la naturaleza síncrona (mismo tiempo-diferente espacio) y asíncrona (diferente tiempo -diferente espacio) de los entornos virtuales de aprendizaje, siempre en el contexto de la modalidad virtual.

El elemento síncrono se materializa en sesiones de diferente tipo (clases expositivas y prácticas, tutorías, seminarios y actividades de diferente índole durante las clases online) donde el profesor y el estudiante comparten un espacio virtual y un tiempo determinado que el estudiante conoce con antelación.

Las actividades síncronas forman parte de las actividades formativas necesarias para el desarrollo de la asignatura y, además, quedan grabadas y alojadas para su posterior visualización.

Por otro lado, estas sesiones no solamente proporcionan espacios de encuentro entre estudiante y profesor, sino que permiten fomentar el aprendizaje colaborativo, al generarse grupos de trabajo entre los estudiantes en las propias sesiones.

Los elementos asíncronos del modelo se desarrollan a través del Campus Virtual, que contiene las aulas virtuales de cada asignatura, donde se encuentran los recursos y contenidos necesarios para el desarrollo de actividades asíncronas, así como para la interacción y comunicación con los profesores y con el resto de departamentos de la Universidad.

4. Actividades formativas

La metodología VIU, basada en la modalidad virtual, se concreta en una serie de actividades formativas y metodologías docentes que articulan el trabajo del estudiante y la docencia impartida por los profesores.

Durante el desarrollo de cada una de las asignaturas, se programan una serie de actividades de aprendizaje que ayudan a los estudiantes a consolidar los conocimientos trabajados en cada una de las asignaturas. A continuación, listamos las actividades genéricas que pueden formar parte de cada asignatura, dependiendo de las competencias a desarrollar en los estudiantes en cada asignatura.

1. Clases presenciales

2. Clases virtuales síncronas

Constituyen el conjunto de acciones formativas que ponen en contacto al estudiante con el profesor, con otros expertos y con compañeros de la misma asignatura en el mismo momento temporal a través de herramientas virtuales. Las actividades recurrentes (por ejemplo, las clases) se programan en el calendario académico y las que son ocasionales (por ejemplo, sesiones con expertos externos) se avisan mediante el tablón de anuncios del campus. Estas actividades se desglosan en las siguientes categorías:

a. Clases expositivas: El profesor expone a los estudiantes los fundamentos teóricos de la asignatura.

b. Clases prácticas: El profesor desarrolla junto con los estudiantes actividades prácticas que se basan en los fundamentos vistos en las clases expositivas. En términos generales, su desarrollo consta de las siguientes fases, pudiéndose adaptar en función de las necesidades docentes:

I. La primera fase se desarrolla en la sala principal de la videoconferencia, donde el profesor plantea la actividad.

II. A continuación, divide a los estudiantes en grupos de trabajo a través de las salas colaborativas y se comienza con la actividad. En esta fase el profesor va entrando en cada sala colaborativa rotando los grupos para resolver dudas, dirigir el trabajo o dar el feedback oportuno. Los estudiantes también tienen posibilidad de consultar al profesor en el momento que consideren necesario.

III. La tercera fase también se desarrolla en la sala principal y tiene como objetivo mostrar el ejercicio o explicar con ejemplos los resultados obtenidos. Por último, se ponen en común las conclusiones de la actividad realizada.

No obstante, el profesor puede utilizar otras metodologías activas y/o herramientas de trabajo colaborativo en estas clases.

c. Seminarios: En estas sesiones un experto externo a la Universidad acude a presentar algún contenido teórico-práctico directamente vinculado con el temario de la asignatura. Estas sesiones permiten acercar al estudiante a la realidad de la disciplina en términos no sólo profesionales, sino también académicos. Todas estas sesiones están vinculadas a contenidos de las asignaturas y del programa educativo.

3. Actividades asíncronas supervisadas

Se trata de un conjunto de actividades supervisadas por el profesor de la asignatura vinculadas con la adquisición por parte de los estudiantes de los resultados de aprendizaje y el desarrollo de sus competencias. Estas actividades, diseñadas con visión de conjunto, están relacionadas entre sí para ofrecer al estudiante una formación completa e integral. Esta categoría se desglosa en el siguiente conjunto de actividades:

a. Actividades y trabajos prácticos: se trata de un conjunto de actividades prácticas realizadas por el estudiante por indicación del profesor que permiten al estudiante adquirir las competencias del título, especialmente aquellas de carácter práctico. Estas actividades, entre otras, pueden ser de la siguiente naturaleza: actividades vinculadas a las clases prácticas (resúmenes, mapas conceptuales, one minute paper, resolución de problemas, análisis reflexivos, generación de contenido multimedia, exposiciones de trabajos, test de autoevaluación, participación en foros, entre otros). Estas actividades serán seleccionadas por el profesor en función de las necesidades docentes. Posteriormente, estas actividades son revisadas por el profesor, que traslada un feedback al estudiante sobre las mismas, pudiendo formar parte de la evaluación continua de la asignatura.

b. Actividades guiadas con recursos didácticos audiovisuales e interactivos: se trata de un conjunto de actividades en las que el estudiante revisa o emplea recursos didácticos (bibliografía, videos, recursos interactivos) bajo las indicaciones realizadas previamente por el profesor; con el objetivo de profundizar en los contenidos abordados en las sesiones teóricas y prácticas. Estas sesiones permiten la reflexión o práctica por parte del estudiante, y pueden complementarse a través de la puesta en común en clases síncronas o con la realización de actividades y trabajos prácticos. Posteriormente, estas actividades son revisadas por el profesor, que traslada un feedback al estudiante sobre las mismas, pudiendo formar parte de la evaluación continua de la asignatura.

4. Tutorías

En esta actividad se engloban las sesiones virtuales de carácter síncrono y las comunicaciones por correo electrónico o campus virtual destinadas a la tutorización de los estudiantes. En ellas, el profesor comparte información sobre el progreso del trabajo del estudiante a partir de las evidencias recogidas, se resuelven dudas y se dan orientaciones específicas ante dificultades concretas en el desarrollo de la asignatura. Pueden ser individuales o colectivas, según las necesidades de los estudiantes y el carácter de las dudas y orientaciones planteadas. Tal y como se ha indicado, se realizan a través de videoconferencia y e-mail.

Se computan una serie de horas estimadas, pues, aunque existen sesiones comunes para todos los estudiantes, éstos posteriormente pueden solicitar al docente tantas tutorías como estimen necesarias.

Dado el carácter mixto de esta actividad formativa, se computa un porcentaje de sincronía estimado del 30%.

5. Estudio autónomo

En esta actividad el estudiante consulta, analiza y estudia los manuales, bibliografía y recursos propios de la asignatura de forma autónoma a fin de lograr un aprendizaje significativo y superar la evaluación de la asignatura de la asignatura. Esta actividad es indispensable para adquirir las competencias del título, apoyándose en el aprendizaje autónomo como complemento a las clases y actividades supervisadas.

6. Examen final

Como parte de la evaluación de cada una de las asignaturas (a excepción de las prácticas y el Trabajo fin de título), se realiza una prueba o examen final. Esta prueba se realiza en tiempo real (con los medios de control antifraude especificados) y tiene como objetivo evidenciar el nivel de adquisición de conocimientos y desarrollo de competencias por parte de los estudiantes. Los exámenes o pruebas de evaluación final se realizan en las fechas y horas programadas con antelación y con los sistemas de vigilancia online (proctoring) de la universidad.

5. Evaluación

5.1. Sistema de evaluación

El Modelo de Evaluación de estudiantes en la Universidad se sustenta en los principios del Espacio Europeo de Educación Superior (EEES), y está adaptado a la estructura de formación virtual propia de esta Universidad. De este modo, se dirige a la evaluación de competencias.

Sistema de Evaluación	Ponderación
Portafolio*	60 %
Sistema de Evaluación	Ponderación
Prueba final*	40 %

***Es requisito indispensable para superar la asignatura aprobar cada apartado (portafolio y prueba final)** con un mínimo de 5 para ponderar las calificaciones.

Los enunciados y especificaciones propias de las distintas actividades serán aportados por el docente, a través del Campus Virtual, a lo largo de la impartición de la asignatura.

Atendiendo a la Normativa de Evaluación de la Universidad, se tendrá en cuenta que la utilización de **contenido de autoría ajena** al propio estudiante debe ser citada adecuadamente en los trabajos entregados. Los casos de plagio serán sancionados con suspenso (0) de la actividad en la que se detecte. Asimismo, el uso de **medios fraudulentos durante las pruebas de evaluación** implicará un suspenso (0) y podrá implicar la apertura de un expediente disciplinario.

5.2. Sistema de calificación

La calificación de la asignatura se establecerá en los siguientes cómputos y términos:

Nivel de aprendizaje	Calificación numérica	Calificación cualitativa
Muy competente	9,0 - 10	Sobresaliente
Competente	7,0 - 8,9	Notable
Aceptable	5,0 -6,9	Aprobado
Aún no competente	0,0 -4,9	Suspenso

Sin detrimento de lo anterior, el estudiante dispondrá de una **rúbrica simplificada** en el aula que mostrará los aspectos que valorará el docente, como así también los **niveles de desempeño que tendrá en cuenta para calificar las actividades vinculadas a cada resultado de aprendizaje.**

La mención de «**Matrícula de Honor**» podrá ser otorgada a estudiantes que hayan obtenido una calificación igual o superior a 9.0. Su número no podrá exceder del cinco por ciento de los estudiantes matriculados en una materia en el correspondiente curso académico, salvo que el número de estudiantes matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor.

6. Bibliografía

M_i_n_e_r_ía_ _d_e_ _D_a_t_o_s_ _y_ _A_p_r_e_n_d_i_z_a_j_e_ _A_u_t_o_m_át_i_c_o_:_ _
T. Hastie, R. Tibshirani, J. Friedman “The elements of statistical learning: data mining, inference, and prediction”, Springer, 2009, ISBN: 9780387848570.
J.H. Maindonald, J. Braun, “Data analysis and graphics using R: an example-based approach”, Cambridge University, 2010, ISBN: 9780521762939.
R.O. Duda, P.E. Hart, D.G. Stork, “Pattern classification” , John Wiley & Sons , 2001 , ISBN: 0-471-05669-3.
H_e_r_r_a_m_i_e_n_t_a_s_ _d_e_ _M_i_n_e_r_ía_ _d_e_ _D_a_t_o_s_:_ _
KDnuggets, “Software para Minería de Datos”. http://www.kdnuggets.com (2016)
R, “Comprehensive R Archive Network”. http://www.cran.es.r-project.org (2016)
Herramientas de red, “R-Net-Tools” https://github.com/r-net-tools (2016)
A_n_ál_i_s_i_s_ _d_e_ _D_a_t_o_s_ _e_n_ _S_e_g_u_r_i_d_a_d_:_ _
David García. “Recopilación de Logs y Proxy” http://www.securityartwork.es/2015/02/26/recopilacion-de-informacion-information-gathering-sobre-logs-de-proxy-i/ Securityatwork.com (2016)
Dzidorius Martinaitis. “Data mining for Network security and Intrusion Detection” https://www.r-bloggers.com/data-mining-for-network-security-and-intrusion-detectio n R-bloggers (2016)
U_s_o_ _d_e_ _R_ _a_v_a_n_z_a_d_o_:_ _
Hadley Wickham, “Advanced R”, CRC Press 2014.
Hadley Wickham “Plyr tutorial” http://plyr.had.co.nz/09-user/ useR! 2009 Christopher Bare, MySQL + R” http://www.r-bloggers.com/mysql-and-r/ (2016) Stacompute “MongoDB + R” https://www.r-bloggers.com/r-and-mongodb/ (2016)
SAPE research group “ggplot2 reference” http://sape.inf.usi.ch/quick-reference/ggplot2 (2016) V.04 11

D_o_c_u_m_e_n_t_a_c_i_ón_ _s_o_b_r_e_ _M_a_r_k_d_o_w_n_ _y_ _N_o_t_e_b_o_o_k_s_:_ _
John Gruber “Markdown Basics” http://daringfireball.net/projects/markdown/basics (2016) Jupyter Project “Notebooks” http://jupyter.org (2016) Jupyter Project “Jupyter Notebook QuickStart”
https://jupyter.readthedocs.io/en/latest/content-quickstart.html (2016)
D_a_t_o_s_ _P_úb_l_i_c_o_s_:_ _
USA Government Open Data: http://www.data.gov/open-gov/ (2016)
EU Open Data: http://ec.europa.eu/digital-agenda/en/open-data-0 (2016) España Open Data: http://www.boe.es/datosabiertos/ (2016)
Generalitat de Catalunya Open Data: http://dadesobertes.gencat.cat/en (2016)
M_o_n_i_t_o_r_i_z_a_c_i_ón_:_ _
Sanders, C., & Smith, J. (2013). Applied network security monitoring: collection, detection, and analysis. Elsevier.
Collins, M. (2017). Network Security Through Data Analysis: From Data to Action. O'Reilly Media, Inc.
Best Practices for MITRE ATT&CK® Mapping: https://us-cert.cisa.gov/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf (2021)

Guía de Seguridad de las TIC CCN-STIC 140. Taxonomía de productos STIC - Anexo B.3-M: Herramientas de gestión de red: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/4309-anexo-b-3m-herramientas-de-gestion-de-red/file.html (2019)