



Datos Generales

Asignatura: ANÁLISIS Y TIPOLOGÍAS MALWARE

Titulación: GRADO EN CIBERSEGURIDAD

Carácter: OBLIGATORIA.

Créditos ECTS: 6 ECTS

Curso: 2º

Distribución temporal: 1º SEMESTRE.

Idioma de impartición: CASTELLANO.

Equipo docente: Carlos Gómez

Aula(s): Aula informatizada

Presentación de la asignatura:

Asignatura para conocer y afianzar los conceptos relacionados con el análisis y las diferentes tipologías de malware que serán de gran importancia de cara a aplicar los conocimientos al área de la ciberseguridad.

Datos Específicos

Resultados del proceso de formación y aprendizaje (RFA)¹

Contenidos o conocimientos (C)	C1	Desarrollar habilidades de cálculo para el análisis en los lenguajes de programación.
	C2	Reconocer estructuras y protocolos para implementar soluciones de seguridad a nivel de arquitectura de redes de la ciberseguridad.
	C3	Aplicar los conocimientos de protección de datos y seguridad de la información en distintos niveles.
	C6	Identificar distintas tipologías de virus informáticos.

¹ La clasificación de los RFA corresponde a la definida en el RD822/2021 y se encuentran definidos en la memoria de verificación del título.

* Extender el contenido utilizando para ello la programación docente. La extensión debe estar en punto intermedio, es decir, ampliar la información en la guía docente pero no llegar a los límites de la programación docente. Se debe incluir el índice de temas a tratar punto por punto (sin desarrollar). Se pueden incluir hasta tres subapartados con ideas claves/subtemas. La extensión máxima será de 2 páginas.

	C7	Reconocer técnicas antiforenses y su aplicación.
	C8	Aplicar bases matemáticas y técnicas de diseño de algoritmos a la criptografía y ciberseguridad.
	C11	Conocer las diferentes topologías de malware para su posterior análisis y mitigación.
	C13	Analizar la gestión de identidades, cifrado, autenticación, confidencialidad, integridad y disponibilidad de la información.
	C14	Valorar los riesgos que suceda un determinado suceso mediante métodos estadísticos y probabilísticos.
Competencias (CO)	CO2	Usar diferentes herramientas de ingeniería y ciberseguridad para la resolución de problemas relacionados con los ciberataques.
	CO3	Llevar a cabo distintos procesos de análisis en las diferentes áreas de la ciberseguridad.
	CO5	Aplicar técnicas de prevención, detección y protección de ataques en un sistema informático.
	CO7	Implementar soluciones criptográficas.
	CO11	Gestionar evidencias de vulnerabilidades.
	CO12	Elaborar análisis forenses.
Habilidades y destrezas (H)	H1	Trabajar en grupo transmitiendo conocimientos y habilidades adquiridos.
	H2	Desarrollar habilidades para el análisis, la elaboración y la colaboración en proyectos, partiendo de las necesidades propias del mercado.
	H4	Tomar decisiones en el ámbito profesional, aplicando los conocimientos y técnicas adquiridas a lo largo de la actividad académica.
	H5	Comunicar de forma clara y concisa, a todo tipo de audiencias, conocimientos, ideas, soluciones, datos, etc. en el ámbito del estudio.
	H6	Ser capaz de trabajar con información técnica en inglés, tanto a nivel de consulta como de su elaboración.

Contenido de la Asignatura*

- **Unidad 1: Introducción al Malware**
 - Historia del software malicioso.
 - Clasificación del malware
 - Contexto y Motivaciones del Malware
- **Unidad 2: Técnicas de Propagación, Infección y Replicación**
 - Vectores de infección.
 - Técnicas de propagación.
 - Técnicas de replicación evasión y persistencia.
- **Unidad 3: Análisis Estático del Malware**
 - Fundamentos de análisis estático.
 - Identificación y clasificación de Malware.
 - Análisis de ficheros ejecutables.
- **Unidad 4: Análisis Dinámico del Malware**
 - Fundamentos de análisis dinámico.
 - Monitoreo de comportamiento del Malware.
 - Técnicas de Ingeniería inversa.
- **Unidad 5: Mitigaciones y Contramedidas**
 - Estrategias de mitigación.
 - Herramientas Anti-Malware
 - Evaluación y Respuesta a Incidentes
- **Unidad 6: Ingeniería Social y su papel en la Propagación del Malware**
 - Introducción a la Ingeniería social
 - Técnicas comunes de Ingeniería Social
 - Estrategias de Defensa contra la Ingeniería Social
 - Simulaciones y Respuesta a Incidentes de Ingeniería Social

Metodologías Docentes y Actividades Formativas²

Metodologías docentes utilizadas en esta asignatura son:

² Se deberán extraer de la memoria verificada del título las metodologías docentes, actividades formativas y sistemas de evaluación. (1 ECTS = 25 horas de trabajo del estudiante).

MD1	Método expositivo.
MD2	Estudios de caso.
MD3	Aprendizaje basado en problemas.
MD4	Aprendizaje basado en proyectos.
MD5	Aprendizaje cooperativo.
MD6	Tutorías.

Actividades formativas utilizadas en esta asignatura son:

Actividades formativas	Horas previstas	% presencialidad
AF1: Clase teórica.	22,5	100
AF2: Clase prácticas.	15	100
AF3: Realización de trabajos (individuales y/o grupales).	12,5	50
AF3: Tutorías (individuales y/o grupales).	5	0
AF5: Estudio independiente y trabajo autónomo del o la estudiante.	89	0
AF6: Pruebas de evaluación.	6	100
Total	150	--

Evaluación: Sistemas y Criterios de Evaluación

Las semanas de evaluación están definidas en el calendario académico publicado en la web de la universidad; la concreción de las fechas se realizará una vez que la docencia haya comenzado.

Sistemas de evaluación utilizados en esta asignatura son:

Denominación	Pond. Mín	Pond. Máx
SE1 Evaluación de la asistencia y participación del o la estudiante.	0	5
SE2 Evaluación de trabajos.	10	35
SE3 Pruebas de evaluación y/o exámenes.	50	70

El estudiantado posee dos modalidades de evaluación para superar la asignatura:

- Evaluación continua con 2 convocatorias/año: ordinaria y extraordinaria.
- Evaluación única con 2 convocatorias/año.

En la Universidad Euneiz la evaluación continua (media ponderada de las diferentes actividades evaluables de la asignatura definidas por el profesorado) es la evaluación primordial; pero Euneiz permite al estudiantado acogerse a la evaluación única.

No se permite el cambio de modalidad de evaluación (de continua a única) escogido por el estudiante a lo largo del curso.

El/la estudiante que desee acogerse a la modalidad de evaluación única deberá solicitarlo por escrito formal que lo justifique dirigido al profesorado responsable de la asignatura y a la Coordinación del título en las dos primeras semanas del inicio de la misma.

Si el/la estudiante no asiste un 80% a las clases presenciales, pasará directamente a la convocatoria extraordinaria de la evaluación única.

De manera excepcional, el/la docente responsable de la asignatura podrá valorar con otros criterios adicionales como la participación, la actitud, el grado de desempeño y aprovechamiento del o la estudiante, etc., la posibilidad de permitir que el/la estudiante continúe en la convocatoria ordinaria, siempre que su asistencia mínima se encuentre por encima del 70%.

Las faltas de asistencia deben justificarse al profesor/a responsable de la asignatura con un plazo máximo de 1 semana. El justificante oficial deberá ser presentado al profesor/a responsable mediante un correo electrónico.

El/la estudiante irá a la evaluación extraordinaria ÚNICAMENTE con las partes suspendidas.

El sistema de calificación de la asignatura sigue lo establecido en el RD 1125/2003 y los resultados obtenidos se calificarán siguiendo la escala numérica de 0 a 10, con expresión de un decimal.

- 0-4,9: Suspenso (SS).



Guía Docente

Curso Académico 2026/27

- 5,0-6,9: Aprobado (AP).
- 7,0-8,9: Notable (NT).
- 9,0-10: Sobresaliente (SB).

La mención de «Matrícula de Honor» podrá ser otorgada a alumnos/as que hayan obtenido una calificación igual o superior a 9,0. Su número no podrá exceder del cinco por ciento de los/las alumnos/as matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos/as matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor».

Será considerado no presentado (NP) el estudiantado matriculado que no realice ninguna actividad evaluativa.

Toda actividad evaluativa escrita (trabajos, exámenes...) considerará las faltas ortotipográficas en la calificación final.

El plagio está prohibido, tanto en los trabajos, como en los exámenes, en caso de detectarse la calificación será suspenso. Los trabajos entregados a través del campus virtual serán objeto de análisis por la herramienta Turnitin:

- Los informes con un índice de similitud entre el 20% y el 30% serán revisados por el profesor/a para analizar las posibles fuentes de plagio y evaluar si están justificadas.
- Cualquier trabajo con un índice de similitud superior al 30%, una vez realizado el análisis del o la docente, no será evaluado.

Recursos materiales e infraestructuras necesarias

Tipo de recurso material y/o infraestructura
Material docente (apuntes, presentaciones, guías, tareas...)
Recursos audiovisuales
Material específico de la asignatura
Aula informatizada
Laboratorio de Ciberseguridad



Bibliografía y otros Recursos de Aprendizaje

Bibliografía Básica

- Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software (English Edition)
- Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware
- Mastering Windows Security and Hardening: Secure and protect your Windows environment from intruders, malware attacks, and other

Bibliografía Complementaria

- Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey of machine learning techniques for malware analysis. Computers & Security, 81, 123-147.
- Gandotra, E., Bansal, D., & Sofat, S. (2014). Malware analysis and classification: A survey. Journal of Information Security, 2014.
- Gandotra, E., Bansal, D., & Sofat, S. (2014). Malware analysis and classification: A survey. Journal of Information Security, 2014.

Otros Recursos de Aprendizaje Recomendados³

- <https://www.udemy.com/course/getting-started-with-malware-analysis/?couponCode=LETSLEARNNOWPP>
- <https://www.udemy.com/course/malware-analysis-of-net-java/?couponCode=LETSLEARNNOWPP>

³ Entre otros recursos de aprendizaje pueden incluirse páginas web, software, materia audiovisual, etc.