Guía docente
270140 - DA - Detección de Amenazas

Última modificación: 09/07/2026

Unidad responsable: Facultad de Informática de Barcelona
Unidad que imparte: 701 - DAC - Departamento de Arquitectura de Computadores.

Titulación: GRADO EN INGENIERÍA INFORMÁTICA (Plan 2010). (Asignatura optativa).

Curso: 2026 **Créditos ECTS:** 6.0 **Idiomas:** Catalán

PROFESORADO

Profesorado responsable:

Otros:

CAPACIDADES PREVIAS

La asignatura requiere conocimientos básicos de ciberseguridad, como criptografía de clave pública y privada, bases de ciberseguridad, actores en el entorno... por lo que debe haberse cursado o estar cursando la asignatura de Seguridad Informática

REQUISITOS

- Corequisito SI

COMPETENCIAS DE LA TITULACIÓN A LAS QUE CONTRIBUYE LA ASIGNATURA

Específicas:
CT2.3. Diseñar, desarrollar, seleccionar y evaluar aplicaciones, sistemas y servicios informáticos, y al mismo tiempo asegurar su fiabilidad, su seguridad y su calidad, conforme a principios éticos y a la legislación y la normativa vigente.
CT2.4. Demostrar conocimiento y capacidad de aplicación de las herramientas necesarias para el almacenaje, el procesamiento y el acceso a los Sistemas de información, incluidos los basados en web.
CT6.3. Demostrar conocimiento de las características, funcionalidades y estructura de los Sistemas Operativos que permita su uso adecuado, administración y diseño, así como la implementación de aplicaciones basadas en sus servicios.
CT7.2. Evaluar sistemas hardware/software en función de un criterio de calidad determinado.
CT7.3. Determinar los factores que inciden negativamente en la seguridad y la fiabilidad de un sistema hardware/software, y minimizar sus efectos.
CTI2.1. Dirigir, planificar y coordinar la gestión de la infraestructura informática: hardware, software, redes y comunicaciones.
CTI2.2. Administrar y mantener aplicaciones, sistemas informáticos y redes de computadores (los niveles de conocimiento y comprensión están en las competencias técnicas comunes).

Genéricas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.
G7. APRENDIZAJE AUTÓNOMO: Detectar carencias en el propio conocimiento y superarlas mediante la reflexión crítica y la elección de la mejor actuación para ampliar este conocimiento. Capacidad para el aprendizaje de nuevos métodos y tecnologías y versatilidad para adaptarse a nueves situaciones.

METODOLOGÍAS DOCENTES

La asignatura estará compuesta básicamente por tres tipos de aprendizaje:
1. Clase magistral de teoría con ejemplos reales e interacción con los estudiantes
2. Clases prácticas de laboratorio para el análisis de casos reales aplicados
3. Charlas de empresa, donde expertos del sector vendrán a mostrar cómo gestionan la seguridad en las empresas

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

1.Analizar brechas de seguridad a través de los logs del sistema
2.Administrar, analizar y monitorear los registros (logs) propios de los Sistemas Operativos (syslog/journalctl en Linux, Event Viewer en Windows), demostrando conocimiento de su estructura para mantener los sistemas y detectar anomalías.
3.Aplicar herramientas de almacenamiento, procesamiento y acceso a la información de seguridad mediante plataformas SIEM y el uso de reglas YARA para centralizar y correlacionar grandes volúmenes de eventos.
4.Comprender el funcionamiento interno de los sistemas de detección (firmas, heurística, comportamiento e IA), leyendo y utilizando eficazmente manuales y especificaciones de productos de ciberseguridad escritos en inglés.
5.Evaluar y comparar diferentes soluciones de hardware y software de defensa (Antivirus, EPP, EDR y XDR) de acuerdo a criterios de calidad y eficacia técnica para seleccionar la mejor opción según el entorno.
6.Evaluar y comparar diferentes soluciones de hardware y software de defensa (Antivirus, EPP, EDR y XDR) de acuerdo a criterios de calidad y eficacia técnica para seleccionar la mejor opción según el entorno.
7.Dirigir y planificar la gestión de la seguridad de la infraestructura informática mediante el diseño de Planes de Ciberseguridad formales, asegurando su fiabilidad de acuerdo con principios éticos y la normativa vigente.
8.Desarrollar estrategias de respuesta automática y orquestación (SOAR), tomando decisiones tecnológicas basadas en criterios objetivos y datos experimentales extraídos de los incidentes.
9.Analizar la presencia de brechas de seguridad a través de los logs del sistema
10.Ejecutar las prácticas y tareas de laboratorio de la asignatura en los plazos establecidos, aplicando de forma progresiva el aprendizaje guiado y dirigido, evaluando de forma crítica el propio progreso, fortalezas y debilidades técnicas en el análisis de incidentes.

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTADO

Tipo	Horas	Porcentaje
Horas aprendizaje autónomo	90,0	60.00
Horas grupo grande	30,0	20.00
Horas grupo pequeño	30,0	20.00

Dedicación total: 150 h

CONTENIDOS

Introducción a CyberThreat Intelligence

Descripción:
Este tema establece los fundamentos de la Inteligencia de Amenazas Cibernéticas (CTI). Se analiza el ciclo de vida de la inteligencia para transformar datos crudos en conocimiento accionable, permitiendo a las organizaciones pasar de una defensa reactiva a una proactiva.

Se estudian los niveles de inteligencia (estratégica, operacional, táctica y técnica) y como conceptos clave como los Indicadores de Compromiso (IoC) y las Tácticas, Técnicas y Procedimientos (TTP) se integran en las herramientas de seguridad (como SIEM o EDR). El objetivo final es aprender a anticiparse a los ataques, perfilar a los actores maliciosos y agilizar la respuesta a incidentes.

Análisis de Logs

Descripción:
Este tema profundiza en el Análisis de Logs, pieza fundamental para la visibilidad y la detección de amenazas. El estudiante aprenderá a extraer, interpretar y correlacionar los registros de los sistemas operativos para rastrear ataques y detectar anomalías.

En entornos Linux, se explorará la gestión y análisis de registros mediante herramientas clave como syslog y journalctl. Por lo que se refiere a Windows, el estudio se centrará en dominar el Event Viewer para identificar eventos críticos de seguridad, tales como inicios de sesión sospechosos o alteraciones del sistema. Este dominio técnico base es el paso previo y esencial para su posterior centralización en sistemas SIEM.

Evolución de la detección de amenazas

Descripción:
Este tema traza la evolución tecnológica de las herramientas de defensa, empezando por los primeros antivirus basados en firmas. Se analiza la transición hacia el Antivirus Next Generation (NGAV) y las plataformas EPP, centradas en maximizar la prevención en los equipos.

Seguidamente, se aborda el cambio de paradigma hacia la monitorización y respuesta continua con la aparición del EDR (Endpoint Detection and Response). Por último, se estudia la culminación de este proceso: el XDR (eXtended Detection and Response), una tecnología que rompe los silos de información integrando datos de endpoint, red, nube e identidad para ofrecer una visibilidad holística y una respuesta automatizada ante ataques complejos.

Antivirus

Descripción:
Este tema profundiza en el funcionamiento detallado de los Antivirus, históricamente la primera línea de defensa a los endpoints. Se analiza la evolución de sus motores para hacer frente a malware cada vez más avanzado.

Empezaremos estudiando la **detección basada en firmas**, eficaz contra software malicioso conocido, pero insuficiente frente a nuevas variantes. Para cubrir estas carencias, se explorarán enfoques más proactivos: el **análisis heurístico** y la **detección por comportamiento**, capaces de identificar acciones sospechosas en tiempo real sin conocimiento previo. Por último, se abordará la integración de la **Inteligencia Artificial**, utilizando el aprendizaje automático para predecir y bloquear amenazas desconocidas (Zero-Day) antes de su ejecución.

EDR/XDR

Descripción:
Este tema profundiza en las tecnologías avanzadas de detección y respuesta: EDR y XDR. El estudiante explorará las **funcionalidades** clave del EDR, diseñado para monitorizar continuamente la actividad en los endpoints*, detectar comportamientos anómalos y facilitar el aislamiento y contención de amenazas eludidas por los antivirus tradicionales.

A continuación, se ampliará la perspectiva hacia el XDR, que unifica la telemetría de múltiples vectores (red, nube, correo e identidad) para una visión global del ataque. Por último, se aprenderá a clasificar y gestionar los diferentes niveles de alerta, una habilidad crítica para priorizar incidentes, reducir la fatiga de alertas y optimizar la eficiencia de los equipos de respuesta.

Respuesta a Incidentes

Descripción:
Este tema se centra en la Respuesta a Incidentes, abordando cómo las organizaciones deben actuar de forma estructurada una vez detectada una brecha de seguridad. Se estudiará el diseño de planes de ciberseguridad, estableciendo protocolos claros y metódicos para la contención, erradicación y recuperación del entorno afectado.

Además, se pondrá especial énfasis en la modernización de esta capacidad mediante la automatización. El estudiante comprenderá el valor y el funcionamiento de las soluciones SOAR (Security Orchestration, Automation, and Response), herramientas clave para orquestar defensas, automatizar tareas repetitivas y reducir drásticamente los tiempos de reacción frente a los ataques.

ACTIVIDADES

Introducción a la CyberThreat Intelligence

Descripción:
Este tema establece los fundamentos de la Inteligencia de Amenazas Cibernéticas (CTI). Se analiza el ciclo de vida de la inteligencia para transformar datos crudos en conocimiento accionable, permitiendo a las organizaciones pasar de una defensa reactiva a una proactiva.

Se estudian los niveles de inteligencia (estratégica, operacional, táctica y técnica) y como conceptos clave como los Indicadores de Compromiso (IoC) y las Tácticas, Técnicas y Procedimientos (TTP) se integran en las herramientas de seguridad (como SIEM o EDR). El objetivo final es aprender a anticiparse a los ataques, perfilar a los actores maliciosos y agilizar la respuesta a incidentes.

Objetivos específicos:
1

Dedicación: 10h
Grupo grande/Teoría: 4h
Grupo pequeño/Laboratorio: 2h
Aprendizaje autónomo: 4h

Análisis de Logs

Descripción:
Este tema profundiza en el Análisis de Logs, pieza fundamental para la visibilidad y la detección de amenazas. El estudiante aprenderá a extraer, interpretar y correlacionar los registros de los sistemas operativos para rastrear ataques y detectar anomalías.

En entornos Linux, se explorará la gestión y análisis de registros mediante herramientas clave como syslog y journalctl. Por lo que se refiere a Windows, el estudio se centrará en dominar el Event Viewer para identificar eventos críticos de seguridad, tales como inicios de sesión sospechosos o alteraciones del sistema. Este dominio técnico base es el paso previo y esencial para su posterior centralización en sistemas SIEM.

Objetivos específicos:
2, 9

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

Dedicación: 17h
Grupo grande/Teoría: 5h
Grupo pequeño/Laboratorio: 6h
Aprendizaje autónomo: 6h

Evolución de la detección de amenazas

Descripción:
Este tema traza la evolución tecnológica de las herramientas de defensa, empezando por los primeros antivirus basados en firmas. Se analiza la transición hacia el Antivirus Next Generation (NGAV) y las plataformas EPP, centradas en maximizar la prevención en los equipos.

Seguidamente, se aborda el cambio de paradigma hacia la monitorización y respuesta continua con la aparición del EDR (Endpoint Detection and Response). Por último, se estudia la culminación de este proceso: el XDR (eXtended Detection and Response), una tecnología que rompe los silos de información integrando datos de endpoint, red, nube e identidad para ofrecer una visibilidad holística y una respuesta automatizada ante ataques complejos.

Objetivos específicos:
4, 5, 6

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.

Dedicación: 13h
Grupo grande/Teoría: 5h
Grupo pequeño/Laboratorio: 4h
Aprendizaje autónomo: 4h

Antivirus

Descripción:
Antivirus
1. Signature Based
2. Detección Heurística
3. Detección por comportamiento
4. Detección con IA

Objetivos específicos:
4, 5, 9

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

Dedicación: 12h
Grupo grande/Teoría: 2h
Grupo pequeño/Laboratorio: 4h
Aprendizaje autónomo: 6h

Examen Parcial

Descripción:
Examen durante la tanda de exámenes parciales con el temario visto hasta la fecha

Objetivos específicos:
1, 2, 3, 4, 9

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

Dedicación: 12h
Actividades dirigidas: 2h
Aprendizaje autónomo: 10h

Charla de empresa

Descripción:
Vendrá un experto/experta en respuesta a incidentes para explicarnos cómo funciona su SOC

Dedicación: 2h
Grupo grande/Teoría: 2h

EDR/XDR

Descripción:
EDR/XDR
1. Funcionalidades
2. Niveles de alerta

Objetivos específicos:
4, 5, 6

Competencias relacionadas:
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.

Dedicación: 16h
Grupo grande/Teoría: 4h
Grupo pequeño/Laboratorio: 4h
Aprendizaje autónomo: 8h

Respuesta a incidentes

Descripción:
Respuesta a Incidentes
1. Planes de ciberseguridad
2. Respuesta automática

Objetivos específicos:
7, 8

Competencias relacionadas:
G7. APRENDIZAJE AUTÓNOMO: Detectar carencias en el propio conocimiento y superarlas mediante la reflexión crítica y la elección de la mejor actuación para ampliar este conocimiento. Capacidad para el aprendizaje de nuevos métodos y tecnologías y versatilidad para adaptarse a nueves situaciones.

Dedicación: 21h
Grupo grande/Teoría: 4h
Grupo pequeño/Laboratorio: 8h
Aprendizaje autónomo: 9h

Segundo Parcial

Descripción:
Examen con todo el temario

Objetivos específicos:
1, 2, 3, 4, 5, 6, 7, 8, 9

Competencias relacionadas:
G7. APRENDIZAJE AUTÓNOMO: Detectar carencias en el propio conocimiento y superarlas mediante la reflexión crítica y la elección de la mejor actuación para ampliar este conocimiento. Capacidad para el aprendizaje de nuevos métodos y tecnologías y versatilidad para adaptarse a nueves situaciones.
G3. TERCERA LENGUA: Conocer el idioma inglés con un nivel adecuado de forma oral y por escrito, y con consonancia con las necesidades que tendrán los graduados y graduadas en ingeniería informática. Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe, y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con la profesión de ingeniero técnico en informática.
G6. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información del ámbito de la ingeniería informática y valorar de forma crítica los resultados de esta gestión.

Dedicación: 27h
Actividades dirigidas: 2h
Aprendizaje autónomo: 25h

Examen de laboratorio

Objetivos específicos:
10

Competencias relacionadas:
G7. APRENDIZAJE AUTÓNOMO: Detectar carencias en el propio conocimiento y superarlas mediante la reflexión crítica y la elección de la mejor actuación para ampliar este conocimiento. Capacidad para el aprendizaje de nuevos métodos y tecnologías y versatilidad para adaptarse a nueves situaciones.

Dedicación: 20h
Actividades dirigidas: 2h
Aprendizaje autónomo: 18h

SISTEMA DE CALIFICACIÓN

La competencia transversal de aprendizaje autónomo se evalúa a partir de los informes de seguimiento entregados durante el curso y pesa un 5% de la nota final.

Las competencias técnicas se evalúan a partir de la nota de teoría (45%) y el examen de laboratorio (50%, N_práctica).

La teoria se evalúa a partir de los controles parciales y el examen final. La nota de los 2 controles parciales se calcula a partir de la media ponderada de las 2 pruebas, con los siguientes pesos: 40 y 60%. Si la nota ponderada de los 2 controles parciales es igual o superior a 5.0, la asistencia al examen final sería opcional. En cualquier caso, la nota media de los parciales de teoría debe superar el 3.5 para poder realizar media con el resto de calificaciones.

En caso que un estudiante se presente al examen final, su nota de teoria sería la más alta que se obtenga entre la nota obtenida en el examen final y la media ponderada de los controles parciales.

De este modo la nota de la asignatura se calcula:
N_parciales =N_p1*0.4 + N_p2*0.6 <-- computa siempre que sea >= 3.5
N_teoría = max(N_parciales, N_final)

N_final = N_teoría * 0.45 + N_práctica * 0.5 + N_seguimiento * 0.05

BIBLIOGRAFÍA

Básica:
- Roberts, Aaron. Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers. Apress, ISBN 978-1484272190.