+34 958 241000 (ext. 20048) gmacia@ugr.es

CONTACTO: GABRIEL MACIÁ
+34 958 241000(EXT.20048)

Máster de Formación Permanente en Ciberseguridad (Información VI Edición - Curso 21/22)

Módulos o Asignaturas

Objetivos

- Conocer los fundamentos de la ciberseguridad, los servicios, mecanismos y políticas, así como el análisis de riesgos y los estándares en el sector.
- Comprender los aspectos normativos y legislativos de la ciberseguridad en relación a cuestiones como la propiedad intelectual, régimen laboral, administrativo y financiero.
- Conocer criptosistemas y esquemas de autenticación, integridad, firma digital y ocultación de información.
- Aprender cuestiones relacionadas con la provisión de seguridad en sistemas operativos.
- Conocer fundamentos y procedimientos de seguridad en apliaciones finales, independientemente del tipo de plataforma considerada (móvil, *cloud*, ...).
- Comprender protocolos específicamente diseñados para la provisión de seguridad en las distintas capas de una red de comunicaciones.
- Conocer tecnologías relacionadas con el acceso a redes y sistemas: cortafuegos, encapsulado, redes privadas virtuales.
- Aprender a gestionar incidentes de seguridad a través de la monitorización de los sistemas, el análisis y detección de eventos no deseados y la adopciónde contramedidas para su solución.
- Saber procedimientos y técnicas de auditoría de sistemas.

- Comprender la legislación y los esquemas actuales involucrados en el análisis forense de sistemas.
- Aprender acerca del test, desarrollo y verificación seguros del software,el análisis de *malware* y la ingeniería inversa de programas.

Estructura

Módulo	Asignatura	Créditos
Gobernanza de la ciberseguridad	Gestión de la ciberseguridad	3
	Derecho de la ciberseguridad	3
Protección de redes y sistemas (24 cr.)	Seguridad de la información	4,5
	Seguridad en Sistemas Operativos	4,5
	Seguridad de Aplicaciones	6
	Comunicaciones seguras	4,5
	Acceso a Redes y Sistemas	4,5
Administración de la seguridad (18 cr.)	Sistemas de Ciberdefensa	4,5
	Hacking Ético	6
	Análisis Forense de Sistemas y	4,5
	Análisis de Malware	3
Ciberseguridad Aplicada (2 cr.)	Ciberseguridad Aplicada	2
TFM	Trabajo Fin de Máster	10

Módulo: Gobernanza de la Ciberseguridad

Gestión de la Ciberseguridad

Teoría: 15h. Prácticas: 8h. Tutorías: 6h. Examen: 1h.

TEORÍA:

1. Introducción. Gestión de seguridad de la información
2. ISO/IEC 27001: Políticas de seguridad, certificación y análisis de riesgos
3. Gestión de servicios y continuidad de negocio
4. Cumplimiento de la seguridad de la información: ENS, NIS, RGPD

PRÁCTICAS:

1. Casos de estudio: ENS, eAdministración, eHealth

Profesorado:

- Dr. Pedro García Teodoro - UGR
  Coordinador de la asignatura
- Dr. Juan Díaz García - SAS

Ciberderecho

Teoría: 15h. Prácticas: 8h. Tutorías: 6h. Examen: 1h.

TEORÍA:

1. Estructuras, procesos y normas sobre ciberseguridad
2. Gobernanza del ciberespacio
3. Derechos: Privacidad y protección de datos
4. Cibercriminalidad
5. Ciberdefensa y ciberguerra

PRÁCTICAS:

1. Seguridad de redes y sistema de información
2. Infraestructuras críticas
3. Ciberespionaje
4. Ciberterrorismo

Profesorado:

- Dra. Marga Robles-UGR
  Coordinadora de la asignatura
- Carlos Seisdedos Semulue - Internet Security Auditors
- Fco. Jose Hernández Guerrero - Fiscal Criminalidad Informática

Módulo: Protección de Redes y Sistemas

Seguridad de la Información

Teoría: 17h. Prácticas: 18h. Tutorías: 9h. Examen: 1h.

TEORÍA:

1. Criptosistemas simétricos
2. Criptosistemas asimétricos
3. Funciones hash
4. Firma digital
5. Certificación digital

PRÁCTICAS:

1. Criptosistemas: AES, RSA, ECC
2. Algoritmos de *hashing*: SHA-2 y SHA-3
3. Firmas y certificación: DSA y PKI

Profesorado:

- Dr. Javier Lobillo Borrero - UGR
  Coordinador de la asignatura
- Dr. Jesús García Miranda - UGR
- Dr. Fco. García Olmedo - UGR
- Dra. Amparo Fúster Sabater - CSIC

Seguridad en Sistemas Operativos

Teoría: 17h. Prácticas: 18h. Tutorías: 9h. Examen: 1h.

TEORÍA:

1. Mecanismos genéricos de seguridad
2. Fortalecimiento del SO
3. Seguridad en Unix/Linux
4. Seguridad en Sistemas Windows
5. Seguridad en dispositivos móviles e IoT
6. Seguridad en máquinas virtuales

PRÁCTICAS:

1. Administración de la seguridad en Linux
2. Detección de intrusiones basada en host
3. Administración de seguridad en sistemas Windows
4. Seguridad en máquinas hipervisores

Profesorado:

- Dr. J. Antonio Gómez Hernández - UGR
  Coordinador de la asignatura
- Dr. J. Manuel Benítez Sánchez - UGR
- Dr. Alejandro León Salas-UGR
- Dr. Gabriel Maciá Fernández-UGR

Seguridad de Aplicaciones

Teoría: 24h. Prácticas: 23h. Tutorías: 12h. Examen: 1h.

TEORÍA:

1. Introducción
2. Ingeniería del software seguro: SDL [Security Development Lifecycle] y programación segura
3. Test de software seguro y auditorías de código
4. Seguridad en bases de datos
5. Seguridad en aplicaciones web

PRÁCTICAS:

1. Codificación segura
2. Herramientas de análisis de software
3. Tests de seguridad de aplicaciones
4. Análisis de seguridad de bases de datos
5. Análisis de seguridad de aplicaciones web

6. Seguridad en aplicaciones móviles
7. Autentificación

6. Análisis de seguridad de aplicaciones móviles
7. Mecanismos de autentificación

Profesorado:

- Dr. Fernando Berzal Galiano - UGR
  Coordinador de la asignatura
- Dr. Pablo García Sánchez - UGR
- Javier Tallón Guerri
- Juan M. Tenorio del Moral - UGR

Comunicaciones Seguras

Teoría: 16h. Prácticas: 19h. Tutorías: 9h. Examen: 1h.

TEORÍA:

1. Seguridad en capa de enlace: redes fijas e inalámbricas
2. Seguridad en capa de red
3. Seguridad en capa de transporte
4. Seguridad en capa de aplicación

PRÁCTICAS:

1. Seguridad y autenticación: sistema RADIUS
2. Seguridad inalámbrica con Aircrack-ng
3. Despliegue de TLS/SSL
4. Servicios de aplicación seguros

Profesorado:

- Dr. Pedro García Teodoro - UGR
  Coordinador de la asignatura
- Dr. Rafael Alejandro Rodríguez Gómez - UGR

Acceso a Redes y Sistemas

Teoría: 18h. Prácticas: 17h. Tutorías: 9h. Examen: 1h.

TEORÍA:

1. Seguridad perimetral y cortafuegos: filtrado y *proxy* (+dinámicos)
2. *Firewalls* inteligentes de nueva generación (NGFW)
3. Tecnologías y sistemas AAA. Protocolos

PRÁCTICAS:

1. Instalación y configuración de cortafuegos con IPTABLES y CISCO
2. *Firewalls* inteligentes
3. Puesta en marcha de sistemas AAA
4. Manejo de redes privadas virtuales

4. Encapsulado de tráfico de red. Protocolos: PPP, IP-IP, GRE
5. Infraestructuras de redes privadas virtuales. Protocolos PPTP, L2TP, SSL
6. Comunicaciones anónimas: redes TOR

5. Despliegue, configuración y uso de redes TOR

Profesorado:

- Dr. Roberto Magán Carrión - UGR
  Coordinador de la asignatura
- Juan M. Tenorio del Moral - UGR

Administración de la Ciberseguridad

Sistemas de Ciberdefensa

Teoría: 16h. Prácticas: 19h. Tutorías: 9h. Examen: 1h.

TEORÍA:

1. Introducción
2. Líneas defensivas de un sistema
3. Sensores de ciberdefensa: tipos, configuración y parsing
4. Integración de datos y detección pasiva
5. Sistemas de detección activa
6. Mecanismo de respuesta
7. Estructura de un CERT

PRÁCTICAS:

1. Monitorización y captura de tráfico
2. Integración: NSM, SIEM, Machine Learning
3. Detección activa y *honeypots*
4. Respuesta a incidentes

Profesorado:

- Dr. José Camacho Páez - UGR
  Coordinador de la asignatura
- Luis Pablo del Árbol Pérez – 11Paths
- Dr. Noemí Marta Fuentes Garc – Fidesol
- Manuel García Cárdenas – Everis
- Antonio Muñoz Ropa – CSIRC- UGR

Hacking Ético

Teoría: 24h. Prácticas: 23h. Tutorías: 12h. Examen: 1h.

TEORÍA:

1. Conceptos básicos sobre *hacking* ético
2. Metodología de las auditorías y tests de penetración
3. Técnicas para la auditoría (*pentesting*):
    a. Recopilación de información
    b. Enumeración
    c. Análisis
    d. Explotación
    e. Persistencia
    f. Documentación

PRÁCTICAS:

1. *Footprinting* y fingerprinting
2. Explotación de memoria
3. Explotación con *Metasploit*
4. Retos de *hacking* ético

Profesorado:

- Dr. Gabriel Maciá Fernández - UGR
  Coordinador de la asignatura
- Alberto Casares Andrés - 4IQ

Análisis Forense de Sistemas y Redes

Teoría: 17h. Prácticas: 18h. Tutorías: 9h. Examen: 1h.

TEORÍA:

1. Fundamentos de forense digital
2. Cibercrimen: normativa e investigación
3. Forense de sistemas y redes
4. Peritaje e Informe forense
5. Forense de dispositivos móviles e IoT
6. Forense de la nube y criptomonedas

PRÁCTICAS:

1. Forense de sistemas
2. Forense de redes
3. Reto de análisis forense

Profesorado:

- Dr. José Ant. Gómez Hernández - UGR
  Coordinador de la asignatura
- Antonio Camarero Calvo - GC
- Francisco Javier García Hernández - GC
- Fco. Rodriguez Gómez - CNP

Análisis de malware

Teoría: 12h. Prácticas: 20h. Tutorías: 4h. Examen: 1h.

TEORÍA:

1. Introducción al análisis de malware
2. Análisis estático de malware
3. Análisis dinámico de malware
4. Funcionalidades avanzadas de malware

PRÁCTICAS:

1. Ejercicios de análisis estático
2. Ejercicios de análisis dinámico
3. Análisis de malware avanzado

Profesorado:

- Dr. Gustavo Romero López - UGR
  Coordinador de la asignatura
- Javier Tallón Guerri - JTSec

Módulo: Ciberseguridad Aplicada

Ciberseguridad aplicada

Teoría: 4h. Prácticas: 6h. Tutorías: 9h. Examen: 1h.

TEORÍA:

1. Introducción
2. Aspectos normativos de la ciberseguridad
3. El entorno de la transformación digital: Riesgo digital y resiliencia
4. Modalidades de comercialización de seguridad: Licencias, servicios, consultoría, paquetes.

PRÁCTICAS:

1. Contenidos normativos en proyectos de ciberseguridad
2. Comercialización práctica de la ciberseguridad

Profesorado:

- Margarita Robles Carrillo - UGR
  Coordinadora de la asignatura
- Luis Pablo del Árbol García - Externo -
  Eleven Paths - Telefónica

Trabajo Fin de Máster (TFM)

Desarrollo que evidencie los conocimientos y capacidades adquiridos en el Máster (90 h). Tutores: cualquier profesor del Máster.

Las plantillas para la memoria, en formato Word y Latex, se pueden descargar aquí.

Distribución de las asignaturas por trimestres (7ª edición - curso 22/23):

1º trimestre

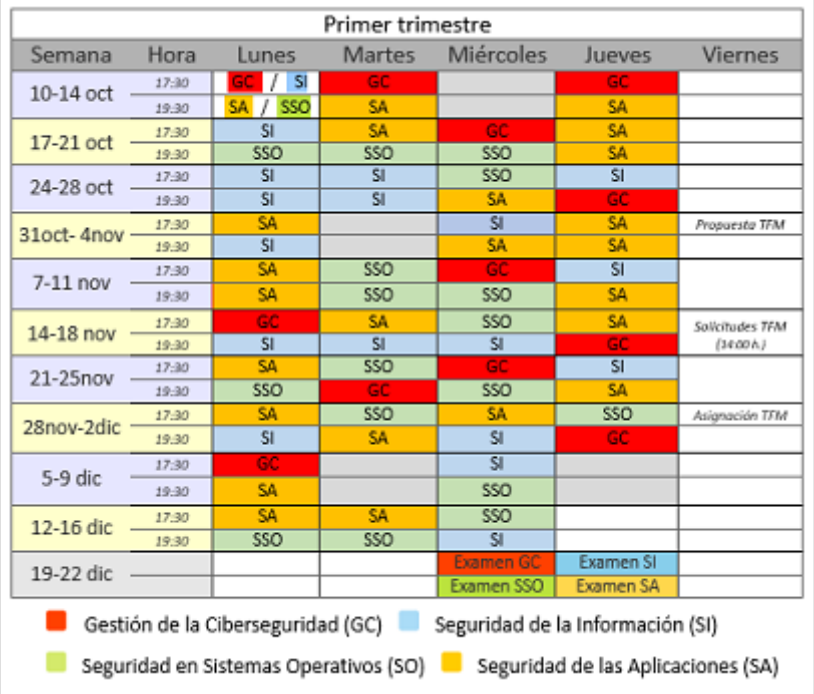
10 octubre de 2021 a 22 diciembre de 2022
Aula de Teoría/Prácticas: Aula 0.4 (Edificio Auxiliar de la ETSIIT)

Gestión de la Ciberseguridad (GC)

Seguridad de la Información (SI)

Seguridad en Sistemas Operativos (SSO)

Seguridad de Aplicaciones (SA)



2º trimestre:

9 enero a 23 marzo de 2023
Aula de Teoría/Prácticas: Aula 0.4 (Edificio Auxiliar de la ETSIIT)

Ciberderecho (Cd)

Comunicaciones Seguras (CS)

Sistemas de Ciberdefensa (SC)

Hacking Ético (HE)

Segundo trimestre

Semana	Hora	Lunes	Martes	Miércoles	Jueves	Viernes
9-13 ene	17:30	Cd - CS	CS	SC	Cd	
	19:30	HE - SC	HE	CS	HE	
16-20 ene	17:30	CS	Cd	SC	CS	
	19:30	HE	HE	Cd	HE	
23-27 ene	17:30	SC	CS	Cd	Cd	
	19:30	HE	HE	SC	CS	
30ene-3feb	17:30	SC	HE	CS	HE	
	19:30	CS	HE	SC	CS	
6-10 feb	17:30	SC	CS	Cd	HE	
	19:30	CS	HE	Cd	HE	
13-17 feb	17:30	SC	HE	SC	HE	
	19:30	CS	HE	SC	HE	
20-24 feb	17:30	CS	HE	Cd	SC	
	19:30	SC	HE	CS	SC	
27feb-3mar	17:30	HE		Cd	HE	
	19:30	SC		CS	SC	
6-10 mar	17:30	HE	HE	Cd	SC	
	19:30	CS	CS	Cd	SC	
20-24 mar	18:00			Examen CS	Examen SC	
	19:00			Examen Cd	Examen HE	

Ciberderecho (Cd) Comunicaciones Seguras (CS)

Sistemas de Ciberdefensa (SC) *Hacking* Ético (HE)

3º trimestre

27 marzo a 23 mayo de 2023
Aula de Teoría/Prácticas: Aula 0.4 (Edificio Auxiliar de la ETSIIT)

Acceso a Redes y Sistemas (ARS)

Análisis Forense de Sistemas y Redes (AFSR)

Análisis de Malware (AM)

Ciberseguridad Aplicada (CA)

Tercer trimestre

Semana	Hora	Lunes	Martes	Miércoles	Jueves	Viernes
27-31mar	17:30	ARS / AM	ARS	AM	AFSR	
	19:30	AFSR	AFSR	ARS	AFSR	
10-14 abr	17:30		AFSR	CA	ARS	
	19:30		ARS	ARS	AM	
17-21 abr	17:30	AFSR	AM	AM	CA	
	19:30	ARS	ARS	ARS	CA	
24-28 abr	17:30	ARS	AFSR	AFSR	AFSR	
	19:30	AFSR	AFSR	AFSR	AFSR	
1-5 abr	17:30		AM		AFSR	
	19:30		AM		ARS	
8-11 may	17:30	ARS	ARS		AFSR	
	19:30	CA	AM		AFSR	
15-19 may	17:30	AM	AM	CA	AFSR	
	19:30	ARS	ARS	AM	ARS	
22-26 may	17:30	ARS	ARS			
	19:30	AFSR	AM			
29-30may	17:30	Exa. ARS	Examen CA			
	19:00	Examen AM	Exa. AFSR			

Análisis Forense de Sistemas y Redes (AFSR) Análisis de *Malware* (AM)

Acceso a Redes y Sistemas (ARS) Ciberseguridad Aplicada (CA)

Presentación y defensa de los TFMs de la VI Edición:

Calendario:

Convocatoria ordinaria (julio):

- Indicación de entrega/defensa y modalidad (presencial/*online*): notificar a través de la actividad correspondiente en la asignatura TFM de Prado, hasta el **4 de julio** de 2023, 14:00 h.

- Entrega del PDF de la memoria: subir la memoria a la actividad correspondiente en Prado hasta el **13 julio** de 2023, 14:00 h.

- Defensa: presencial/*online* ante la Comisión de evaluación, **20, 21 o 22 de julio** de 2023, según el día y hora que establezca la comisión de evaluación.

Convocatoria extraordinaria (septiembre):

- Entrega del PDF de la memoria indicando la modalidad de defensa (presencial/*online*): subir la memoria a la actividad correspondiente en Prado, hasta el **7 de septiembre** de 2023, 14:00 h.

- Defensa: presencial/*online* ante la Comisión de evaluación, **13-15 de septiembre** de 2023, según el día y hora que establezca la comisión de evaluación

Plantillas:

Se puede descargar aquí el archivo con las plantillas para la memoria del TFM en formato docx y latex.