uc3m | Universidad Carlos III de Madrid

DENOMINACIÓN ASIGNATURA: Sistemas de Ciberdefensa		
MÁSTER: Máster Universitario en Ciberseguridad	**CURSO: 1º**	**CUATRIMESTRE: 1º**

PLANIFICACIÓN SEMANAL DE LA ASIGNATURA

SEMANA	SESIÓN	DESCRIPCIÓN DEL CONTENIDO DE LA SESIÓN	GRUPO (marcar X)		Indicar espacio distinto de aula (aula informática, audiovisual, etc.)	Indicar SI/NO es una sesión con 2 profesores	TRABAJO SEMANAL DEL ALUMNO		
			GRANDE	PEQUEÑO			DESCRIPCIÓN	HORAS PRESENCIALES	HORAS TRABAJO (Max. 7h semana)
1	1	**Presentación de la asignatura** **Introducción a la Ciberdefensa**	X				Repasar contenidos de la sesión 1. Completar tareas del lab., si es necesario. Preparar sesiones 3 y 4.	1,66	
	2	**Mini-lab: Configuración del entorno virtual**		X	Lab.			1,66	4
2	3	**Sensores locales: Auditoría y análisis de eventos (I)**: Introducción a los sensores locales **Mini-lab: Rsyslog**		X	Lab.		Repasar contenido de las sesiones 3 y 4. Completar tareas de los mini-labs., si es necesario. Preparar sesión 5 y mini-labs.	1,66	
	4	**Sensores locales: Auditoría y análisis de eventos (II)**: Gestión de usuarios y accesos **Mini-lab: Gestión de usuarios**		X	Lab.			1,66	4
3	5	**Sensores locales: Auditoría y análisis de eventos (III)**: Análisis de logs de seguridad **Mini-lab: Rotación de logs**		X	Lab.		Repasar contenido de la sesión 5. Completar tareas mini-lab., si es necesario. Preparar sesiones 7 y 8.	1,66	
	6	**Mini-lab: Configuración de logs**		X	Lab.			1,66	4
4	7	**Firewalls y segmentación de redes (I)**: Fundamentos de filtrado de tráfico	X				Repasar contenidos de las sesiones 7 y 8. Preparar sesión 9.	1,66	
	8	**Firewalls y segmentación de redes (II)**: Tipos de cortafuegos	X					1,66	3
5	9	**Firewalls y segmentación de redes (III)**:	X				Repasar contenidos de la sesión 9.	1,66	4

		Segmentación de redes					Completar tareas del mini-lab, si es necesario. Preparar laboratorio firewall.		
	10	**Mini-lab: iptables**		X	Lab.			1,66	
6	11	**Laboratorio de Firewalls (I)**		X	Lab.	Sí	Completar tareas del lab., si es necesario. Editar entregable del laboratorio. Preparar sesiones 13 y 14.	1,66	
	12	**Laboratorio de Firewalls (II)**		X	Lab.	Sí		1,66	7
7	13	**Sistemas de Detección y Prevención de Ataques (I)**: Detección de firmas de ataques	X					1,66	
	14	**Sistemas de Detección y Prevención de Ataques (II)**: Detección de anomalías	X				Repasar contenidos de las sesiones 13 y 14. Preparar sesiones 15 y 16.	1,66	3
8	15	**Sistemas de Detección y Prevención de Ataques (III)**: Prevención de ataques	X				Repasar contenidos de la sesión 15. Completar tareas del mini-lab., si es necesario. Preparar laboratorio IDS/IPS.	1,66	
	16	**Mini-lab: Snort**		X	Lab.			1,66	4
9	17	**Laboratorio de IDS/IPS (I)**		X	Lab.	Sí	Completar tareas lab., si es necesario. Editar entregable del laboratorio. Preparar sesiones 19 y 20.	1,66	
	18	**Laboratorio de IDS/IPS (II)**		X	Lab.	Sí		1,66	7
10	19	**Sistemas de Gestión de Eventos e Información de Seguridad (SIEM) (I)**: Conceptos y arquitecturas de SIEMs	X					1,66	
	20	**Sistemas de Gestión de Eventos e Información de Seguridad (SIEM) (II)**: Reglas de agregación y correlación	X				Repasar contenido de las sesiones 19 y 20. Preparar sesiones 21 y 22	1,66	3
11	21	**Sistemas de Gestión de Eventos e Información de Seguridad (SIEM) (III)**: Arquitecturas distribuidas de sensores de detección **Mini-lab: OSSIM**		X	Lab.		Repasar contenidos de las sesiones 21 y 22. Completar tareas de los mini-labs., si es necesario. Preparar laboratorio SIEM.	1,66	
	22	**Sistemas de Gestión de Eventos e Información de Seguridad (SIEM) (IV)**: Estrategias de sensorización. **Mini-lab: Normalización de logs**		X	Lab.			1,66	4
12	23	**Laboratorio de SIEM (I)**		X	Lab.	SÍ	Editar entregable del laboratorio. Preparar examen	1,66	
	24	**Laboratorio de SIEM (II)**		X	Lab.	SÍ		1,66	7
							Subtotal	**40**	**54**
TOTAL *(Total 1 + Total 2. <u>Máximo 180 horas</u>)*								**94**	