ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

93001005 - Servicios de Control de Acceso

PLAN DE ESTUDIOS

09AW - Master Universitario En Ciberseguridad

CURSO ACADÉMICO Y SEMESTRE

2019/20 - Primer semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	93001005 - Servicios de Control de Acceso
No de créditos	4.5 ECTS
Carácter	Obligatoria
Curso	Primer curso
Semestre	Primer semestre
Período de impartición	Septiembre-Enero
Idioma de impartición	Castellano
Titulación	09AW - Master Universitario En Ciberseguridad
Centro responsable de la titulación	09 - Escuela Tecnica Superior de Ingenieros de Telecomunicacion
Curso académico	2019-20

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Miguel Jimenez Gañan (Coordinador/a)	D-4311 ETSIINF	m.jimenez@upm.es	Sin horario.
Maria Del Socorro Bernardos Galindo	D-5206 ETSIINF	mariadelsocorro.bernardos@upm.es	Sin horario.

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

2.3. Profesorado externo

Nombre	Correo electrónico	Centro de procedencia
Carlos Lentisco Sánchez	clentisco@upm.es	ETSIT
Juan Carlos Yelmo García	juancarlos.yelmo@upm.es	ETSIT
Vicente Jara Vera	vicente.jara@upm.es	ETSIT
Víctor Villagrá González	victor.villagra@upm.es	ETSIT
Carmen Sánchez ávila	carmen.sanchez.avila@upm.es	ETSIT

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

El plan de estudios Master Universitario en Ciberseguridad no tiene definidas asignaturas previas recomendadas para esta asignatura.

3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Redes de computadores

4. Competencias y resultados de aprendizaje

4.1. Competencias

CB07 - 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

CB10 - 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

CE04 - Capacidad para establecer una categorización de servicios de ciberseguridad para proteger a las infraestructuras conectadas en red.

CE05 - Capacidad de analizar y diseñar servicios de seguridad de control de acceso, protección de la información en tránsito y protección perimetral

CG03 - Dotar al alumno de la capacidad de diseñar e implantar procedimientos de protección de la información asociados con los sistemas de información, las redes y comunicaciones telemáticas y los servicios de Internet, así como en la protección contra el fraude utilizando estos sistemas

CT12 - Aprendizaje autónomo, adaptación a nuevas situaciones y motivación por el desarrollo profesional permanente

4.2. Resultados del aprendizaje

RA10 - Analizar y seleccionar los mecanismos adecuados para proteger las comunicaciones

RA8 - Diseñar un sistema seguro de control de acceso

RA9 - Diseñar un sistema de control perimetral

RA11 - Analizar y seleccionar los mecanismos adecuados para proteger los sistemas y servicios

RA12 - Analizar riesgos de pérdida de privacidad y robo de información y diseñar las soluciones adecuadas

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

La asignatura contempla, desde un punto de vista tanto teórico como práctico, el Control de Acceso desde diferentes puntos de vista. Comienza analizando de manera general diferentes elementos que forman parte del control de acceso y diferentes aproximaciones seguidas para su implementación, A continuación se abordan diferentes tecnologías y métodos para realizar el control de acceso a diferentes recursos y dispositivos en red, incluyendo sistemas centralizados de autenticación y autorización, mecanismos de gestión de identidad en redes de computadores, sistemas de acceso a la red o a dispositivos, así como mecanismos de autenticación actuales como los biométricos o multi-factor.

También se trata el tema de la seguridad perimetral de una red, analizando diferentes tipos de firewalls en base al nivel de la información que contemplan, detallando sus capacidades y limitaciones. Otros elementos contemplados son los detectores de intrusiones (IDS/IPS). Ambas tecnologías se prueban por medio de la experimentación práctica con diferentes tecnologías comprobando su configuración y funcionamiento.

Finalmente, se analizan sistemas utiilzados para capturar y comprobar la actividad maliciosa, así como los mecanismos utilizados en nubes tanto públicas como privadas para controlar el acceso a los recursos, tanto de gestión de la nube como los alojados en ella.

5.2. Temario de la asignatura

1. Introducción al control de acceso
   1.1. Autenticación, autorización y mecanismos de control
   1.2. Modelos de control de acceso: DAC, MAC, RBAC, basado en reglas y basado en contexto
2. Sistemas de control de acceso
   2.1. Tecnologías Single Sign-on
   2.2. Sistemas centralizados: LDAP, RADIUS, TACACS, DIAMETER
   2.3. Network Access Control y 802.X
   2.4. Sistemas basados en biometría
   2.5. Autenticación multi-factor
3. Seguridad perimetral y firewalls
   3.1. Tipos de firewalls
   3.2. Firewalls en el diseño de red
   3.3. Firewalls de filtrado de paquetes
   3.4. Firewalls con estado
   3.5. NAT
   3.6. Sistemas UTM (Gestión Unificada de Amenazas)
4. Sistemas de detección y protección contra intrusiones IDS e IPS
   4.1. Características de IDS/IPS
   4.2. Firmas IPS
   4.3. Gestión y monitorización de IPS
   4.4. Correlación Global
5. Redes trampa
   5.1. HoneyWALLs
   5.2. HoneyPOTs
   5.3. HoneyNETs
6. Control de acceso en la nube

6.1. Mecanismos de control de acceso en nubes públicas y privadas

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	Actividades de evaluación
1				
2				
3	**Tema 1** Duración: 04:00 LM: Actividad del tipo Lección Magistral **Tema 1** Duración: 02:00 PR: Actividad del tipo Clase de Problemas **Tema 2** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 2** Duración: 02:00 PR: Actividad del tipo Clase de Problemas			
4	**Tema 2** Duración: 06:00 LM: Actividad del tipo Lección Magistral **Tema 2** Duración: 02:00 PR: Actividad del tipo Clase de Problemas	**Tema 2** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		
5	**Tema 2** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 3** Duración: 04:00 LM: Actividad del tipo Lección Magistral	**Tema 3** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio		
6	**Tema 3** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 3** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio		
7	**Tema 4** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 5** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Tema 6** Duración: 01:00 LM: Actividad del tipo Lección Magistral	**Temas 4** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio		**Entregas y Trabajos** TG: Técnica del tipo Trabajo en Grupo Evaluación continua y sólo prueba final Duración: 00:00

8				**Examen** EX: Técnica del tipo Examen Escrito Evaluación continua y sólo prueba final Duración: 04:00
9				
10				
11				
12				
13				
14				
15				
16				
17				

Las horas de actividades formativas no presenciales son aquellas que el estudiante debe dedicar al estudio o al trabajo personal.

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
7	Entregas y Trabajos	TG: Técnica del tipo Trabajo en Grupo	Presencial	00:00	40%	/ 10	CB07 CT12 CB10 CE05 CG03
8	Examen	EX: Técnica del tipo Examen Escrito	Presencial	04:00	60%	4 / 10	CE05 CG03 CE04

7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
7	Entregas y Trabajos	TG: Técnica del tipo Trabajo en Grupo	Presencial	00:00	40%	/ 10	CB07 CT12 CB10 CE05 CG03
8	Examen	EX: Técnica del tipo Examen Escrito	Presencial	04:00	60%	4 / 10	CE05 CG03 CE04

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen	EX: Técnica del tipo Examen Escrito	Presencial	04:00	60%	4 / 10	CE05 CG03 CE04

Trabajos y Prácticas. Reentrega de aquellos suspensos	TG: Técnica del tipo Trabajo en Grupo	Presencial	00:00	40%	/ 10	CB07 CT12 CB10 CE05 CG03

7.2. Criterios de evaluación

La evaluación consiste en una mezcla entre trabajos y prácticas propuestas en grupo, y un examen escrito individual. Los trabajos y prácticas computan el 40% de la nota, no siendo obligatorio realizar todos, y el examen individual computa el 60% restante, siendo obligatorio superarlo mínimo con un 4. En la convocatoria extraordinaria se podrán repetir aquellos trabajos o prácticas no superados, o el examen, guardándose la nota de aquellos elementos que se hayan superado.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
The Path to Self-Sovereign Identity	Recursos web	http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
Network Access Control For Dummies	Bibliografía	Jay Kelley; Rich Campagna; Denzil Wessels. For Dummies, 2009
Network Security Assessment, 3rd Edition	Bibliografía	Chris McNab O'Reilly Media, Inc, 2016
Biometrics: Personal Identification in a Networked Society	Bibliografía	A. K. Jain, R. Bolle and S. Pankanti (eds.) Kluwer Academic Press, 1999.

Handbook of Biometrics,	Bibliografía	A. K. Jain, P. Flynn, Patrick, A. (Eds.) Springer, 2008.
Biometric Systems. Technology, Design and Performance Evaluation	Bibliografía	J. L. Wayman, A. K. Jain, D. Maltoni and D. Maio (eds.), Springer, 2005.
Técnicas biométricas aplicadas a la seguridad	Bibliografía	M. Tapiador y J. A. Sigüenza (coord.) Ra-Ma, 2005.
Handbook of Face Recognition	Bibliografía	S. Z. Li and A. K. Jain (eds.) Springer, 2005.
Handbook of Fingerprint Recognition,	Bibliografía	D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar Springer, 2005.
Guidelines on Firewalls and Firewall Policy	Otros	NIST, 2009. https://www.nist.gov/publications/guidelines-firewalls-and-firewall-policy
Firewall Fundamentals: An introduction to network and computer firewall security	Bibliografía	Wes Noonan and Ido Dubrawsky. Cisco Press, 2006