



INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

1 DIRECCIÓN DE POSGRADO

1.1 FORMATO GUÍA PARA REGISTRO DE ASIGNATURAS

Hoja 1 de 3

I. DATOS DEL PROGRAMA Y LA ASIGNATURA

1.1 NOMBRE DEL PROGRAMA: Maestría en Ciencias en Ingeniería de Cómputo

1.2 COORDINADOR DEL PROGRAMA: Dr. José Luis Oropeza Rodríguez

1.3 NOMBRE DE LA ASIGNATURA: Seguridad en dispositivos móviles /Mobile Security

1.4 CLAVE: _____ (Para ser llenado por la SIP)

1.5 TIPO DE ASIGNATURA:

OBLIGATORIA	☐	OPTATIVA	☒
SEMINARIO	☐	ESTANCIA	☐

1.6 NÚMERO DE HORAS:

TEORÍA	80	PRACTICA		T-P	
--------	---------------------------------	----------	----------------------	-----	----------------------

1.7 UNIDADES DE CRÉDITO:

1.8 FECHA DE LA ELABORACIÓN DEL PROGRAMA DE LA ASIGNATURA:

13	12	2013
d	m	a

1.9 SESIÓN DEL COLEGIO DE PROFESORES EN QUE SE ACORDÓ LA IMPLANTACIÓN DE LA ASIGNATURA:

SESIÓN No.	3 Extr
------------	--------

FECHA:	13	11	2013
	d	m	a

1.10 FECHA DE REGISTRO EN SIP:

d	M	a

 (Para ser llenado por la SIP)

II. DATOS DEL PERSONAL ACADÉMICO

2.1 COORD. ASIGNATURA: Dr. Ponciano Jorge Escamilla Ambrosio CLAVE: 10095-EA-14

2.2 PROFR. PARTICIPANTE: Dr. Moisés Salinas Rosales CLAVE: 8657-EC-12

III. DESCRIPCIÓN DEL CONTENIDO DEL PROGRAMA DE LA ASIGNATURA

III.1 OBJETIVO GENERAL:

At the end of the course the student will have a comprehensive understanding of the main information and network security aspects that arise in mobile communication systems, including smartphones and mobile telecommunication systems, wireless sensor networks, the internet of things and safety-critical devices.

III.2 DESCRIPCIÓN DEL CONTENIDO

TEMAS Y SUBTEMAS	TIEMPO
1. Introduction to mobile security 1.1. Smartphones 1.2. Mobile Device Components 1.3. Security Challenges	10 hrs
2. Telecom Security 2.1. General telecom vulnerabilities 2.2. Basics of Telecom Security 2.3. Telecom Security from 1G to 4G	10 hrs
3. Smartphone security 3.1. Mobile operating systems 3.2. OS security models 3.3. Best practices for security and privacy in mobile app development	10 hrs
4. Mobile Internet security 4.1. WiFi Security 4.2. Personal area networks 4.3. Near field communication	10 hrs
5. Mobile location privacy 5.1. Mobile location 5.2. Location-based services 5.3. Location privacy	10 hrs
6. Wireless sensor networks security 6.1. Fundamentals of network security 6.2. Challenges of security in WSNs 6.3. Security attacks in sensor networks 6.4. Protocols and mechanisms for security 6.5. IEEE 802.15.4 and ZigBee security	10 hrs
7. Internet of things security 7.1. RFID Security 7.2. SCADA Security 7.3. M2M Security	10 hrs

8. Security in safety-critical devices 8.1. Medical devices 8.2. Vehicle safety 8.3. Smart grid 8.4. Other safety-critical areas	10 hrs

III.3 BIBLIOGRAFIA UTILIZADA EN LA ASIGNATURA

Books

1. John R. Vacca, Computer and Information Security Handbook, 2nd Edition, Morgan Kaufmann, 2013.
2. Frank Adelstein, Sandeep K.S. Gupta, Golden G. Richard III, and Loren Schwiebert, Fundamentals of Mobile and Pervasive Computing, McGraw-Hill, 2005.
3. Nouredine Boudriga, Security of Mobile Communications, CRC Press, 2010.
4. Levente Buttyán and Jean-Pierre Hubaux, Security and Cooperation in Wireless Networks, Cambridge University Press, 2007.
5. Abhishek Dubey and Anmol Misra, Android Security: Attacks and Defenses, CRC Press, 2013.
6. Himanshu Dwivedi, Chris Clark, and David Thiel, Mobile Application Security, McGraw-Hill, 2010
7. Patrick Traynor, Patrick McDaniel, and Thomas La Porta, Security for Telecommunications Networks, Springer, 2008.

Recommended paper reading list

Links to additional reading lists:

1. <http://cups.cs.cmu.edu/courses/ups-sp14/>
2. <http://www.cl.cam.ac.uk/~rja14/book.html>

III.4 PROCEDIMIENTOS O INSTRUMENTOS DE EVALUACIÓN A UTILIZAR

Performance on the course will be assessed with the following criteria:

Midterm Exam 30%

Final Exam 20%

Homework 20%

Final Project 30%