INSTITUTO POLITÉCNICO NACIONAL

SECRETARIA DE INVESTIGACIÓN Y POSGRADO

DIRECCIÓN DE POSGRADO

FORMATO GUÍA PARA REGISTRO DE ASIGNATURAS

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: **Ciberseguridad** / Cibersecurity

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

1.5 TIPO DE ASIGNATURA:

OBLIGATORIA		OPTATIVA	**X**
SEMINARIO		ESTANCIA	

1.6 NÚMERO DE HORAS:

TEORÍA	**X**	PRACTICA		T-P	

1.7 UNIDADES DE CRÉDITO: **8**

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. Moisés Salinas Rosales CLAVE: 8657-EC-12

2.2 PROFR. PARTICIPANTE: Dr. Eleazar Aguirre Anaya CLAVE: 8954-EC-12

2.3 PROFR. PARTICIPANTE: Dr. Ponciano Jorge Escamilla Ambrosio CLAVE: 10095-EA-14

III. DESCRIPCIÓN DEL CONTENIDO DEL PROGRAMA DE LA ASIGNATURA

III.1 OBJETIVO GENERAL:

At the end of the course the student will have a holistic perspective on the structure of the cyberspace ecosystem. Topics include global networking and communication, data mining and information fusion, secure networks and intrusion detection, forensic computing and investigation, incident response and risk management, security and privacy, and policy and assurance issues. The course also features expert lectures and case-based projects on cybersecurity in several areas including healthcare, finance, media, government, defense, and critical infrastructure

III.2 DESCRIPCIÓN DEL CONTENIDO

TEMAS Y SUBTEMAS	TIEMPO
1. Introduction to Cybersecurity 1.1. Requirements for information security on Cyberspace 1.2. Technologies for Cybersecurity 1.3. Research on Cybersecurity	8 hr.
2. Ethics in Cyber Security & Cyber Law 2.1. Privacy 2.2. Intellectual Property 2.3. Professional Ethics 2.4. Freedom of Speech 2.5. Fair User and Ethical Hacking 2.6. Internet Fraud 2.7. Electronic Evidence 2.8. Cybercrimes 2.9. Cyberwarfare	10 hr.
3. Information Security Fundamentals and Best Practices 3.1. Protecting Computer System and its Contents 3.2. Securing Computer Networks 3.3. Compromised Computers 3.4. Secure Communications 3.5. Information Security Best Practices 3.6. Privacy Guidelines 3.7. Safe Internet Usage 3.8. Incident Management and Response	12 hr.
4. Network Security 4.1. Network attack techniques 4.2. Network defend approaches 4.3. Traffic tracking and analysis 4.4. Secure routing protocols 4.5. Protocol scrubbing 4.6. Reaction techniques for network attacks 4.7. Network Server's Operating Systems Security	14 hr.

5. Secure Software and Browser Security 5.1. Software Construction 5.2. Software Design and Architecture 5.3. Software Testing 5.4. Methodologies 5.5. The Web Model 5.6. Browser Security 5.7. HTML5 Security	14 hr.
6. Forensics 6.1. Forensic Technologies 6.2. Digital Evidence Collection 6.3. Evidentiary Reporting	4 hr.
7. Cybersecurity in critical infrastructure 7.1. Critical infrastructure concept 7.2. Cybersecurity requirements of critical infrastructure 7.3. Critical infrastructure protection 7.4. SCADA and control systems cybersecurity	10 hr.
8. Resiliency and Information Risk Management 8.1. Asset Evaluation and Business Impact Analysis 8.2. Risk Identification 8.3. Risk Quantification 8.4. Risk Response Development and Control 8.5. Security Policy, Compliance, and Business Continuity	8 hr.

III.3 BIBLIOGRAFIA UTILIZADA EN LA ASIGNATURA

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. Noureddine 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. Chwan-Hwa Wu and J. David Irwin, Introduction to Computer Networks and Cybersecurity, 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.
8. Shoemaker, D. and Conklin, W.A., Cybersecurity: The essential body of knowledge, Course Technology, Cengage Learning, USA, 2012.
9. Selected papers on the literature.

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%