



**INSTITUTO POLITECNICO NACIONAL**  
**SECRETARIA DE INVESTIGACION Y POSGRADO**  
**DIRECCIÓN DE ESTUDIOS DE POSGRADO**

*FORMATO GUIA PARA REGISTRO DE ASIGNATURAS*

Hoja 1 de 3

### I. DATOS DEL PROGRAMA Y LA ASIGNATURA

1.1 NOMBRE DEL PROGRAMA: MAESTRÍA EN TECNOLOGÍA DE CÓMPUTO

1.2 COORDINADOR DEL PROGRAMA: DR. JUAN CARLOS HERRERA LOZADA

1.3 NOMBRE DE LA ASIGNATURA: SEGURIDAD INFORMÁTICA

1.4 CLAVE: 07A5139 (Para ser llenado por la SIP)

1.5 TIPO DE ASIGNATURA:

	OBLIGATORIA	<input type="checkbox"/>	OPTATIVA	<input checked="" type="checkbox"/>
	SEMINARIO	<input type="checkbox"/>	ESTANCIA	<input type="checkbox"/>

1.6 NUMERO DE HORAS: **72**

	TEORIA	<input type="checkbox"/>	PRACTICA	<input type="checkbox"/>	T-P	<b>4</b>
--	--------	--------------------------	----------	--------------------------	-----	----------

1.7 UNIDADES DE CREDITO:

	<b>8</b>
--	----------

1.8 FECHA DE LA ELABORACION DEL PROGRAMA DE LA ASIGNATURA:

	17	05	2013
	d	m	a

1.9 SESION DEL COLEGIO DE PROFESORES EN QUE SE ACORDO LA IMPLANTACION DE LA ASIGNATURA:

	SESION No.	7a.	EXT		FECHA:	12	06	2013
						d	m	a

1.10 FECHA DE REGISTRO EN SIP:

				(Para ser llenado por la SIP)
	d	m	a	

### II. DATOS DEL PERSONAL ACADEMICO

2.1 COORD. ASIGNATURA: EDUARDO RODRÍGUEZ ESCOBAR CLAVE: 8595-ED-12

2.2 PROFR. PARTICIPANTE: VICTOR MANUEL SILVA GARCÍA CLAVE: 8813-ED-12

ROLANDO FLORES CARAPIA CLAVE: 7953-EC-11

MARLON DAVID GONZÁLEZ RAMÍREZ CLAVE: 8733-EB-12

### III. DESCRIPCION DEL CONTENIDO DEL PROGRAMA DE LA ASIGNATURA

#### III.1 OBJETIVO GENERAL:

QUE EL ESTUDIANTE

1. DETECTE VULNERABILIDADES

2. RECONOZCA Y CARACTERICE LOS DIFERENTES TIPOS DE ATAQUES

3. APLIQUE LAS MEDIDAS DE SEGURIDAD BÁSICAS

4. INTERPRETE LAS NORMAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA

#### III.2 DESCRIPCION DEL CONTENIDO

TEMAS Y SUBTEMAS	TIEMPO
1. Introducción a la seguridad informática 1.1 Conceptos básicos 1.2 Usuarios domésticos 1.3 Entornos Empresariales 1.4 Errores de programación 1.5 Agujeros de seguridad en los sistemas operativos 1.6 Software dañino	16 hrs.
2. Ataques 2.1 Caracterización 2.2 Clasificación 2.3 Detección 2.4 Prevención 2.5 Principios del análisis forense	20 hrs.
3. Planeación de soluciones de seguridad 3.1 Estrategias de seguridad física y lógica 3.2 Métodos y políticas 3.3 Usuarios 3.4 Tecnología 3.5 Servicio y soporte	20 hrs.
4. Normas y estándares 4.1 Organismos de estandarización (ISO, ANSI, IEC) 4.2 Gestión 4.3 Auditoría 4.4 Certificación	16 hrs.

