



## INFORMACIÓN GENERAL

<b>Materia</b>	Seguridad en Sistemas de Información
<b>Titular / Cotitular</b>	Luis Julián Domínguez Pérez / Jezreel Mejía Miranda / Mirna Muñoz Mata
<b>Fecha de elaboración</b>	2015-04-09

## INTRODUCCIÓN GENERAL DE LA MATERIA

Este es un curso de introducción a un campo muy amplio de la computación, redes y la seguridad informática. Se cubrirán temas de seguridad computacional, de seguridad en la red, así como de los aspectos relevantes de criptografía.

## OBJETIVO GENERAL

Revisar los aspectos generales de la seguridad en sistemas de información que afectan los sistemas informáticos.

## OBJETIVOS PARTICULARES

El objetivo de este curso es de interesar a los asistentes en las diversas áreas de la computación que requieren atención específica sobre aspectos de seguridad, así como de mostrar las consecuencias de un uso inadecuado de los recursos informáticos, y sus posibles soluciones.

Se busca sentar las bases de la criptografía necesaria para proveer de servicios de seguridad y aplicaciones. Se conocerán las herramientas existentes para el experto en seguridad, y los aspectos de administración de la seguridad de los sistemas de información

También se busca que al terminar el módulo, los asistentes se profundice en estos temas.

## TEMARIO

1. Introducción
  - Introducción a la seguridad en los sistemas de información
  - Conceptos generales de la seguridad de la información
2. Criptografía
  - Introducción a la criptografía
    - Introducción a la criptografía
    - Criptografía Simétrica
    - Criptografía Asimétrica
    - Infraestructura de Llave Pública (PKI)
  - Criptografía en la seguridad de la información
    - Firmas digitales
    - Privacidad y Seguridad
    - Tópicos selectos de criptografía aplicada
3. Seguridad Perimetral
  - Modelo TCP/IP

- Modelo TCP/IP
  - IGMP
  - IP
  - TCP/UDP
- Seguridad en redes
  - Intranet, Extranet, Internet. DMZ
  - Planeación de una red de datos
  - Segmentación en IPv4, e IPv6
  - SNMP
  - Políticas de acceso
  - Administración de la red, y sus herramientas
- Seguridad perimetral
  - Firewall
  - Mecanismos de prevención y detección de intrusos
  - Pasarelas de aplicación
- Redes privadas virtuales
- Privacidad en la red
  - Seguridad versus privacidad
  - Técnicas de anonimato en la red
- 4. Seguridad del Software y políticas de seguridad
  - Estándares y mejores prácticas de la seguridad de la información en el desarrollo del software
  - Certificaciones relacionadas a la seguridad en sistemas de información
  - ISO 27001 - Sistemas de Gestión de Seguridad de la Información
  - Principales controles y mecanismos para la detección y mitigación de riesgos de seguridad en aplicaciones
  - Creación y gestión de políticas de seguridad informática
  - Vulnerabilidades de software

### BIBLIOGRAFÍA

No.	Título	Autor	Editorial	Año
1	An introduction to mathematical cryptography. ISBN: 978-0-387-77993-5	Hofftein, Pipher, Silverman	Springer	2008
2	Understanding cryptography. ISBN: 978-3-642-04100-6	Paar, Pelzl	Springer	2010
3	???			
4	???			

**NOTA:** El docente y el alumno pueden hacer uso de la biblioteca digital [http://www.cimat.mx/es/Catalogos\\_Servicios\\_en\\_Linea](http://www.cimat.mx/es/Catalogos_Servicios_en_Linea) pueden acceder utilizando correo institucional, utilizando su cuenta y contraseña.



CENTRO DE  
INVESTIGACIÓN EN  
MATEMÁTICAS, A.C.

## MAESTRÍA EN INGENIERÍA DE SOFTWARE

Plan de Estudios 2015

---

### EVALUACIÓN

ASPECTO A EVALUAR	PORCENTAJE
Examen escrito	50
Programas	30
Ensayos	20
Total	100