

**GOBIERNO CONSTITUCIONAL DEL ESTADO LIBRE Y SOBERANO DE OAXACA  
INSTITUTO ESTATAL DE EDUCACIÓN PÚBLICA DE OAXACA  
COORDINACIÓN GENERAL DE PLANEACIÓN EDUCATIVA  
COORDINACIÓN GENERAL DE EDUCACIÓN MEDIA SUPERIOR Y SUPERIOR**

**PROGRAMA DE ESTUDIO**

NOMBRE DE LA ASIGNATURA

**Seguridad Computacional**

CICLO

CLAVE DE LA ASIGNATURA  
**20901RC**

TOTAL DE HORAS  
**85**

OBJETIVO(S) GENERAL(ES) DE LA ASIGNATURA

El alumno conocerá, identificará, evaluará e instalará diferentes técnicas, mecanismos, políticas y arquitecturas más utilizadas para el establecimiento de la seguridad en una red computacional.

TEMAS Y SUBTEMAS

- 1. Introducción a la seguridad en redes.**
  - 1.1 Vulnerabilidades, riesgos y ataques.
  - 1.2 Elementos de seguridad, identificación y autenticación, control de acceso, no repudio y responsabilidad.
  - 1.3 Organizaciones, estándares y certificaciones.
- 2. Mecanismos de seguridad basados en criptografía**
  - 2.1 Áreas de la criptología.
  - 2.2 Máquinas criptográficas.
  - 2.3 Clasificación de los algoritmos criptográficos: simétricos y asimétricos.
  - 2.4 Algoritmos criptográficos simétricos.
  - 2.5 Algoritmos criptográficos asimétricos.
  - 2.6 Certificados digitales.
  - 2.7 Infraestructura para uso y administración de los certificados digitales.
- 3. Protocolos y herramientas de seguridad**
  - 3.1 Protocolos de la capa de red.
  - 3.2 Protocolos de la capa de transporte.
  - 3.3 Protocolos de la capa de aplicación.
  - 3.4 Protocolos en tiempo real.
  - 3.5 Relación entre herramientas, servicios y políticas de seguridad.
  - 3.6 Programas para generar o quebrantar contraseñas.
- 4. Tendencias en seguridad**
  - 4.1 Sistemas de detección de intrusos.
  - 4.2 Herramientas para la detección de intrusos.
  - 4.3 Cómputo forense.
  - 4.4 Herramientas para el cómputo forense.
- 5. Diseño de sistemas seguros**
  - 5.1 Políticas de seguridad.
  - 5.2 Evaluación de las medidas de seguridad.
  - 5.3 Metodologías de la seguridad en las organizaciones.
  - 5.4 Metodologías de la seguridad en los sistemas.
  - 5.5 Mantenimiento de sistemas seguros.

ACTIVIDADES DE APRENDIZAJE

Sesiones dirigidas por el profesor. Las sesiones se desarrollarán utilizando medios de apoyo didáctico como son la computadora, el proyector de video y el uso de software (preferentemente de distribución libre).



**COORDINACIÓN  
GENERAL DE EDUCACIÓN  
MEDIA SUPERIOR Y SUPERIOR**

Asimismo, se realizarán programas de cómputo y se desarrollarán problemas aplicables a cada unidad. Los profesores a cargo de la asignatura deberán ponerse previamente de acuerdo e informarán a los alumnos sobre los algoritmos, herramientas y protocolos que se estudiarán a lo largo del curso.

#### CRITERIOS Y PROCEDIMIENTOS DE EVALUACIÓN Y ACREDITACIÓN

La calificación final de la materia se conforma de tres evaluaciones parciales y una evaluación final. Todas las evaluaciones deben incluir al menos un examen, un proyecto, tareas, prácticas, investigaciones, exposiciones, etc., según lo considere el profesor a cargo.

La evaluación final puede incluir un proyecto final, que abarque los conocimientos adquiridos a lo largo del curso.

Los elementos a considerar en cada evaluación, así como el alcance y requerimientos de los proyectos los asignará el profesor a cargo, preferentemente al inicio del semestre o al inicio de cada evaluación. La suma de todos los criterios y procedimientos de evaluación y acreditación deberán integrar el 100% de la calificación.

#### BIBLIOGRAFÍA

##### Bibliografía básica:

- **Computer communications security principles, standard protocols and techniques**, Ford, Warwick, Prentice Hall, 1993
- **Técnicas criptográficas de protección de datos**, Fúster, A., RA-MA, 2004, 3ª ed.
- **Network and internetwork security: Principles and practice**, Stallings, William; Prentice Hall and IEEE Press, 1995, 1ª ed.
- **Cryptography and network security: Principles and practice**, Stallings, William, Prentice Hall, 2003, 3ª ed.

##### Bibliografía de consulta:

- **Applied cryptography**, Schneier, Bruce, John Wiley & sons, 1996, 2ª ed.
- **Handbook of applied cryptography**, Menezes, A.; Oorschot, Van; Vanstone, S., CRC Press, 2001, 1ª ed.
- **Digital evidence and computer crime**, Casey, E., Academic Press, 2000, 1ª ed.
- **Network intrusion detection** Northcutt, Stephen; Novak Judy, SAMS, 2002, 3ª ed.
- **Hackers 2 secretos y soluciones para la seguridad de las redes**, McClure Stuart; Scambray Joel; Kurtz, George, McGraw-Hill, 2001, 1ª ed.
- **Hack attacks revealed. A complete reference with custom security hacking toolkit**, Chirillo, J., John Wiley & Sons, 2001, 1ª ed.

#### PERFIL PROFESIONAL DEL DOCENTE

Licenciado en computación, Maestría o Doctorado en Ciencias de la Computación.