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 ESTUDIOS

NOMBRE DE LA ASIGNATURA
SEGURIDAD DE CENTROS DE INFORMÁTICA

CICLO	CLAVE DE LA ASIGNATURA	TOTAL DE HORAS
NOVENO SEMESTRE	RI-04	80

OBJETIVO(S) GENERAL(ES) DE LA ASIGNATURA

Adquirir los conocimientos referentes a la seguridad física y lógica que se deben implementar en los centros de informática y sistemas de información respectivamente. Así como la forma de hacer la recuperación después de un desastre, con la finalidad de comprender y explicar las razones e importancia de mantener la seguridad de la información y de la infraestructura existente en el centro de cómputo.

TEMAS Y SUBTEMAS

1. CONCEPTOS DE SEGURIDAD EN COMPUTACIÓN
    - 1.1. Conceptos básicos de seguridad
    - 1.2. Tipos de centros de cómputo
    - 1.3. Objetivos principales de la seguridad de cómputo
        - 1.3.1. La confidencialidad
        - 1.3.2. La integridad
        - 1.3.3. La disponibilidad
    - 1.4. Definición de una política de seguridad en computación
    - 1.5. Organización y división de responsabilidades
    - 1.6. Documentación concerniente a la seguridad
    - 1.7. Uso y administración de registros o bitácoras
    - 1.8. Políticas hacia el personal
    - 1.9. Función de los auditores internos y los externos

2. CONTROL DE ACCESO
    - 2.1. Protección perimetral
    - 2.2. Identificación y autenticación
    - 2.3. Control de acceso por mandato
        - 2.3.1. Modelo de Bell y LaPadula
        - 2.3.2. Modelo de Biba
        - 2.3.3. Modelo de Clark y Wilson
    - 2.4. Control de acceso criptográfico

2.4.1. Kerberos

2.4.2. Tristrata: seguridad empresarial

3. SEGURIDAD FÍSICA

3.1. Ubicación del edificio o sala para los equipos

3.2. Preparación de espacios, ubicación y construcción del centro

3.3. Acceso: normas de acceso a las salas con equipo; formas y medios para control del acceso

3.4. Factores que intervienen en la seguridad física

3.4.1. Fenómenos naturales

3.4.2. Incendios

3.4.3. Terrorismo

3.5. Planes y simulacros para la recuperación en caso de desastre

3.6. Seguros

4. SEGURIDAD DE LOS SISTEMAS Y APLICACIONES

4.1. Consistencia, funcionalidad e integración de entornos operativos: usuarios, categorías, derechos de acceso

4.2. Llaves de acceso

4.3. Estándares de programación y operación de sistemas

4.4. Respaldos externos y recuperación de la información

4.5. Equipos respaldados en espejo

4.6. Medios de almacenamiento

4.7. Herramientas para reparación y recuperación

4.8. Métodos para evitar la piratería

4.9. Tipos de virus y vehículos de transmisión

4.9.1. Caballos de Troya

4.9.2. Gusanos

4.9.3. Bombas de tiempo

4.9.4. Otros tipos de virus

4.9.5. Negación de permisos

4.9.6. Puertas traseras de las aplicaciones

4.9.7. Antivirus

4.10. Planes y simulacros para la recuperación en caso de desastres

5. SEGURIDAD EN EL MANEJO DE DATOS, CRIPTOGRAFÍA

5.1. Antecedentes históricos

5.2. Cifrados simétricos o de clave privada

5.2.1. Algoritmos antiguos

5.2.2. Cifrado DES

5.3. Cifrados asimétricos o de clave pública

5.3.1. Cifrado RSA

6. SEGURIDAD EN REDES

6.1. Tecnologías de encriptación

6.2. Validación y firmas digitales

6.3. Firewalls

6.4. Virtual Private Network (VPN)

6.5. Protocolos de seguridad

7. DETECCIÓN DE INTRUSOS Y SOBREVIVIENCIA DEL SISTEMA

7.1. Bitácora

7.2. Monitoreo y análisis de los usuarios

7.3. Detección de ataques conocidos

7.4. Monitoreo de tráfico en la red

7.5. Verificación de la integridad de los archivos críticos del sistema

7.6. Tipos de atacantes

7.6.1. Internos

7.6.2. Externos

ACTIVIDADES DE APRENDIZAJE

Sesiones teóricas dirigidas por el profesor, así mismo realizarán trabajos de investigación extra-clase, también se realizará la elaboración de un plan de contingencia y administración de riesgos, para que los alumnos tengan los conocimientos de los puntos básicos a considerar, se tomarán en cuenta las participaciones y se realizarán dinámicas intergrupales.

CRITERIOS Y PROCEDIMIENTOS DE EVALUACIÓN Y ACREDITACIÓN

Se realizan tres evaluaciones parciales y una evaluación ordinaria final de la asignatura.

Para las evaluaciones parciales, se deberá realizar un examen escrito y se podrá complementar la evaluación con exámenes prácticos, avances de proyectos, tareas, investigaciones y otras actividades académicas previamente aprobadas de acuerdo con la normatividad Universitaria. Queda a criterio del profesor la ponderación de todas las actividades.

Para la evaluación ordinaria final, se deberá realizar un examen escrito y se podrá complementar la evaluación con proyectos, exposiciones, tareas e investigaciones realizadas a lo largo del semestre. Queda a criterio del profesor la ponderación de todas las actividades.

Para la calificación final de la asignatura, se establece la ponderación de las evaluaciones parciales y ordinaria final con base en la normatividad de la Universidad.

BIBLIOGRAFÍA (TIPO, TÍTULO, AUTOR, EDITORIAL Y AÑO)

Básica:

• 19 Puntos críticos sobre seguridad del software. Howard, Michael. McGraw-Hill. 2006, 1ª Edición.

• Academia de networking de Cisco Systems: Fundamentos de seguridad de redes: especialista en firewall Cisco. Cisco Press. 2005.

• Administración de la función informática: el factor AFI. Hernández Jiménez, Ricardo. Trillas. 1998

• Computer security handbook. Bosworth, Seymour; Kabay, M. E. Wiley. 2002.

• Cracking sin secretos, ataques y defensas de software. Zemanek, Jakub. Alfaomega. 2004.

• Fundamentos de seguridad de redes. Maiwald, Eric. McGraw-Hill. 2005, 2ª Edición.

• Seguridad de redes: los mejores trucos. Lockhart, Andrew. Anaya Multimedia. 2007, 1ª Edición.

• Seguridad en centros de cómputo: políticas y procedimientos. Fine, Leonard H. Trillas. 2002.

• Seguridad informática: las amenazas y vulnerabilidades más peligrosas al desnudo. Firtman, Sebastian. M.P. Ediciones. 2005.

Consulta:

• Administración de centros de cómputo. Hernández Jiménez, Ricardo. Trillas. 1991, 3ª Edición.

• Administración de datos y archivos por computadora. Arranz, R. Megabyte Noriega. 1994, 2ª Edición.

• Computer security, privacy and politics. Subramanian, Ramesh. IRM Press. 2008.

• Continuous integration: improving software quality and reducing risk. Duvall, Paul; Matyas, Steve; Glover, Andrew. Addison-Wesley, Signature Series. 2007.

• Diseño de seguridad en redes. Kaeo, Merike. Cisco Press. 2003.

• Diseño de un sistema de gestión de seguridad de información: óptica ISO 27001:2005. Alexander Servat, Alberto G. Alfaomega. 2007, 1ª Edición.

• Distributed operating systems: concepts and design. Sinha, Pradeep K. Wiley. 1997.

• El Tao de la monitorización de seguridad en redes: más allá de la detección de intrusiones. Bejtlich, Richard. Pearson. 2005.

• Enciclopedia de la seguridad informática (incluye CD-ROM). Álvaro Gómez Vieites Thy. Alfaomega. 2007, 1ª Edición.

• Fundamentos de comercio electrónico. Elsenpeter, Robert C.; Velte, Toby J. McGraw-Hill. 2001.

• Hackers 3: secretos y soluciones para la seguridad de redes. MacClure, Stuart; Scambray, Joel; Kurtz, George. McGraw-Hill. 2002.

• Hackers en Windows. Scambray, Joel. McGraw-Hill. 2009, 3ª Edición.

• Introducción a la criptografía. Pino Caballero, Gil. Rama. 2003, 2ª Edición.

• Introducing Microsoft Net. Platt, David S. Microsoft Press. 2002, 1ª Edición.

• Linux: administración del sistema y la red. Alegría Loinaz, Iñaki; Cortiñas Rodríguez, Roberto; Ezeiza Ramos, Aitzol. Pearson. 2005.

• Microsoft Windows Server 2008: guía del administrador. Matthews, Marty. McGraw-Hill. 2009, 1ª Edición.

• Network security, a beginner's guide. Maiwald, Eric. McGraw-Hill. 2003, 2ª Edición.

• Official guide to the CISSP. Tipton, Harold F.; Henry, Kevin. Auerbach. 2007.

• Protección Informática. Gratton, Pierre. Trillas. 2002.

• Redes de computadoras. Tanenbaum, Andrew S. Prentice Hall. 2003, 4ª Edición.

• Security planning and disaster recovery. Maiwald, Eric; Sieglein, William. McGraw-Hill. 2002.

• Seguridad de la información. Aceituno Canal, Vicente. Limusa. 2006.

• Seguridad en Linux. Krishnamurthy, Mohan. Anaya Multimedia. 2008, 1ª Edición.

• Seguridad en redes telemáticas. Carracedo, G. McGraw-Hill. 2004, 1ª Edición.

• Seguridad informática, técnicas criptográficas. Pino Caballero. Computec Ra-Ma.

• Seguridad y comercio en el web. Garfinkel, Spafford. McGraw-Hill. 1999.

• Sistemas distribuidos: conceptos y diseño. Coulouris, George; Dollimore, Jean; Kinderberg, Tim. Addison Wesley. 2001, 3ª Edición.

• Sistemas distribuidos: conceptos y diseño. Coulouris, George; Dollimore, Jean; Kinderberg, Tim. Addison Wesley. 2001, 3ª Edición.

• Sistemas operativos modernos. Tanenbaum, Andrew S. Prentice Hall. 2003, 2ª Edición.

• Virus de sistemas informáticos e Internet. Rodao, Jesús de Marcelo. Alfaomega-Rama. 2000.

• Virus informáticos: tipos-protección-diagnosis-soluciones. Levin, Richard B. McGraw-Hill. 1992, 1ª Edición.

PERFIL PROFESIONAL DEL DOCENTE

Licenciatura en Informática, Ingeniería en Sistemas Computacionales o afines, con grado de Maestría y preferentemente de Doctorado en Tecnologías de la Información o afines. Con experiencia profesional y docente de un año.