Programa de Asignatura

Historia del programa

Lugar y fecha de elaboración	Participantes	Observaciones (Cambios y justificaciones)
Cancún, Q. Roo, 20/02/2017	Dr. David Israel Flores Granados	Creación del programa para incorporarse como asignatura básica en Ingeniería en Datos e Inteligencia Organizacional.

Relación con otras asignaturas

Anteriores	Posteriores
IT0322 Teoría de la Información	Negocios digitales
Tema(s) Todos	Tema(s) Pasarelas de pago. Planes de contingencia

Nombre de la asignatura	Departamento o Licenciatura
Seguridad de datos	Ingeniería en Datos e Inteligencia Organizacional

Ciclo	Clave	Créditos	Área de formación curricular
4 - 4	ID0414	8	Licenciatura Básica

Tipo de asignatura	Horas de estudio			
	HT	HP	TH	HI
Seminario	32	32	64	64

Objetivo(s) general(es) de la asignatura

Objetivo cognitivo

Revisar la teoría que sustenta los principales métodos de seguridad en datos para la identificación de los componentes fundamentales que aseguran la integridad, confidencialidad y autentificación durante su transmisión y compartición.

Objetivo procedimental

Determinar los mecanismos adecuados de seguridad en datos para la implementación de aplicaciones, sistemas o configuraciones de dispositivos necesarios que proporcionen la integridad, confidencialidad y autentificación de los datos que se transmiten.

Objetivo actitudinal

Fomentar la responsabilidad en la aplicación de normativas específicas de seguridad para la operación de datos en sistemas.

Unidades y temas

Unidad I. EL PROCESO DE SEGURIDAD

Describir la historia, procesos de seguridad e importancia del aseguramiento de la información para el diseño de políticas de seguridad de datos en organizaciones.

1) Definiciones básicas (Riesgos, Ataques, Intrusos).

2) Servicios de Seguridad en Computadoras, Redes y Comunicaciones

3) Organismos reguladores para la seguridad en la información

Unidad II. CONFIDENCIALIDAD Y AUTENTICIDAD

Explicar el funcionamiento de los principales servicios de Confidencialidad y Autenticidad en redes de comunicación, así como sus características más importantes para su aplicación en la selección de equipos de seguridad.

1) Cifrado Simétrico para la Confidencialidad de la Información

2) Cifrado Asimétrico para la Autentificación de la Información

3) Claves Públicas

4) Aplicaciones de Confidencialidad Aplicaciones de Autenticidad

5) Proyecto integrador

Unidad III. SEGURIDAD EN REDES

Emplear mecanismos de seguridad en redes para la implementación de dispositivos físicos y de software en las organizaciones.

1) Captura y filtrado de tráfico en capas de red y transporte.

2) Arquitecturas de Seguridad IP

3) Secure Socket Layer y Transport Layer Security

4) Secure Electronic Transaction

5) Detección de intrusos

6) Proyecto

Unidad IV. SEGURIDAD EN DATOS PARA ORGANIZACIONES MODERNAS

Precisar situaciones específicas para la aplicación de metodologías y herramientas de seguridad en organizaciones modernas.

1) Seguridad en bases de datos

2) Seguridad para grandes volúmenes de datos.

3) Ingeniería Social

4) Proyecto integrador

Actividades que promueven el aprendizaje

Docente	Estudiante

Promover el trabajo individual en la definición de propuestas de solución a problemas determinados. Coordinar la discusión de casos prácticos. Realizar demostraciones de herramientas y métodos Fomentar la investigación de tópicos en el área. Definir estrategias para identificar las principales ventajas de las TIC en la seguridad de datos.	Realizar tareas asignadas Participar en el trabajo individual y en equipo Resolver casos prácticos Discutir temas en el aula Participar en actividades extraescolares

Actividades de aprendizaje en Internet

Elaborar resúmenes sobre políticas de seguridad y protocolos de seguridad mediante una investigación documental de forma individual y por equipos usando los enlaces de Internet:

http://cseweb.ucsd.edu/~mihir/cse207/ (Consultado el 19/01/2017)
http://cobweb.ecn.purdue.edu/~kak/compsec/Lectures.html (Consultado el 19/01/2017)
http://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/ (Consultado el 20/01/2017)

Criterios y/o evidencias de evaluación y acreditación

Criterios	Porcentajes
Examen	30
Evidencias individuales (investigación, ensayos, lecturas, etc.)	20
Evidencias equipo (ejercicios, casos, proyectos, etc.)	30
Evidencias grupales (asambleas, lluvias de ideas, etc.)	20
Total	100

Fuentes de referencia básica

Bibliográficas

Carr, J. (2011). Inside cyber warfare: Mapping the cyber underworld. (1a. edición) EUA: O'Reilly Media, Inc.

Charles, P., & Pfleeger, S. L. (2012). Analyzing Computer Security: A Threat/vulnerability/countermeasure Approach. (1a. edición) EUA: Prentice Hall.

Goodrich, M., & Tamassia, R. (2010). Introduction to computer security. (1a. edición) EUA: Addison-Wesley Publishing Company.

Stallings, William. (2003). Network Security Essentials: Applications and Standards. (1a. edición) EUA: Prentice Hall.

Vacca, J. R. (2013). Cyber security and IT infrastructure protection. (1a. edición) EUA; Syngress.

Web gráficas

.

Fuentes de referencia complementaria

Bibliográficas

Davies, D. & Price, W. (1989). Security for Computer Networks. (1a.edición) EUA: John Wiley & Sons.

Guerra P, Farris D. (2017). Data Security for Modern Enterprises: Data Security in the World of Cloud Computing, Big Data, Data Science, and Modern Attacks (1a. edición) EUA:O¿ Rilley .

Harrington, Jan L. (2005). Network Security: A Practical Approach. (1a. edición) USA: Morgan Kaufman.

Poole, Owen. (2003). Network Security: A Practical Guide. (1ª. edición) Inglaterra: Butterworth/Heineman.

Web gráficas

.

Perfil profesiográfico del docente

Académicos

Maestría en Tecnologías de la Información, Maestría en Ciencias de la Computación, Maestría en Sistemas.

Docentes

Tener experiencia docente a nivel superior mínima de 3 años.

Profesionales

Tener experiencia en desarrollo de guías instruccionales y sistemas.