UNIVERSIDAD INTERAMERICANA DE PUERTO RICO
RECINTO METROPOLITANO
FACULTAD DE CIENCIAS Y TECNOLOGÍA
DEPARTAMENTO DE CIENCIAS DE COMPUTADORSA Y MATEMÁTICAS
PROGRAMA GRADUADO EN CIENCIAS EN SEGURIDAD DE LA INFORMACIÓN

PRONTUARIO

I. INFORMACIÓN

Título del Curso	:	Seguridad en Base de Datos
Código y Número	:	INSE 5600
Créditos	:	Tres (3)
Término Académico	:	
Profesor(a)	:	
Horas de Oficina	:	
Teléfono de la Oficina	:	787-250-1912 Ext 2230
Correo Electrónico	:	

II. DESCRIPCIÓN

Análisis de medidas y niveles de seguridad aplicados a las bases de datos relacionales en ambientes cliente/servidor así como los derechos de privacidad. Evaluación de los diferentes tipos de vulnerabilidad, los riesgos y las medidas de seguridad en las bases de datos. Requisito: INSE 5101.

III. OBJETIVOS

1. Mencionar de los conceptos fundamentales de bases de datos.
2. Definir de los aspectos primordiales en bases de datos relacionales, orientadas a objetos, jerárquicas y de redes.
3. Definir de los conceptos básicos de seguridad en las bases de datos.
4. Describir de las bases de datos de producción en un ámbito empresarial.
5. Analizar de las destrezas de implementación de base de datos.
6. Describir de los aspectos de seguridad en las bases de datos.
7. Implementar de medidas de seguridad y controles de acceso
8. Identificar y aplicar aspectos legales y forenses de las bases de datos.

IV. CONTENIDO TEMÁTICO

A. Aspectos fundamentales de bases de datos.

1. Diferentes bases de datos incluyendo bases de datos de producción.
    a. Definición de términos

1) Base de datos
2) Llaves primarias y foráneas
2) Lenguaje SQL
3) Creación de Tablas
4) Estructura Lógica y Física de una base de datos
5) DDL
6) DML
7) Diagrama Entidad-Relación

2. Aspectos fundamentales de seguridad.

b. Seguridad de la base de datos.
c. Controles de Acceso.
d. Tipos de cuentas y privilegios de cuentas
e. Auditoría
f. Autenticación
g. Encripción
h. Integridad

3. Riesgos y aspectos vulnerables en sistemas de base de datos (DBMS)
   a. Riesgos en sistemas de base de datos.
   b. Aspectos legales de seguridad
   c. HIPAA Compliance (Privacy and Security)

4. Infraestructura de un sistema de base de datos seguro
   a. Método de autenticación de las bases de datos.
   b. Niveles de protección de bases de datos.
   c. Autenticación con PKI
   d. Probando las vulnerabilidades de SQL
   e. Controles de Acceso en bases de datos.
5. Implementación de las bases de datos.
   a. Aspectos de implementación de las bases de datos.
   b. Medidas de seguridad a implementarse.
   c. Restricciones a las bases de datos.
   d. Aspectos de recuperación de un DBMS.
   e. Aspectos del sistema operativo
   f. Normas y procedimientos para realizar métodos de respaldo y recuperación.
   g. Aspectos forenses y legales de las bases de datos

V. ACTIVIDADES

1. Lecturas
2. Exámenes
3. Ejercicios
4. Proyectos

Revisado por Dr. José R. Vallés diciembre/2016

VI. EVALUACIÓN DEL CURSO:

A. Criterios:	Puntos	Porcientos
1. Exámenes Parciales	100	30 %
2. Proyectos	100	30%
3. Laboratorios	50	10%
4. Examen Final	100	30%
	350	100%

VII. NOTAS ESPECIALES

1. Recuerde que cualquier tarea del curso debe cumplir con el Reglamento General de Estudiantes de Estudiante, Capítulo V, Artículo 1, Sección B.2 que establece "El plagio, la falta de honradez, el fraude, la manipulación o falsificación de datos y cualquier otro comportamiento inapropiado relacionado con la labor académica son contrarios a los principios y normas institucionales y están sujetos a sanciones disciplinarias."

2. Todo estudiante que requiera servicios auxiliares o asistencia especial deberá solicitar los mismos al inicio del curso o tan pronto como adquiera conocimiento de que los necesita, mediante el registro correspondiente en la oficina del Consejero Profesional José Rodríguez, Coordinador de Servicios a los estudiantes con Impedimentos, ubicada en el Programa de Orientación Universitaria.

3. Uso de dispositivos electrónicos

   Se desactivaran los teléfonos celulares y cualquier otro dispositivo electrónico que pudiese interrumpir los procesos de enseñanza y aprendizaje o alterar el ambiente conducente a la excelencia académica. Las situaciones apremiantes serán atendidas, según corresponda. Se prohíbe el manejo de dispositivos electrónicos que permitan acceder, almacenar o enviar datos durante evaluaciones o exámenes.

4. Cumplimiento con las disposiciones del Título IX

   La Ley de Educación Superior Federal, según enmendada, prohíbe el discrimen por razón de sexo en cualquier actividad académica, educativa, extracurricular, atlética o en cualquier otro programa o empleo, auspiciado o controlado por una institución de educación superior independientemente de que esta se realice dentro o fuera de los predios de la institución, si la institución recibe fondos federales.

Revisado por Dr. José R. Vallés diciembre/2016

Conforme dispone la reglamentación federal vigente, en nuestra unidad académica se ha designado un(a) Coordinador(a) Auxiliar de Titulo IX que brindará asistencia y orientación con relación a cualquier alegado incidente constitutivo de discrimen por sexo o género, acoso sexual o agresión sexual. Se puede comunicar con el Coordinador(a) Auxiliar, George Rivera, Director de Seguridad, al teléfono 787-250-1912, extensión 2147, o al correo electrónico grivera@metro.inter.edu .

El Documento Normativo titulado Normas y Procedimientos para Atender Alegadas Violaciones a las Disposiciones del Título IX es el documento que contiene las reglas institucionales para canalizar cualquier querella que se presente basada en este tipo de alegación. Este documento está disponible en el portal de la Universidad Interamericana de Puerto Rico (www.inter.edu).

VIII RECURSOS EDUCATIVOS

Natan, R.B. (2005) Implementing Database Security and Auditing: Includes Examples for Oracle, SQL Server, DB2 UDB, Sybase, Elsevier Press. ISBN:1-55558-334-2

Computadoras

Servicios de Internet

IX. REFERENCIAS

http://www.databasesecurity.com/dbsec-books.htm

http://databases.about.com/od/security/Database_Security_Issues.htm

http://www.bitpipe.com

http://www.governmentsecurity.org/articles/database-security-common-sense-principles.html

IX. BIBLIOGRAFÍA

A. Bibliografía General:

Litchfield,D., Anley, C., Heasman, J. and Grindlay, B.(2005). The database Hackers Handbook : Defending database servers, Indianapolis, Ind:John Wiley & Sons, ISBN:0-7645-7801-4.

Revisado por Dr. José R. Vallés diciembre/2016

Natan, R. B.(2005).Implementing Database Security and Auditing, Elsevier ,Jordan Hill, Oxford, ISBN: 1-555583342

Gertz, M. and Jajodia, S. (2008). Handbook of Database Security Applications and Trends, Springer Publishers, ISBN: 978-0-387-48532-4

Revisado por Dr. José R. Vallés diciembre/2016