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

I. INFORMACION GENERAL

Título del Curso	: Desarrollo de Proyecto en Seguridad
Código y Número	: INSE 6980
Créditos	: Tres (3)
Término Académico	:
Profesor	:
Horas de Oficina	:
Teléfono de la Oficina	: (787)250-1912
Correo Electrónico	:

II. DESCRIPCIÓN

Desarrollo de un plan de seguridad estratégico para el análisis de situaciones vulnerables en una red de una empresa. Realización de un proyecto práctico o teórico. Se requiere previa autorización del profesor y el Coordinador del Programa. Calificación: P/NP.
3 créditos

III. OBJETIVOS

Al terminar este curso los estudiantes podrán:

1. Desarrollar una propuesta para desarrollar atender un problema de seguridad en una empresa.
   1.1. Evidenciar la viabilidad del sistema propuesto

2. Desarrollar un plan que proponga una solución al problema o problemas en cuestión

3. Publicar en el Web la documentación del sistema abierto desarrollado

4. Entregar en CD el material publicado en el Web, la propuesta, el contenido del proyecto incluyendo la programación.

IV. CONTENIDO TEMÁTICO

A. Desarrollo de propuesta (La Propuesta debe contener)
   1. Introducción
      a. Descripción del problema(s) o necesidad(es) de la organización en lo que respecta a las áreas de seguridad en la informática.

      b. Si aplica, mencionar antecedentes de ataques u otra problemática que hayan alterado la seguridad de los sistemas de información.

   2. Realizar un avalúo del equipo actual con el que cuenta la organización incluyendo todo tipo de computadoras, servidores, programas o aplicaciones y conexiones físicas a otras computadoras o sistemas de información o la Internet.
   3. Analizar los niveles de vulnerabilidad de la organización en cuanto a los sistemas de información se refiere. Realizar un análisis de riesgo.
   4. Recomendar algún tipo de estrategia para reducir el nivel de vulnerabilidad en los sistemas de información. Dichas estrategias podrían consistir de lo(s) siguiente(s):
      1. Integración de uno o varios programas o aplicaciones o equipo que sirva para satisfacer las necesidades de seguridad en la organización y que a su vez reduzcan lo mas posible el nivel de vulnerabilidad.

   3. Si aplica, realizar una tarea de análisis forense en una computadora, servidor(es) o sistemas de información en cuestión. Describir su propósito y detallar su procedimiento.

   5. Analizar las políticas actuales de la organización, si alguna, relacionadas a la seguridad en las redes o sistemas de información . Si amerita, proveer recomendaciones a las políticas ya establecidas o recomendar políticas que se atemperen a las metas de la organización.

B. El Contenido de la documentación del sistema a publicarse en el Web
   1. Abstracto explicativo del sistema
   2. Introducción
   3. Descripción del problema
   4. Importancia del proyecto
   5. Justificación (viabilidad)
   6. Conclusiones
   7. Bibliografía (Estilo APA)

V. ACTIVIDADES

A. Reuniones periódicas
B. Correo electrónico

1. **LIBRO DE TEXTO**:

No hay libro de texto asignado para este curso.

2. **RECURSOS**:

Lecturas y proyectos publicados en el servidor institucional sisab.lce.org.
Computadoras
Servicios de Internet

VI. EVALUACIÓN

Propuesta	25%
Desarrollo del sistema	50%
Presentación	25%
Total	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.

   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

IX. BIBLIOGRAFÍA

American Psychological Association. (2004). APA Style Helper 5.0: Software for New Writers in the Behavioral Sciences. American Psychological Association. ISBN: 1591471370

Fineberg, S. Open Systems still stands the tests of time. Accounting Today, 4/5/2004, Vol. 18 Issue 6, p20. (*AN 12720543*)

Khosrow-Pour, M. (2002). Annals of Cases on Information Technology, Vol. 5. Idea Group. ISBN: 1591400619

Knapp, S. & VandeCreek, L. (2003). Guide to the 2002 Revision of the American Psychological Association's Ethics Code. Professional Resource Exchange, Incorporated. ISBN: 1568870795

Nolle, T. Time to Take Open Source Seriously. Network Magazine, Apr2004, Vol. 19 Issue 4, p82. (*AN 12726029*)

Traoré, I., Aredo, D. & Ye, H. An integrated framework for formal development of open distributed systems. Information & Software Technology, Apr2004, Vol. 46 Issue 5, p281. (*AN 12237765*)