UNIVERSIDAD TECNOLÓGICA DE PANAMÁ
FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES
DEPARTAMENTO DE PROGRAMACIÓN DE COMPUTADORAS

Seguridad en los Sistemas de Información

Profesor: Isabel Leguías **Fecha: 02/04/19**

ASPECTOS GENERALES DEL CURSO FC-FISC-1-1-2016

a) OBJETIVOS

➢ General:

- Estudiar la seguridad de las aplicaciones en un Sistema Informático para el fortalecimiento a través de los servicios de seguridad.
- Describir las vulnerabilidades, amenazas y ataques en un Sistema Informático de tal forma, de aplicar los mecanismos de seguridad adecuados.
- Describir el proceso de llevar a cabo el análisis de riesgo y pan de contingencia en el desarrollo del software
- Conocer las políticas y normas de seguridad en el desarrollo de los Sistemas de Información

➢ Específicos:

- Conocer y comprender los conceptos básicos sobre Seguridad Informática.
- Describir los servicios básicos que garantizan la Integridad, Confiabilidad, Disponibilidad y no repudio de la información.
- Describir las diversas amenazas, vulnerabilidades y ataques en un sistema informático.
- Describir los mecanismos de seguridad que permitan la protección de un sistema informático, al igual que los controles adecuados para la autenticación y autorización.
- Determinar los diferentes vectores de ataques para la aplicación de estrategias de defensa.
- Describir los controles adecuados para análisis de riesgo en el desarrollo de aplicaciones.
- Conocer el ciclo de vida para la seguridad en el desarrollo de aplicaciones.
- Comprender la seguridad en el software y en los sistemas.

b) CONTENIDOS

	Semanas
CAPITULO I: INTRODUCCION A LA SEGURIDAD	2
CAPITULO II: MECANISMOS DE SEGURIDAD	2
CAPITULO III: AUTENTICACIÓN Y CONTROL DE ACCESO	2
CAPITULO IV: PRINCIPIOS DE SEGURIDAD DEL SOFTWARE Y DEL SISTEMA	1
CAPITULO V: SEGURIDAD EN EL CICLO DE VIDA	1
CAPITULO VI: VECTORES DE ATAQUE	1
CAPITULO VII: ESTRATEGIAS DE DEFENSA	1
CAPITULO VIII: SEGURIDAD WEB	2
CAPITULO IX: ANALISIS DE RIESGO	2
CAPITULO X: PLAN DE CONTINGENCIA Y POLITICAS DE SEGURIDAD	2

c) NORMAS A SEGUIR EN LA ASIGNATURA

- En caso de ausencia a algún parcial o actividad presencial, deberá entregar una copia de certificado médico o constancia de su ausencia. (Ver Estatuto Universitario artículo 183 parágrafo c y artículos 265-268).
- Respetar las pautas y fechas de entrega de tareas, actividades grupales, informes de laboratorios, etc. No se aceptarán trabajos tardíos.
- Todas las tareas, elaboración de artículos, investigaciones, proyecto final e informes de laboratorios deberán ser colocados en la plataforma Moodle, el cual es utilizado como apoyo al curso.

d) EVALUACIÓN

Actividades de Evaluación	Porcentaje (%)
Parciales	**25%**
Laboratorios (individual)	**20%**
Trabajos Grupales y Tareas (Individuales)	**15%**
Portafolio(individual)	**5%**
Artículo del Proyecto	**5%**
Semestral	
Proyecto (Escrita)	**15%**
Demostración (Proyecto)	**15%**
Total	**100%**

Descripciones de las Actividades de Evaluación:

1. **Parciales**

Se aplicarán y evaluarán parciales en los que se incluirán, tanto al material expuesto en clase como el obtenido por autoevaluación de aprendizaje, con la guía del docente.

2. **Examen Semestral - Proyecto de investigación**

La evaluación semestral se dará a través de un proyecto de investigación, el cual demostraran los aprendizajes recibidos y obtenidos por parte del alumno en la asignatura.

Se asigna un proyecto final, en grupos de 2 estudiantes, el cual básicamente es un trabajo relacionado con la seguridad en sistemas de información. Los detalles de este proyecto de grupos estarán disponibles más adelante en Moodle. Se sugiere que inicien con búsqueda de información en un área de Seguridad en los Sistemas de Información que les interés más y desarrollar una "pregunta de investigación" a su alrededor.

Por ejemplo, si su área de interés general está en seguridad en aplicaciones web, usted querría refinarla más al considerar un aspecto específico, por ejemplo, Implementación de un Sistema de Detección de Intrusos para el Sistema de Matricula.

A continuación, desarrollar su pregunta de investigación en torno a eso. En este caso, un ejemplo de una pregunta de investigación sería: "¿Es posible detectar ataques con el sistema de detección de intrusos?" Por favor, tenga en cuenta que su pregunta de investigación debe ser interesante, importante y relevante, sobre todo que resuelva un problema

a. **Demostración-sustentado:** Los estudiantes de cada grupo deberán desarrollar parte práctica como parte del proyecto final del curso, explicando de forma detallada con sus respectivos resultados.

- **Artículos del proyecto:** Elaboración de un artículo científico de los resultados obtenidos en el proyecto final.

- **Tareas, lecturas, resúmenes y Trabajos Grupales:** Son temas tratados sobre los tópicos presentados en el plan de contenido y que tienen importancia dentro de la asignatura.

- **Laboratorios** Se pretende que cada alumno realice una serie de laboratorios de forma continua durante el desarrollo de las sesiones de aprendizaje.

  Para el caso de trabajos grupales se involucrarán los debates o foros relacionados con temas de actualidad, al igual que resolución de problemas, lecturas, resúmenes, etc.

- **Portafolio:** Es la carpeta profesional y técnica en la que el alumno evidenciará su participación, aportes, avances de conocimientos a lo largo del curso. Su detallada y cuidadosa elaboración garantiza un alto desempeño y rendimiento académico.

- **Artículo:** Cada grupo de estudiantes elaborará un artículo del proyecto de investigación desarrollado en el semestre

e) BIBLIOGRAFÍA

AUTOR	NOMBRE DEL LIBRO	EDITORIAL
1. Effy OZ	Administración de los Sistemas de Información	Editorial Thomson
2. Laudon, Kenneth , Laudon Jane	Sistemas de Información Gerencial	Prentice Hall - Pearson Octava Edición
3. O Brien James	Sistemas de Información Gerencial	Mc Graw Hill
2. Piattini Mario G., del Peso Emilio	Auditoria Informática. Un enfoque práctico.	Alfaomega – Ra-Ma Segunda Edición
3. Echenique, José Antonio	Auditoria Informática	Mc Graw Hill
4. Braude, Eric J.	Ingeniería de Software.	Alfaomega
5. Muñoz, Raso Carlos	Auditoría en Sistemas Computacionales	Prentice Hall
6. Lamére J.M	La Seguridad Informática. Metodología	Ediciones Arcadia S.A
7. Luis Angel Rodríguez	Seguridad de la Información en Sistemas de Cómputo	Ventura Ediciones
8. Gomez Vieites, Alvaro	Enciclopedia de la Seguridad Informática	Alfaomega – Ra-Ma
9. Aceituno Canal, Vicente	Seguridad de la Información	Limusa, Noriega Editores

f) INFOGRAFÍA

Carlos M. Fabuel Díaz. (2013). Implementación de un Sistema de Seguridad Perimetral. Proyecto Fin de Carrera. Universidad Politécnica de Madrid. http://oa.upm.es/22228/1/PFC_CARLOS_MANUEL_FABUEL_DIAZ.pdf

Mark Rhodes-Ousley. (2012). Information Security. Second Edition.
http://www.flow.com.sa/EN/img/books/InformationSecurityEnglish.pdf

Justin Clarke, Nitesh Dhanjai. (2005). Network Security Tools. O'Reilly.
http://commons.oreilly.com/wiki/index.php/Network_Security_Tools

Wiley Brand. (2016). Cybersecurity. Dummies. Palo Alto Networks 2nd Edition.
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/education/cybersecurity-for-dummies.pdf

g) EQUIPO DOCENTE

Prof. Isabel Leguías

h) COMUNICACIÓN CON EL DOCENTE

Correo electrónico: **isabel.leguias@utp.ac.pa**

Horario de atención a los alumnos: **Martes y Miércoles 4:30 pm a 5:45 pm .**

CRONOGRAMA DEL ESTUDIANTE FC-FISC-1-2-2016

Nº	SEMANA	CONTENIDO	EVALUACIÓN
1	**01 al 05 abril**	Discusión del contenido, evaluación y organización del curso en el semestre. **I. INTRODUCCIÓN A LA SEGURIDAD** 1.0 . Introducción 1.1 Conceptos de Seguridad 1.1.1 Consideraciones de Seguridad 1.1.2 Definiciones	• Diagnóstico formativo
2	**08 al 12 abril**	1.2 Servicios de Seguridad 1.2.1 Confidencialidad 1.2.2 Autenticación 1.2.3 Integridad 1.2.4 No Repudio 1.2.5 Disponibilidad 1.3 Amenazas, Vulnerabilidades y Ataques 1.3.1 Atacantes 1.3.2 Amenazas y sus tipos	• **Tarea No.1** Investigar sobre los tipos de amenazas • **Trabajo Grupal No. 1** El Arte de la Guerra • **Laboratorio # 1**. Investigar y realizar un cuadro de los diversos atacantes
3	**15 al 17 abril**	**II. MECANISMOS DE SEGURIDAD** 2.1 Criptografía 2.1.1. Historia 2.1.2. Conceptos 2.1.3. Técnicas Criptografías 2.1.3.1. Simétrica 2.1.3.2. Asimétrica 2.2. Hash 2.3 Firma Digital	• **Laboratorio #2** Técnicas Criptográficas • **Trabajo Grupal # 2** Cuadro comparativo de las técnicas criptográficas
4	**22 al 26 abril**	2.4 Cortafuego 2.4.1. Características básicas de un cortafuego 2.4.2. Tipos de cortafuegos 2.5. Sistemas de Detección y Prevención de Intrusos 2.5.1. Tipos IDS 2.5.1.1 HIDS 2.5.1.2 NIDS 2.5.2. Tipos de IPS 2.5.2.1 HIPS 2.5.2.2. NIPS 2.5.2.3. WIPS 2.5.2.4. NBA	• **Laboratorio #3** • **Tarea #3** Cuadro comparativo de herramientas de cortafuego • **Trabajo grupal # 3** Cuadro comparativo de sistemas de detección y prevención de intrusos

5	**29 al 30 abril y 2 mayo**	**III. AUTENTICACIÓN Y CONTROL DE ACCESO** 3.1 Introducción 3.2. Autenticación y autorización 3.3 aplicaciones de Autenticación	• **Laboratorio #4** • **Trabajo grupal # 4** Investigar sobre aplicaciones de autenticación • **Parcial #1 Capítulo 1**
6	**6 al 10 mayo**	3.4 Control de Acceso 3.4.1. Control de Acceso Discrecional 3.4.2. Control de Acceso Mandatorio 3.4.3. Control de Acceso Basado en Roles	• **Laboratorio #5** • **Trabajo grupal # 5** Investigar sobre los diversos métodos de control de acceso •
7	**13 al 17 mayo**	**IV. PRINCIPIOS DE SEGURIDAD DEL SOFTWARE Y DEL SISTEMA** 4.1. Confidencialidad, Integridad y Disponibilidad 4.2. Aislamiento 4.3. Modelos de Amenazas 4.4 Errores frente a vulnerabilidades	• **Laboratorio #5 cont.** • Trabajo Grupal # **6** Realizar un cuadro que indique las amenazas y vulnerabilidades en software • Seguimiento #1 del Proyecto
8	**20 al 24 mayo**	**V. SEGURIDAD EN EL CICLO DE VIDA** 5.1. Diseño del Software 5.2. Implementación 5.3. Actualización continua y parches 5.4. Ingeniería Moderna de Software	• **Laboratorio #6** • Tarea **# 4** Investigue sobre metodologías utilizadas para la seguridad en el ciclo de vida software • **Parcial #2 Cap 2 (2.1 al 2.3) y Cap 3**
9	**27 al 31 mayo**	**VI. VECTORES DE ATAQUE** 6.1. Denegación de Servicio 6.2. Información sobre fugas 6.3. Escalamiento de privilegios	• **Laboratorio #6 cont.** • **Trabajo grupal #7** Investigar sobre los diferentes vectores de ataque
10	**3 al 7 junio**	**VII. ESTRATEGIAS DE DEFENSA** 7.1. Verificación del Software 7.2. Seguridad basada en el lenguaje 7.3. Prueba 7.4. Mitigación 7.4.1. Prevención de ejecución de Datos (DEP) 7.4.2. Asignación Aleatoria de espacio de direcciones (ASLR) 7.4.3. Integridad de la Pila 7.4.4. Fortificar la fuente 7.4.5. Integridad del control de flujo 7.4.6. Integridad del puntero de código 7.4.7. Sandboxing y fallas basadas en software 7.4.8 Aislamiento	• **Laboratorio #7** • **Trabajo Grupal # 8** Investigar cuales son los apropiados mecanismos de defensa que deben aplicarse en el desarrollo de software
11	**10 al 14 junio**	**VIII. Seguridad Web**	• **Laboratorio #5 cont.**

		8.1 Protección de servicios de larga duración 8.2. Seguridad del Navegador 8.3. Inyección SQL	• Trabajo Grupal # **9** Investigue sobre las vulnerabilidades de seguridad en Web
12	**17 al 21 junio**	8.4. Cross Site Scripting (XSS) 8.5 Solicitud de falsificación de sitios cruzados (XSRF) 8.6 cifrado de scripts 8.7 Web Tracking y Web proxy	• **Laboratorio #8** • Tarea #5
13	**24 al 28 junio**	**IX. ANALISIS DE RIESGO** 9.1. Introducción 9.2. Definición de riesgo 9.3. Proceso de la Administración del Riesgo	• **Laboratorio #8 cont.** • Trabajo Grupal # **6** • Caso de estudio • **Seguimiento #2 Proyecto**
14	**1 al 5 julio**	9.3.1. Identificación de riesgo 9.3.2. Análisis de riesgo 9.3.3. Mitigar el riesgo 9.3.4. Supervisión de la administración del riesgo	• **Laboratorio # 8** • **Caso de estudio** • **Parcial #3 Cap VII y VIII**
15	**8 al 12 julio**	**X. PLAN DE CONTINGENCIA Y POLITICAS DE SEGURIDAD** 10.1 Introducción 10.2 Importancia del plan de contingencia 10.3 Metodología para el desarrollo de planes de contingencia 10.3.1 Objetivos 10.3.2 Alcance 10.3.3 Identificación de desastres probables 10.3.4 Inventario y recursos críticos	• **Laboratorio # 9** • Caso de estudio
16	**15 al 19 julio**	10.3.5 Nexo con Seguridad de la Información 10.3.6 Respaldos 10.3.7 Procedimientos de Emergencia y Recuperación 10.3.8 Implantación, Entrenamiento y Pruebas 10.3.9 Mantenimiento 10.4 Políticas de Seguridad	• **Portafolio Electrónico** • **Seguimiento #3 Proyecto** • **Caso de estudio**
	22 de julio al 3 de agosto	**SEMESTRALES**	Exámenes Semestrales

CUADRO DE CALIFICACIONES - ESTUDIANTE FC-FISC-1-5-2016

UNIVERSIDAD TECNOLÓGICA DE PANAMÁ
FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES
DEPARTAMENTO DE PROGRAMACIÓN DE COMPUTADORAS

Seguridad en los Sistemas de Información

Profesor:_____

Nombre: _____ **Cédula:** _____**Grupo:** _____ **Fecha:** _____

ASISTENCIA Y PARTICIPACIÓN				
Semana Nº.	*Asistencia* (Coloque un v si asistió y un guión si no asistió)			*Participación*
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

Invest./Trabajos Grupales/Quiz/ Tareas/Otros			
Nº.	*Actividad*	*Nota*	*Fecha*
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

LABORATORIOS		
Fecha	*Nota*	*Observación*

Parciales			
N°	**Tema**	**Fecha**	**Nota**
1			
2			
3			
4			

Proyecto(s)			
N°	**Tema**	**Fecha**	**Nota**
1			
2			
3			
4			