UNIVERSIDAD TECNOLÓGICA DE PANAMÁ
FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES
DEPARTAMENTO DE SISTEMAS DE INFORMACION, EVALUACION Y CONTROL DE RECURSOS INFORMATICOS

Seguridad Informática

Profesor: José Moreno
Fecha:21/3/22

ASPECTOS GENERALES DEL CURSO FC-FISC-1-2-2017

a) OBJETIVOS

- **Meta del Docente**
  - Usar estrategias didácticas activas para que los estudiantes adquieran las competencias relacionadas a la Seguridad en los Sistemas de Información

- **Metas del Alumno**
  - Conocer los conceptos generales de la seguridad física y lógica en ambientes de Tecnología de Computación.
  - Aplicar metodologías y técnicas que conduzcan a la práctica de una cultura de seguridad informática
  - Conocer las mejores prácticas para seguridad informática.
  - Estudiar la seguridad de los componentes de un Sistema de Información como parte del plan de seguridad de la organización.
  - Conocer las políticas y normas de seguridad en el desarrollo de los sistemas de información.
  - Definir los principios de Seguridad Informática para fundamentar la estructura de la Seguridad Informática en los entornos de Tecnología de Computación y así mitigar los riesgos.
  - Reconocer una diversidad de amenazas que impactan a la seguridad informática de los entornos de Tecnología de Computación.

b) CONTENIDOS

	Tema	Duración
Capítulo I	PRINCIPIOS DE SEGURIDAD INFORMATICA	**1 semanas**
Capítulo II	ANALISIS Y GESTION DEL RIESGO	**1 semanas**
Capítulo III	CRIPTOGRAFIA	**4 semanas**
Capítulo IV	SEGURIDAD EN SISTEMAS OPERATIVOS Y HARDWARE	**4 semanas**
Capítulo V	SEGURIDAD EN REDES	**2 semanas**
Charlas y Proyectos		**4 semanas**

c) NORMAS A SEGUIR EN LA ASIGNATURA

- A los proyectos señalados para el semestre podrán ser añadidos algunos a criterio del facilitador, así como a sugerencia de los estudiantes. Los proyectos y charlas son **grupales**.
- Se asignarán tareas para las diferentes sesiones y dependiendo de los temas. Las mismas son de carácter **individual** y/o **grupal.**
- Deberá procurar mantener al día su **portafolio estudiantil** ya que el mismo será revisado a lo largo del semestre.
- Los proyectos, investigaciones y tareas formales deberán ser entregadas en el formato de Trabajos Formales, mismo que se anexa al final del documento.
- Deberá inscribirse en la plataforma de apoyo a los cursos presenciales en teams (ya inscritos):
- La asistencia es un aspecto de mucha importancia para el curso. Recuerde que, de acuerdo al estatuto universitario **(ART. 265, 267)**, si usted falta a un 15% de las clases, su calificación final se verá reducida en una nota. Si las faltas superan el 33%, no tendrá derecho a calificación final.
- No está permitido ausentarse en la fecha de los exámenes parciales. Los quices o exámenes cortos así como los parciales no son recuperables.
- Algunos materiales que veremos en el curso, principalmente lecturas o artículos de actualidad, podrían estar en idioma inglés.

NORMAS PARA LA ELABORACIÓN DE TRABAJOS FORMALES

FORMATO GENERAL

- Todo trabajo deberá utilizar para el contenido fuente tamaño 12 y tipo Arial.
- Los títulos y subtítulos deberán ser resaltados en negrita y en tamaño 14.
- Los márgenes de los documentos serán de 1 pulgada en todas las direcciones.
- El espaciado del documento será de 1.5 líneas.
- Si utiliza tablas y/o ilustraciones, deberá colocarle un pie que las identifique y una numeración secuencial.
- Las páginas deberán estar numeradas y tamaño 8.5 * 11
- Para las referencias bibliográficas deberá utilizar el formato APA, el cual indica la manera correcta de referenciar, libros de texto, direcciones electrónicas, artículos, etc.
- Los trabajos deben ser entregados en un cartapacio de color **CREMA,** utilizando un gancho de plástico o metal dependiendo de la naturaleza del mismo.
- El uso de encabezado y pie de página está permitido.

Los puntos a presentar en la mayoría de los trabajos escritos son:

- Página de presentación
- Indicé
- Introducción
- Contenido (texto, imágenes, gráficos, etc.)
- Conclusiones
- Bibliografía
- Anexos

Las direcciones de internet se presentarán así:

- Nombre del sitio
- URL: http://...
- Fecha de Consulta
- Responsable / Autor de la información

d) EVALUACIÓN

Descripción	Porcentaje(P)
Asistencia/Participación	**-**
Parciales	**30**
Semestral	**30**
Quiz / Tareas	**10**
Investigaciones	**-**
Trabajos Grupales	**-**
Laboratorios	**15**
Proyectos	**10**
Portafolio	**5**
	100%

Descripciones de las Actividades de Evaluación:

1. Asistencia y Participación:

La participación activa en las clases es un elemento de valoración, evidenciado por su capacidad de trabajo en equipo, desarrollo del espíritu crítico y fomento de la cualidad de liderazgo.

2. Parciales

La evaluación del aprendizaje de los alumnos se realizará de forma continua durante el desarrollo de las sesiones de aprendizaje, valorando la comprensión de los conceptos, la familiarización y resolución de problemas a través de la herramienta.

3. Examen Semestral

El propósito de la evaluación semestral de los aprendizajes será evaluar el grado de conocimiento que ha obtenido el alumno sobre la asignatura.

4. Quices

Son pruebas cortas que tienen el propósito de verificar la asimilación del contenido y aplicación de los conceptos.

5. Tareas, Investigaciones y Trabajos Grupales

Son temas tratados sobre los tópicos presentados en el plan de contenido o de actualidad y que tienen importancia dentro de la asignatura.

6. Laboratorios y Proyectos:

Se pretende que cada alumno realice una serie de laboratorios de forma continua durante el desarrollo de las sesiones de aprendizaje, los cuales le permitan adquirir los conocimientos básicos sobre la administración de servidores.

Adicionalmente, desarrollarán diversos proyectos que con lleven la aplicación y reforzamiento de los conceptos aprendidos en las diferentes temáticas del Sistemas Operativos, Sistemas Operativos II y Sistemas Operativos III.

7. 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.

e) BIBLIOGRAFÍA

AUTOR	AÑO	LIBRO	PAIS	EDITORIAL
Lardent, ALberto	2001	Sistemas de información para la gestión empresaria. Procedimientos, Seguridad y Auditoría.	Argentina	Prentice Hall
Lamére J.M	2000	La Seguridad Informática. Metodología		Ediciones Arcadia S.A
O Brien James	1995	Sistemas de Información Gerencial		Mc Graw Hill
Piattini Mario G., del Peso Emilio	2001	Auditoria Informática. Un enfoque práctico.	México	Alfaomega – Ra-Ma Segunda Edición
Echenique, José Antonio	2001	Auditoria Informática	México	Mc Graw Hill
Braude, Eric J.	2008	Ingeniería de Software.		Alfaomega
Muñoz, Razo Carlos	2006	Auditoría en Sistemas Computacionales	México	Prentice Hall

Gomez Vieites, Alvaro	2011	Enciclopedia de la seguridad informática	México	Alfaomega-Ra-Ma

f) EQUIPO DOCENTE

Ing. José Moreno

g) COMUNICACIÓN CON EL DOCENTE

Correo electrónico: **jose.moreno3@utp.ac.pa**

Horario de atención a los alumnos: **viernes – 10:00am a 15:00pm**

CRONOGRAMA DEL ESTUDIANTE

FC-FISC-1-3-2017

SEMANA		CONTENIDO	EVALUACIÓN
1	21 – 25 Marzo	**Capítulo I – PRINCIPIOS DE SEGURIDAD INFORMATICA** 1.1. Introducción 1.2. Importancia de la Seguridad de la Información 1.3. Características de la Seguridad de la Información 1.3.1. Integridad 1.3.2. Confidencialidad 1.3.3. Privacidad 1.4. Seguridad informática como proceso 1.5. Ciclo de Vida de la Seguridad Informática 1.6. Vulnerabilidades y Amenazas a la Seguridad Informática 1.6.1. Amenazas intencionales Remotas 1.6.2. Malware (Ciberdelincuentes) 1.6.3. Virus 1.6.4. Adware 1.6.5. Backdoors 1.6.6. Botnet 1.6.7. Gusanos 1.6.8. Hoax 1.6.9. Hijacker 1.6.10. Keylogger 1.6.11. Phishing 1.6.12. Pup 1.6.13. Roguer 1.6.14. Riskware 1.6.15. Rootkit 1.6.16. Spam 1.6.17. Troyano 1.6.18. Spyware 1.6.19. Ransomware 1.6.20. Otros 1.7. Política de Seguridad 1.8. Organización de la Seguridad	• Laboratorio 1 • Caso de Estudio Árbol de la ciencia.
2	28 Marzo – 1 Abril	**Capitulo II - ANALISIS Y GESTION DEL RIESGO** Concepto de Control 2.1. Introducción 2.2. Definición de riesgos 2.3. Proceso de la Administración del Riesgo 2.3.1. Identificación de riesgo 2.3.2. Análisis de riesgo 2.3.3. Mitigar el riesgo 2.3.4. Supervisión de la administración del riesgo	▪ Laboratorio 2 ▪ Tarea 1
3	4 – 8 Abril	**Capítulo III - CRIPTOGRAFIA** 3.1. Introducción	▪ Laboratorio 3 ▪ Tarea 2

		3.2. Conceptos 3.3. Criptografía 3.3.1. Historia 3.3.2. Conceptos	
4	**11 – 15 Abril**	3.3.3. Técnicas Criptográficas 3.1.1.1. Simétrica 3.1.1.2. Asimétrica 3.1.1.3. Criptografía de Clave Pública 3.1.1.4. Criptografía de Clave Privada 3.1.1.5. Criptografía de Clave Privada	▪ Quiz 1 ▪ Charla 1 ▪ Laboratorio 4
5	**18 – 22 Abril**	3.4. PKI (Public Key Infrastructure) 3.5. Firmas Digitales	▪ Quiz 2 ▪ Laboratorio 5
6	**25 – 29 Abril**	3.6. Técnica Hashing 3.7. PGP (Pretty Good Privacity)	▪ Laboratorio 6 ▪ Parcial 1
7	**2 – 6 Mayo**	**Capítulo IV - SEGURIDAD EN SISTEMAS OPERATIVOS Y HARDWARE** 4.1. Adecuación de las instalaciones 4.2. Controles de Protección Física	▪ Práctica
8	**9 - 13 Mayo**	4.3. Controles Biométricos 4.4. Adecuación de los equipos	▪ Laboratorio 7 ▪ Práctica
9	**16 – 20 Mayo**		▪ Conferencia OWASP
10	**23 – 27 Mayo**	4.5. Plan de copias de Seguridad o Respaldo 4.6. Políticas de Seguridad de Sistemas Operativos	▪ Práctica ▪ Laboratorio 8
11	**30 mayo – 3 Junio**	4.7. Políticas de Seguridad de Hardware	▪ Parcial 2 ▪ Laboratorio 9
12	**6 – 10 Junio**	Capítulo V - SEGURIDAD EN REDES 5.1. Seguridad en Redes de Ordenadores 5.2. Riesgos y Vulnerabilidades en la conexión a Internet 5.2.1. Entornos de WEB y BASE DE DATOS 5.1.1.1. Ataques por Injección (SQL INJECTION) 5.1.1.2. Ataques por DOS y DDOS 5.1.1.3. Ataques Injection script maliciosos (Cross Site Scripting – XSS) 5.1.1.4. Fuerza Bruta 5.1.1.5. Cortafuego de Aplicaciones WEB (WAF – ModSecurity y ModEvasive) 5.3. La Función de los Servidores Proxy 5.3.1. Características 5.3.2. Servicio de Proxy Inverso 5.4. Cortafuegos 5.4.1. Características 5.4.2. Tipos de Cortafuegos	▪ Laboratorio

		5.4.1.1. Cortafuegos UTM vs Next Generation	
13	**13 – 17 Junio**	5.5. Sistemas de detección y Prevención de Intrusos 5.5.1. Tipo de IDS 5.5.1.1. HIDS, NIDS, MHIDS 5.5.2. Tipos de IPS 5.5.2.1. HIPS NIPS, IPS NEXT GENERATION (Mitigadores de Ataques) 5.6. Seguridad en las Redes Inalámbricas 5.6.1. Riesgos y Vulnerabilidades de las Redes Inalámbricas. 5.6.2. Seguridad en las Redes Inalámbricas 5.6.2.1. Protocolo WPA, Autentificación Robusta: estándar 802.1x, Protocolo WPA2-RSN.	▪ Laboratorio 10 ▪ Parcial 3
14	**20 – 24 Junio**	**Charlas/Proyectos**	
15	**27 Junio – 1 Julio**	**Charlas/Proyectos**	
16	**4– 8 Julio**	**Charlas/Proyectos**	
17	**11 – 15 Julio**	**Charlas/Proyectos**	
	18 – 22 Julio		• Examen Semestral

CUADRO DE CALIFICACIONES - ESTUDIANTE

FC-FISC-1-4-2017

UNIVERSIDAD TECNOLÓGICA DE PANAMÁ
FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES
DEPARTAMENTO DE PROGRAMACIÓN DE COMPUTADORAS
(NOMBRE DE LA ASIGNATURA)

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			