UNIVERSIDAD TECNOLÓGICA DE PANAMÁ

FACULTAD DE INGENIERIA DE SISTEMAS COMPUTACIONALES

DEPARTAMENTO DE SISTEMAS DE INFORMACIÓN, CONTROL Y EVALUACIÓN DE RECURSOS INFORMÁTICOS

1. IDENTIFICACIÓN DE LA ASIGNATURA

DENOMINACIÓN DE LA ASIGNATURA:		**SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN**					
CÓDIGO DE ASIGNATURA:	**8411**	CANTIDAD DE CRÉDITOS:	**3**	Nº. DE HORAS TEÓRICAS:	**3**	HORAS DE LABORATORIO:	**1**
TOTAL DE HORAS:	**4**	PRERREQUISITOS:	**8457**	FUNDAMENTAL	**Sí**	ÚLTIMA REVISIÓN:	**2024**

2. DESCRIPCIÓN DE LA ASIGNATURA

La asignatura está orientada a que el estudiante conozca la importancia de la seguridad para los sistemas informáticos, los riesgos, amenazas y las vulnerabilidades a los cuales están expuestos, así como los mecanismos de seguridad, y herramientas disponibles para la protección de éstos. Al igual que la protección en el desarrollo de software.
El curso propone una revisión desde un enfoque teórico-práctico de los diferentes apartados que constituyen el objeto de la Seguridad en los Sistemas de Información.

3. OBJETIVOS

- **Generales:**
  - 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 forma tal, de aplicar los mecanismos de seguridad adecuados.
  - Describir el proceso para llevar a cabo el análisis de riesgo y plan 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 diferentes amenazas, vulnerabilidades, ataque a los que se enfrentan los sistemas informáticos.
  - Describir los mecanismos de seguridad que permiten la protección de un sistema informático, al igual que los controles adecuados para la autenticación y autorización de la información.
  - Describir los controles adecuados para el análisis de riesgo en el desarrollo de las aplicaciones
  - Comprender la seguridad en el ciclo de vida del desarrollo del software y en los sistemas.
  - Conocer y aplicar planes de contingencia y políticas de seguridad a los sistemas de información.

4. CONTENIDOS DE LA ASIGNATURA.

Módulo I:	**Conceptos Generales de seguridad informática**	**Duración**:	2 semanas

CONTENIDO	**ESTRATEGIAS**	**RECURSOS**	**EVALUACIÓN**
1. Introducción a la Seguridad en Redes 1.0. Introducción 1.1. Conceptos de seguridad 1.1.1. Consideraciones de Seguridad 1.1.2. Definiciones 1.2. Servicios de Seguridad 1.2.1. Confiabilidad 1.2.2. Integridad 1.2.3. Disponibilidad 1.2.4. No repudio 1.2.5. Disponibilidad	❖ Presentar el tema ❖ Preguntas y respuestas ❖ Síntesis final ❖ Demostración por el profesor y alumnos ❖ Complementar y aclarar ❖ Asignar ejercicios ❖ Retroalimentación ❖ Asignar ejercicios ❖ Trabajo en casa ❖ Revisión y retroalimentación ❖ Laboratorios	❖ Tablero ❖ Diapositivas ❖ Computador ❖ Proyector multimedia ❖ Bibliografía ❖ Apuntes ❖ Internet ❖ videos	**Sumativa**: ❖ Tareas ❖ Talleres ❖ Trabajos grupales ❖ Informe de laboratorio ❖ Quiz

1.3. Amenazas, vulnerabilidades y ataques 1.3.1. Atacantes 1.3.2. Amenaza y sus tipos 1.3.3. Vulnerabilidades 1.3.4. Ataques 1.3.5. Tipos de ataques, atacantes y categorías de ataques			

Módulo II:	**Mecanismos de seguridad, Autenticación y Control de Acceso**	**Duración**:	5 semanas

CONTENIDO	**ESTRATEGIAS**	**RECURSOS**	**EVALUACIÓN**
2.1. Criptográfica 2.1.1. Historia 2.1.2. Conceptos 2.1.3. Técnicas criptográficas 2.1.3.1. simétrica 2.1.2.3. asimétrica 2.2. Funciones Hash 2.3. Firma Digital 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 de IDS 2.5.1.1. IDS de hardware (HIDS) 2.5.1.2. IDS de red (NIDS) 2.5.2. Tipos de IPS	❖ Presentar el tema ❖ Preguntas y respuestas ❖ Síntesis final ❖ Presentación del asunto ❖ Demostración por el profesor y alumnos ❖ Complementar y aclarar ❖ Asignar ejercicios ❖ Orientación individual ❖ Retroalimentación ❖ Asignar ejercicios ❖ Trabajo en casa ❖ Revisión y retroalimentación ❖ Laboratorios	❖ Tablero ❖ Diapositivas ❖ Computador ❖ Proyector multimedia ❖ Bibliografía ❖ Apuntes ❖ Internet ❖ videos	**Sumativa**: ❖ Tareas ❖ Talleres ❖ Trabajos grupales ❖ Informe de laboratorio ❖ Parcial No. 1

2.5.2.1. IPS de hardware (HIPS) 2.5.2.2. IPS de red (NIPS) 2.5.2.3. IPS inalámbricos (WIPS) 2.5.2.4. Normas básica de autoprotección (NBA) 2.6. Autenticación y control de acceso 2.6.1. Introducción 2.6.2. Autenticación y autorización 2.7. Aplicaciones de Autenticación 2.8. Control de Acceso 2.8.1. Control de Acceso Discrecional 2.8.2. Control de Acceso Mandatorio 2.8.3. Control de Acceso basado en roles			

Módulo III:	**Seguridad en el Ciclo de Vida del Software, Vectores de ataque y Estrategias de Defensa**	**Duración**:	5 semanas

CONTENIDO	**ESTRATEGIAS**	**RECURSOS**	**EVALUACIÓN**
3.1. Seguridad en el Ciclo de Vida del Software 3.1.1. Diseño del Software 3.1.2. Implementación 3.1.3. Actualización continua y parches 3.1.4. Ingeniería Moderna de Software	❖ Investigaciones ❖ Síntesis y/o resúmenes ❖ Presentaciones orales (charlas) ❖ Resolución de problemas ❖ Ejercicios escritos	❖ Tablero ❖ Diapositivas ❖ Computador ❖ Proyector multimedia ❖ Bibliografía ❖ Apuntes ❖ Internet	**Sumativa**: ❖ Tareas ❖ Trabajos grupales ❖ ParciaL no. 2 ❖ Informe de laboratorio ❖ Talleres

3.2. Vectores de Ataque 3.2.1. Denegación de servicio 3.2.2. Información sobre fuga 3.2.3. Escalamiento de privilegios 3.3. Estrategias de Defensa 3.3.1. Verificación del software 3.3.2. Seguridad basada en el lenguaje 3.3.4. Prueba 3.4. Mitigación 3.4.1. Prevención de ejecución de Datos (DEP) 3.4.2. Asignación Aleatoria de espacios de direcciones (ASLR) 3.4.3. Integridad de la Pila 3.4.4. Fortificar la fuente 3.4.5. Integridad del control de flujo 3.4.6. Integridad del puntero de código 3.4.7. Sandboxing y fallas basadas en software 3.4.8. Aislamiento 3.5. Seguridad Web 3.5.1. Protección de servicios de larga duración 3.5.2. Seguridad del Navegador 3.5.3. Inyección SQL 3.5.4. Cross Site Scripting (XSS) 3.5.5. Solicitud de falsificación de sitios cruzados (XSRF) 3.5.6. Cifrado de scripts 3.5.7. Web Tracking y Web proxy	❖ Lecturas ❖ Portafolio estudiantil ❖ Presentaciones de ensayos ❖ Exposiciones ❖ Laboratorios	❖ videos	

Módulo IV:	**Análisis de Riesgo, Plan de Contingencia y Políticas de Seguridad**	**Duración**:	4 semanas

CONTENIDO	**ESTRATEGIAS**	**RECURSOS**	**EVALUACIÓN**
4.1. Análisis de Riesgo 4.1.1. Introducción 4.1.2. Definición de riesgo 4.1.3. Proceso de la administración del riesgo 4.1.3.1. Identificación del riesgo 4.1.3.2. Análisis de riesgo 4.1.3.3. Mitigar el riesgo 4.1.4. Supervisión de la administración del riesgo 4.2. Plan de Contingencia y Políticas de Seguridad 4.2.1. Introducción 4.2.2. Importancia del plan de contingencia 4.2.3. Metodología para el desarrollo de planes de contingencia 4.2.3.1. Objetivos 4.2.3.2. Alcance 4.2.3.3. Identificación de desastres probables 4.2.3.4. Inventario y recursos críticos 4.2.3.5. Nexo con seguridad de la Información 4.2.3.6. Respaldos 4.2.3.7. Procesamiento de Emergencia y Recuperación 4.2.3.8. Implantación, Entrenamiento y Prueba	❖ Investigaciones ❖ Síntesis y/o resúmenes ❖ Presentaciones orales (charlas) ❖ Resolución de problemas ❖ Ejercicios escritos ❖ Lecturas ❖ Portafolio estudiantil ❖ Presentaciones de ensayos ❖ Exposiciones ❖ Laboratorios	❖ Tablero ❖ Diapositivas ❖ Computador ❖ Proyector multimedia ❖ Bibliografía ❖ Apuntes ❖ Internet ❖ Videos	**Sumativa**: ❖ Tareas ❖ Crucigrama, sopa de letras ❖ Trabajos grupales ❖ Parcia no. 3 ❖ Informe de laboratorio ❖ Quiz

4.2.3.9. Mantenimiento 4.2.4. Políticas de seguridad			

5. EVALUACIÓN SUGERIDA.

CRITERIOS DE EVALUACIÓN	PORCENTAJE
Portafolio	5 %
Trabajos grupales presenciales	10 %
Tareas, casos de estudios, foros, debates, elaboración y lectura de artículos	5 %
Presentaciones orales (exposiciones, demostraciones, proyectos)	10 %
Laboratorios	10 %
Parciales	30 %
Semestral	30 %
Total :	100%

* Valores definidos por el Estatuto Universitario

6. REFERENCIAS BIBLIOGRÁFICAS.

[1] "Administración de los Sistemas de Información", Effy Oz, 5ta edición, Editorial Thomson, 2008

[2] "Sistemas de Información Gerencial", Laudon Kenneth, Laudon Jane decimosegunda. Edition, Editorial Prentice Hall, 2012

[3] “Sistemas de Información Gerencial”, James OBrien, 4ta edición, Pearson Education, Mc Graw Hill,.

[4] “Auditoria Informática. Un enfoque práctico”, Mario G Piattini, Emilio del Peso, 2da. Edición, Alfaomega- Ra-ma. 1997

[5] “Auditoria Informática”, José Antonio Echenique, 7ma edición, McGraw-Hill,2006. [6] "Ingeniería de Software", Eric J. Braude, Alfaomega,2003.

[7] “Auditoría en Sistemas Computacionales”, Carlos Raso Muñoz, Prentice Hall, 2002

[8] “Enciclopedia de la Seguridad Informática”, Alvaro Gomez Vieites, 2da edición, Alfaomega – Ra-Ma, 2017
[9] “Seguridad de la Información”, Vicente Aceituno Canal, Limusa, Noriega Editores,2004.

Infografía

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