SÍLABO
SEGURIDAD INFORMATICA

ÁREA CURRICULAR: TECNOLOGIA DE INFORMACION

I. DATOS GENERALES

1.1	Departamento Académico	: Ingeniería y Arquitectura
1.2	Semestre Académico	: 2019-II
1.3	Código de la asignatura	: 090862E2040
1.4	Ciclo	: Electivo de Especialidad
1.5	Créditos	: 04
1.6	Horas semanales totales	: 8
	1.6.1 Horas lectivas (Teoría, Práctica, Laboratorio)	: 4 (T=4, P=0, L=0)
	1.6.2 Horas no lectivas	: 4
1.7	Condición de la asignatura	: Electiva de especialidad
1.8	Requisito(s)	: 09067909040 Seguridad y Auditoria de Sistemas de Información
1.9	Docentes	: Ing. Mauricio Raúl Marín Bao

II. SUMILLA

El curso forma parte de la formación especializada; tiene carácter teórico – práctico. Le permite al estudiante desarrollar un conocimiento amplio sobre conceptos de seguridad tanto para plataformas de sistemas operativos, redes y de gestión informática, y la capacidad de poder aplicar los conocimientos al desarrollo de una infraestructura segura en una empresa.

El curso se desarrolla mediante las unidades de aprendizaje siguientes:
I. Sistemas de Seguridad. II. Seguridad en la Infraestructura de la Red. III. Control de Accesos. IV. Análisis de la Información de Seguridad. V. Criptografía. VI. Seguridad Organizacional.

III. COMPETENCIAS Y SUS COMPONENTES COMPRENDIDOS EN LA ASIGNATURA

3.1 Competencia

- Aplica conocimientos de computación y matemáticas apropiadas para los resultados del estudiante y las disciplinas enseñadas.
- Analiza un problema e identifica y define los requerimientos apropiados para su solución.
- Diseña, implementa y evalúa un sistema basado en computadoras, procesos, componentes o programa que satisfagan las necesidades requeridas.
- Comprende los aspectos y las responsabilidades profesional, ética, legal, de seguridad y social.
- Analiza el impacto local y global de la computación en los individuos, organizaciones y la sociedad.
- Usa técnicas, destrezas, y herramientas modernas necesarias para la práctica de la computación.

3.2 Componentes

Capacidades

- Comprende la importancia de la seguridad en un ambiente productivo.
- Identifica problemas de seguridad comunes en ambientes TI.
- Diseña una red segura
- Identifica vulnerabilidades en las redes de datos
- Utiliza aplicaciones para reducir problemas de seguridad en la red
- Aplica métodos de control de acceso lógico
- Aplica métodos de control de acceso físico
- Identifica funciones laborales (roles) en entornos empresariales.
- Selecciona los mejores métodos de control de acceso de acuerdo a la necesidad
- Reconoce patrones. Aprender a analizar información.
- Elabora documentos de resultados.
- Reconoce los conceptos de criptografía.

- Utiliza algunos métodos criptográficos para asegurar la información.
- Recomienda planes de respaldo de información.
- Recomienda planes de recuperación de desastres
- Asiste ante situaciones donde se involucre ingeniería social

Contenidos actitudinales

- Valora su carrera al elegir los temas de redacción en temas tecnológicos y científicos.
- Aprende a trabajar en equipo.
- Aprende de sus propios errores a partir de su propia experiencia
- Entiende que conocimientos debe lograr para aprender los contenidos de manera más eficiente
- Es responsable y cumple con las actividades asignadas por el docente

IV. PROGRAMACIÓN DE CONTENIDOS

UNIDAD I: SISTEMAS DE SEGURIDAD y SEGURIDAD EN LA INFRAESTRUCTURA DE LA RED

CAPACIDAD:

- Comprende la importancia de la seguridad en un ambiente productivo.
- Identifica problemas de seguridad comunes en ambientes TI.
- Diseña una red segura
- Identifica vulnerabilidades en las redes de datos
- Utiliza aplicaciones para reducir problemas de seguridad en la red

SEMANA	CONTENIDOS CONCEPTUALES	CONTENIDOS PROCEDIMENTALES	ACTIVIDAD DE APRENDIZAJE	HORAS	
				L	T.I.
1	**Primera sesión** Conceptos Generales de la Seguridad Informática	- Explica los conceptos generales de la seguridad informática.	**Lectivas (L):** - Desarrollo del tema – 3h - Ejercicios en aula - 1h - Ejercicios en laboratorio 0h **De trabajo Independiente (T.I):** - Desarrollo de ejercicios - 4 h	4	4
2	**Primera sesión** Proceso de la Seguridad Informática	- Explica como es el proceso de la seguridad informática.	**Lectivas (L):** - Desarrollo del tema – 3h - Ejercicios en aula - 1h - Ejercicios en laboratorio 0h **De trabajo Independiente (T.I):** - Desarrollo de ejercicios - 4 h	4	4
3	**Primera sesión** Riesgos, Ataques y Código Malicioso	- Identifica los riesgos, ataques y código malicioso presente en los ambientes computacionales y la relación con las personas.	**Lectivas (L):** - Desarrollo del tema – 3h - Ejercicios en aula - 1h - Ejercicios en laboratorio 0h **De trabajo Independiente (T.I):** - Desarrollo de ejercicios - 4 h	4	4
4	**Primera sesión** Ataques TCP/IP e Ingeniería Social	- Analiza los ataques TCP/IP y Explica los conceptos de ataque de ingeniería social y como mitigarlo.	**Lectivas (L):** - Desarrollo del tema – 3h - Ejercicios en aula - 1h - Ejercicios en laboratorio 0h **De trabajo Independiente (T.I):** Desarrollo de ejercicios - 4 h	4	4

UNIDAD II : CONTROL DE ACCESOS					
CAPACIDAD: • Aplica métodos de control de acceso lógico • Aplica métodos de control de acceso físico • Identifica funciones laborales (roles) en entornos empresariales. • Selecciona los mejores métodos de control de acceso de acuerdo a la necesidad					
SEMANA	**CONTENIDOS CONCEPTUALES**	**CONTENIDOS PROCEDIMENTALES**	**ACTIVIDAD DE APRENDIZAJE**	**HORAS**	
				L	**T.I.**
5	**Primera sesión** Infraestructura y Conectividad	- Analiza los aspectos de seguridad relacionados a la Infraestructura y Conectividad.	**Lectivas (L):** - Desarrollo del tema – 3h - Ejercicios en aula - 1h - Ejercicios en laboratorio 0h **De trabajo Independiente (T.I):** Desarrollo de ejercicios - 4 h	4	4
6	**Primera sesión** Monitoreo y Detección de Intrusos	- Explica las acciones de monitoreo y detección de intrusos, así como el análisis de casos de uso.	**Lectivas (L):** - Desarrollo del tema – 3h - Ejercicios en aula - 1h - Ejercicios en laboratorio 0h **De trabajo Independiente (T.I):** Desarrollo de ejercicios - 4 h	4	4
7	**Primera sesión** Análisis de la Seguridad Física	- Analiza la seguridad física.	**Lectivas (L):** - Desarrollo del tema – 3h - Ejercicios en aula - 1h - Ejercicios en laboratorio 0h **De trabajo Independiente (T.I):** Desarrollo de ejercicios - 4 h	4	4
8	**Primera sesión** Examen Parcial				

UNIDAD III : ANALISIS DE LA INFORMACION DE SEGURIDAD y CRIPTOGRAFIA					
CAPACIDAD: • Reconoce patrones. Aprender a analizar información. • Elabora documentos de resultados. • Reconoce los conceptos de criptografía. • Utiliza algunos métodos criptográficos para asegurar la información.					
SEMANA	**CONTENIDOS CONCEPTUALES**	**CONTENIDOS PROCEDIMENTALES**	**ACTIVIDAD DE APRENDIZAJE**	**HORAS**	
				L	**T.I.**
9	**Primera sesión** Respuesta a Incidentes	- Analiza el proceso de respuesta incidentes de seguridad.	**Lectivas (L):** - Desarrollo del tema – 3h - Ejercicios en aula - 1h - Ejercicios en laboratorio 0h **De trabajo Independiente (T.I):** Desarrollo de ejercicios - 4 h	4	4
10	**Primera sesión** CSIRT	- Analiza la importancia de los CSIRT.	**Lectivas (L):** - Desarrollo del tema – 3h - Ejercicios en aula - 1h - Ejercicios en laboratorio 0h **De trabajo Independiente (T.I):** Desarrollo de ejercicios - 4 h	4	4
11	**Primera sesión** Conceptos generales de criptografía, hashing y encriptación	- Explica los conceptos generales de criptografía, hashing y encriptación.	**Lectivas (L):** - Desarrollo del tema – 3h - Ejercicios en aula - 1h - Ejercicios en laboratorio 0h **De trabajo Independiente (T.I):** Desarrollo de ejercicios - 4 h	4	4
12	**Primera sesión** Protocolos relacionados a criptografía. Criptografía en llaves públicas (PKI)	- Explica los conceptos relacionados a protocolos relacionados a criptografía.	**Lectivas (L):** - Desarrollo del tema – 3h - Ejercicios en aula - 1h - Ejercicios en laboratorio 0h **De trabajo Independiente (T.I):** Desarrollo de ejercicios - 4 h	4	4

UNIDAD IV: SEGURIDAD ORGANIZACIONAL					
CAPACIDAD: • Recomienda planes de respaldo de información. • Recomienda planes de recuperación de desastres • Asiste ante situaciones donde se involucre ingeniería social					
SEMANA	**CONTENIDOS CONCEPTUALES**	**CONTENIDOS PROCEDIMENTALES**	**ACTIVIDAD DE APRENDIZAJE**	**HORAS**	
				L	**T.I.**
13	**Primera sesión** Conceptos de recuperación de desastres, alta disponibilidad y políticas organizacionales	- Explica los conceptos de recuperación de desastres, alta disponibilidad y políticas organizacionales.	**Lectivas (L):** - Desarrollo del tema – 3h - Ejercicios en aula - 1h - Ejercicios en laboratorio 0h **De trabajo Independiente (T.I):** Desarrollo de ejercicios - 04h	4	4
14	**Primera sesión** Tendencias de Seguridad en la Actualidad. Revisión de Casos de Uso Típicos y su recomendación	- Analiza en conjunto los casos y tendencias más recientes de seguridad informática. Se crea conciencia al respecto y se entrega conocimiento para afrontar problemas típicos.	**Lectivas (L):** - Desarrollo del tema – 3h - Ejercicios en aula - 1h - Ejercicios en laboratorio 0h **De trabajo Independiente (T.I):** Desarrollo de ejercicios - 4 h	4	4
15	**Primera sesión** Exposiciones.- Presentación del trabajo de curso	- Realizan exposición de los trabajos asignados.	**Lectivas (L):** - Desarrollo del tema – 3h - Ejercicios en aula - 1h - Ejercicios en laboratorio 0h **De trabajo Independiente (T.I):** Desarrollo de ejercicios - 4 h	4	4
16	Examen final.				
17	Entrega de promedios finales y acta de la asignatura				

V. ESTRATEGIAS METODOLÓGICAS

- **Método Expositivo – Interactivo**. Disertación docente, exposición del estudiante.
- **Método de Discusión Guiada**. Conducción del grupo para abordar situaciones y llegar a conclusiones y recomendaciones.
- **Método de Demostración – Ejecución**. El docente ejecuta para demostrar cómo y con que se hace y el estudiante ejecuta, para demostrar que aprendió

VI. RECURSOS DIDÁCTICOS

- **Equipos**: Una computadora personal para el profesor, ecran y proyector de multimedia.
- **Materiales**: Separata del alumno.

VII. EVALUACIÓN DEL APRENDIZAJE

El promedio final (PF) de la asignatura se obtiene con la siguiente fórmula:

$$PF = (2*PE+EP+EF)/4$$

Donde: PF = Promedio Final.
PE = Promedio de Evaluaciones.
EP = Examen Parcial (escrito)
EF = Examen Final (escrito)

$$PE = ((P1+P2+P3+P4–MN)/3 + W1) /2$$

Donde: P1...P4 = Práctica calificada
MN = Menor nota
W1 = Trabajo 1

VIII. FUENTES DE CONSULTA.

8.1 Bibliográficas

- Whitman, Michael (2010). Management of Information Security. Tercera Edición. Publisher: Course Technology.
- Dulaney, Emmett. (2017). CompTIA Security+ Study Guide. Publisher: Sybex.

IX. APORTE DE LA ASIGNATURA AL LOGRO DE RESULTADOS

El aporte de la asignatura al logro de los Resultados del Estudiante (*Student Outcomes*) en la formación del graduado en Ingeniería de Computación y Sistemas, se establece en la tabla siguiente:

K = clave **R** = relacionado **Recuadro vacío** = no aplica

a.	Habilidad para aplicar conocimientos de computación y matemáticas apropiadas para los resultados del estudiante y las disciplinas enseñadas.	R
b.	Habilidad para analizar un problema e identificar y definir los requerimientos apropiados para su solución.	R
c.	Habilidad para diseñar, implementar y evaluar un sistema basado en computadoras, procesos, componentes o programa que satisfagan las necesidades requeridas.	K
d.	Habilidad para trabajar con efectividad en equipos para lograr una meta común.	
e.	Comprensión de los aspectos y las responsabilidades profesional, ética, legal, de seguridad y social.	R
f.	Habilidad para comunicarse con efectividad con un rango de audiencias.	
g.	Habilidad para analizar el impacto local y global de la computación en los individuos, organizaciones y la sociedad.	R
h.	Reconocer la necesidad y tener la habilidad para comprometerse a un continuo desarrollo profesional.	
i.	Habilidad para usar técnicas, destrezas, y herramientas modernas necesarias para la práctica de la computación.	R
J	Comprensión de los procesos que soportan la entrega y la administración de los sistemas de información dentro de un entorno específico de aplicación.	