SILABO

I. INFORMACIÓN GENERAL

1.1.	**Nombre de la asignatura**	**SEGURIDAD DE INFORMACIÓN**
1.2.	**Código**	IS16101
1.3.	**Año Calendario**	2019
1.4.	**Semestre Académico**	II
1.5.	**Créditos Académicos**	04
1.6.	**Pre - requisitos**	IS16091
1.7.	**N° total de horas presenciales:**	
	• **HORAS TEORICAS**	03
	• **HORAS PRACTICAS**	02
	• **TOTAL HORAS**	05
1.8.	**Duración del ciclo**	17 SEMANAS
1.9.	**Docente responsable**	Mag. Edison Chiclla Carrasco

II. SUMILLA

La asignatura de Seguridad de Información, es una asignatura de naturaleza Teórico – Práctica, tiene como propósito desarrollar en los alumnos, la habilidad para comprender los conceptos básicos de seguridad de la información e implementar mecanismos de protección en entornos empresariales Se desarrollará los siguientes temas: Introducción a Ethical hacking, fases del Ethical hacking, seguridad perimetral, criptografía y seguridad física.

III. COMPETENCIA

El estudiante elaborara un proyecto de implementación de un sistema de seguridad usando las herramientas y aplicando la teoría impartida en clase y los casos prácticos impartidos en laboratorios, centralizado en los que controla vulnerabilidades, almacenamiento de logs, monitoreo y mecanismos de protección frente a ataques.

IV. RESULTADOS DE APRENDIZAJE

1. Elabora esquemas en el que aplique la teoría en casos prácticos empresariales justificando cada uno de ellos, demostrando calidad de información y responsabilidad en su presentación.
2. Realiza un Ethical hacking completo, aplicando las 5 fases y entregando un informe sustentando por cada fase sus resultados, evidencias y recomendaciones.
3. implementa soluciones de seguridad informática que ayuden a minimizar el riesgo de ataques a las organizaciones.
4. Implementa las soluciones de seguridad Web basadas en certificados digitales, demostrando seguridad y dominio del tema y presentando su trabajo en la fecha indicada.

V. CONTENIDO PROGRAMÁTICO

Unidad 1: Introducción al Ethical Hacking

- Conceptos Básicos
- Historia de los Hackers
- Tipos de Ethical Hacking
- Etapas del Ethical Hacking
- Metodologías de Evaluación
- SO Linux

Unidad 2: Seguridad en Protocolos TCP/IP

- Protocolos de la pila TCP/IP
- Sniffing
- Envenenamiento ARP
- Denegación de Servicio
- Malware (Virus, Troyanos, Gusanos, Bombas Lógicas, Botnets, etc)
- Google Hacking
- Interrogación DNS

Unidad 3: Scanning y Análisis de vulnerabilidades

- Escaneo de Puertos y Enumeración de Servicios
- Nmap
- Analizadores a Nivel Plataforma
- Analizadores a Nivel Aplicación

Unidad 4: Inseguridad en Aplicaciones Web

- Vulnerabilidades Web
- Frameworks de Aprendizaje
- Trabajando con Exploits
- Metasploit Framework
- La Navaja Suiza del Hacker
- Password Cracking

VI. ESTRATEGIAS DIDÁCTICAS

La asignatura está organizada en momentos presenciales. En la fase presencial se trabaja con técnicas participativas, haciendo un seguimiento individual y grupal de los logros de cada estudiante, este a su vez desarrolla trabajos en los cuales plasmará los conocimientos adquiridos en cada sesión de clase.

VII. MATERIALES

- Clases teóricas: equipo multimedia, diapositivas, pizarra, plumones,
- Clases prácticas: Resumen de lecturas entregadas previamente, estudio de casos

VIII. EVALUACIÓN

Promedio Parcial 1						Promedio Parcial 2						Nota Final		
PC1	IF1	EXP1	EA1	EP1	PP1	PC2	IF2	EXP2	EA2	EP2	PP2	PF	A	PA

							(PC1+IF1+EXP1+EA1+EP1)/5					(PC2+IF2+EXP2+EA2+EP2)/5	(PP1+PP2)/2	Reemplaza al promedio final siempre que haya obtenido 7 como mínimo	
Código	Nombres	Practica Calificada	Investigación Formativa	Exposición	Evaluación Actitudinal	Examen Parcial 01	Promedio Parcial 1	Practica Calificada	Investigación Formativa	Exposición	Evaluación Actitudinal	Examen Parcial 02	Promedio Parcial	Promedio Final	Aplazado	Promedio Acta
		Nota: Las notas para la obtención del promedio parcial 1 estará abierto desde la semana 1 hasta la semana 8						Nota: Las notas para la obtención del promedio parcial 2 estará abierto desde la semana 9 hasta la semana 16							Nota: La nota del aplazado será en la semana 17	

Leyenda:

Promedio Parcial 1

Practica Calificada	=	PC1
Investigación Formativa	=	IF1
Exposición	=	EXP1
Evaluación Actitudinal	=	EA1
Examen Parcial 01	=	EP1
Promedio Parcial : (PC1+IF1+EXP1+EA1+EP1)/5	=	PP1

Nota: Las notas para la obtención del promedio parcial 1 estará abierto desde la semana 1 hasta la semana 8

Promedio Parcial 2

Practica Calificada	=	PC2
Investigación Formativa	=	IF2
Exposición	=	EXP2
Evaluación Actitudinal	=	EA2
Examen Parcial 01	=	EP2
Promedio Parcial : (PC2+IF2+EXP2+EA2+EP2)/5	=	PP2

Nota: Las notas para la obtención del promedio parcial 2 estará abierto desde la semana 9 hasta la semana 16

Nota Final

Promedio Final: (PP1+PP2)/2	=	PF
Aplazado : Reemplaza al promedio final siempre que haya obtenido 7 como mínimo	=	A
Promedio Acta	=	PA

Nota: La nota del aplazado será en la semana 17

Resultado de aprendizaje	Contenidos	Evidencias	Indicadores	Instrumentos

Unidad 1: Introducción al Ethical Hacking	• Conceptos Básicos • Historia de los Hackers • Tipos de Ethical Hacking • Etapas del Ethical Hacking • Metodologías de Evaluación • SO Linux	Examen Escrito Practica de calificada	Define y analiza la importancia del Ethical Hacking	Escala de evaluación Lista de cotejo Registro de Asistencia
Unidad 2: Seguridad en Protocolos	• TCP/IP • Protocolos de la pila TCP/IP • Sniffing • Envenenamiento ARP • Denegación de Servicio • Malware (Virus, Troyanos, Gusanos, Bombas Lógicas, Botnets, etc) • Google Hacking • Interrogación DNS	Examen Escrito Práctica de calificada	Comprende y explica la importancia de la seguridad en los protocolos de comunicación	Escala de evaluación Lista de cotejo Registro de Asistencia
Unidad 3: Scanning y Análisis de vulnerabilidades	• Escaneo de Puertos y Enumeración de Servicios • Nmap • Analizadores a Nivel Plataforma • Analizadores a Nivel Aplicación	Examen Escrito Practica de calificada	Evalúa las vulnerabilidades de los sistemas informáticos	Escala de evaluación Lista de cotejo Registro de Asistencia
Unidad 4: Inseguridad en Aplicaciones Web	• Vulnerabilidades Web • Frameworks de Aprendizaje • Trabajando con Exploits • Metasploit Framework • La Navaja Suiza del Hacker • Password Cracking	Examen Escrito Practica de calificada	Elaborar medidas de seguridad para las aplicaciones web	Escala de evaluación Lista de cotejo Registro de Asistencia

Mag. Edison Chiclla Carrasco
DOCENTE DEL CURSO

ANEXOS

PROGRAMACIÓN DE ACTIVIDADES

Nro. de Sesión	Fecha y Hora	Contenidos	Actividad de Aprendizaje	Docente Responsable
1	18/09/201	Conceptos Básicos	Exposición dialogada	Mag.

	9			Edison Chiclla Carrasco
2	20/09/2019	Historia de los Hackers	Exposición dialogada	
3	25/09/2019	Tipos de Ethical Hacking	Exposición dialogada y Actividades prácticas	
4	27/09/2019	Etapas del Ethical Hacking	Exposición dialogada y Actividades prácticas	
5	02/10/2019	Metodologías de Evaluación	Exposición dialogada y Actividades prácticas	
6	04/10/2019	SO Linux	Exposición dialogada y Actividades prácticas	
7	09/10/2019	TCP/IP	Exposición dialogada y Actividades prácticas	
8	11/10/2019	Protocolos de la pila TCP/IP	Exposición dialogada y Actividades prácticas	
9	16/10/2019	Sniffing	Exposición dialogada y Actividades prácticas	
10	18/10/2019	Envenenamiento ARP	Exposición dialogada y Actividades prácticas	
11	23/10/2019	Denegación de Servicio	Exposición dialogada y Actividades prácticas	
12	25/10/2019	Malware (Virus, Troyanos, Gusanos, Bombas Lógicas, Botnets, etc)	Exposición dialogada y Actividades prácticas	
13	30/10/2019	Google Hacking	Exposición dialogada y Actividades prácticas	
14	01/11/2019	Interrogación DNS	Exposición dialogada y Actividades prácticas	
15	06/11/2019	Examen Practico Primera Parcial	***Practica Calificada***	
16	08/11/2019	Examen Teórico Primera Parcial	***Evaluación Escrita***	
17	13/11/2019	Introducción a escaneo de puertos	Exposición dialogada y Actividades prácticas	
18	15/11/2019	Escaneo de Puertos y Enumeración de Servicios	Exposición dialogada y Actividades prácticas	
19	20/11/2019	Nmap	Exposición dialogada y Actividades prácticas	
20	22/11/2019	Uso de herramientas de scanning	Exposición dialogada y Actividades prácticas	
21	27/11/2019	Introducción al Análisis de Vulnerabilidades	Exposición dialogada y Actividades prácticas	
22	29/11/2019	Analizadores a Nivel Plataforma	Exposición dialogada y Actividades prácticas	
23	04/12/2019	Analizadores a Nivel Aplicación	Exposición dialogada y Actividades prácticas	
24	06/12/2019	Reconociendo vulnerabilidades a nivel plataforma con Nessus,NeXpose	Exposición dialogada y Actividades prácticas	
25	11/12/2019	Vulnerabilidades Web	Exposición dialogada y Actividades prácticas	
26	13/12/2019	Frameworks de Aprendizaje	Exposición dialogada y Actividades prácticas	
27	18/12/2019	Explotando vulnerabilidades Web (RFI, SQLi, LFI)	Exposición dialogada y Actividades prácticas	
28	20/12/201	Trabajando con Exploits	Exposición dialogada y Actividades	

	9		prácticas	
29	25/12/2019	Metasploit Framework	Exposición dialogada y Actividades prácticas	
30	27/12/2019	La Navaja Suiza del Hacker	Exposición dialogada y Actividades prácticas	
31	01/01/2020	Password Cracking	Exposición dialogada y Actividades prácticas	
32	03/01/2020	Explotando vulnerabilidades con Metasploit	Exposición dialogada y Actividades prácticas	
33	08/01/2020	Examen Practico Primera Parcial	***Practica Calificada***	
34	10/01/2020	Examen Teórico Primera Parcial	***Evaluación Escrita***	
35	13/01/2020	Examen Práctico y Escrito Subsanación	***Subsanación***	