I. INFORMACIÓN GENERAL

CURSO	:	Fundamentos De Ciberseguridad
CÓDIGO	:	SI466
CICLO	:	202102
CUERPO ACADÉMICO	:	**Burga Durango, Daniel Wilfredo**
CRÉDITOS	:	3
SEMANAS	:	16
HORAS	:	3 H (Teoría) Semanal
ÁREA O CARRERA	:	Computacion E Informatica

II. MISIÓN Y VISIÓN DE LA UPC

Misión: Formar líderes íntegros e innovadores con visión global para que transformen el Perú.

Visión: Ser líder en la educación superior por su excelencia académica y su capacidad de innovación.

III. INTRODUCCIÓN

Descripción:
El Curso Electivo de Fundamentos de Ciberseguridad, en la Carrera de Ingeniería de Sistemas de Información es de carácter teórico-práctico. La ciberseguridad es una industria dinámica y en crecimiento. Como disciplina académica, la ciberseguridad nunca ha sido más profunda ni más importante, ya que ha evolucionado de una concentración relativamente oscura a un campo altamente complejo e interdisciplinario rico en posibilidades de investigación y aplicaciones del mundo real.
Las ciberamenazas contra, gobiernos, empresas o individuos, están tomando continuamente formas más complejas y peligrosas. En este momento, los ciberatacantes altamente calificados de todo el mundo están en el proceso de diseñar métodos de ataque revolucionarios para frustrar las últimas innovaciones en ciberseguridad. Como consecuencia, los profesionales de la ciberseguridad de hoy en día deben poseer una variedad de habilidades académicas, técnicas y una nueva mentalidad, para asegurar la información, servicios, infraestructura y personas de diferentes vectores ataques.
Propósito:
El propósito de este curso, es proporcionar una introducción a las disciplinas que son fundamentales para proteger los activos de la organización en el mundo moderno. Aprenderá cómo se pueden aplicar los marcos de ciberseguridad

IV. LOGRO (S) DEL CURSO

Al finalizar el curso, desarrolla conocimientos de ciberseguridad y ayudarlo a prepararse para la certificación de Fundamentos de Ciberseguridad del ISACA (CSX), así mismo mejorar sus habilidades en el manejo de herramientas de ciberseguridad.

V. UNIDADES DE APRENDIZAJE

UNIDAD Nº: 1 Visión Global de la ciberseguridad

LOGRO

Logro de la unidad: Al finalizar la unidad el alumno, identificará los conceptos necesarios para reconocer y mitigar los ataques contra las redes empresariales y la infraestructura de misión crítica, explica cómo convertirse en un especialista en ciberseguridad, explora el panorama de la ciberseguridad.

TEMARIO

TEMARIO
Introducción a la ciberseguridad
Las cinco fase de Penetration Testing
Herramientas y técnicas de Open Source Intelligence (OSINT).
Introducción al Footprinting
Introducción al Scanning
Introducción a la Enumeration
Introducción al ¿System Hacking¿
PRÁCTICAS DE LABORATORIO:
Footprinting: AnyWho, nslookup, Maltego, Recon-Ng, theHarvester, Shodan, G.Dorks
Scanning: DNS Enumeration, hPing3, nikTo, NMap , Web Data Extractor
Enumeration: Nbtstat, netuse, null session, netDiscover, smbclient, superscan, Pstools
System hacking: ADS Spy, Link Control Protocol, pwdump, x.exe, sthC, snow,

HORA(S) / SEMANA(S)

9 H / semana 1, 2 y 3

UNIDAD Nº: 2 Ciberamenazas , Vectores de Ataque y Malware

LOGRO

Logro de la unidad: Al finalizar la unidad, el estudiante comprende los diferentes vectores de ataque, que se ven comúnmente en el entorno actual, conocen cómo se llevan a cabo los ataques. Comprende cómo se distribuye el malware y evade las medidas de seguridad usando virtualización.

TEMARIO

TEMARIO
Introducción a las amenazas ciberinteligentes y la cadena Cyber Kill
Introducción a los virus y gusanos
Introducción al Sniffing traffic y Denegación de servicio
Introducción a la Ingeniería social
Introducción a ¿Session Hijacking¿ y ¿Hacking Web Servers¿

PRACTICAS DE LABORATORIO
Viruses & Worms: bintext, delME, Internet Worm Maker Thing, JPS.
Sniffing Traffic: macof, Driftnet, SMAC, tshark, urlsnarf, WebSpy
Denial of Service & Hijacking: hping3, LOIC; Hamster, Ferret
Hacking Web Servers: dirbuster, WPScan,
Web Applications: burpSuite, HTTPRecon, IDServe, nikto,Virus Total, WGet

HORA(S) / SEMANA(S)

12 H / Semana 4, 5, 6 y 7

UNIDAD Nº: 3 Ingeniería de Seguridad

LOGRO

Logro de la unidad: Al finalizar la unidad, el alumno entiende los conceptos fundamentales de modelos de seguridad, entender la aplicación y uso de la criptografía, métodos de ataques criptográficos, emplear la criptografía en la seguridad de red.

TEMARIO

TEMARIO
Ciberseguridad y el IoT: Sector industrial, hogar conectado, wearables del consumidor
Introducción a la Inyección SQL
Introducción al Mobile Hacking
Introducción al IDS, Firewalls y Honeypots
Introducción al Buffer Overflows

PRACTICA DE LABORATORIO
SQL Injection: BlindElephant, phpID, sqlmap
IDS, Firewalls & Honeypots
Buffer Overflows: make, compile, run, stack

HORA(S) / SEMANA(S)

9 H / Semana 9, 10 y 11

UNIDAD Nº: 4 Detectar y Mitigar CiberAtaques

LOGRO

Logro de la unidad: Al finalizar la unidad, el alumno analiza la detección y mitigación de amenazas, identifica los vectores de ataque, explica cómo utilizar herramientas y principios para proteger la información. Realiza sugerencias sobre qué tipo de estrategias de mitigación es adecuada.

TEMARIO

TEMARIO
Introducción al análisis forense digital moderno
El proceso de investigación
Búsqueda, captura y evidencia digital
Discos duros y sistemas de archivos
Análisis forense de Windows
Recuperación y borrado de archivos

TEMARIO DE CLASE
Investigative Processs: Inspector File, RecoveryMyFile, md5sum
First Responder: chkdik and format NTFS; Hex workshop bit flipping and overwiew
Computer Forensics: FileMerlin, FileViewer, Paraben P2 Explorer.
Hard disks and File Systems: Efsinfo, FileScanvenger, ProcessMonitor, Regshot, Easycleaner Regshot, HDValet Regshot, Rname it, Add/Remove Pro
Recovering Files: DDR, Scavenger, Handy, Necleus,Testdisk, Total Recall, WinUndelete

HORA(S) / SEMANA(S)

16 H / Semana 12, 13, 14 y 15

VI. METODOLOGÍA

En el curso se aplicará una metodología activa, dinámica participativa con el uso de herramientas. El profesor cumplirá el rol de facilitador y compartirá sus experiencias en clase contribuyendo al crecimiento profesional del estudiante.

VII. EVALUACIÓN

FÓRMULA

10% (EA1) + 5% (PA1) + 25% (TF1) + 15% (EB1) + 10% (CL1) + 10% (CL2) + 10% (PC1) + 15% (PC2)

TIPO DE NOTA	PESO %
CL - CONTROL DE LECTURA	10
PC - PRÁCTICAS PC	10
EA - EVALUACIÓN PARCIAL	10
CL - CONTROL DE LECTURA	10
PC - PRÁCTICAS PC	15
PA - PARTICIPACIÓN	5
TF - TRABAJO FINAL	25
EB - EVALUACIÓN FINAL	15

VIII. CRONOGRAMA

TIPO DE PRUEBA	DESCRIPCIÓN NOTA	NÚM. DE PRUEBA	FECHA	OBSERVACIÓN	RECUPERABLE
CL	CONTROL DE LECTURA	1	Semana 3	Evidencia de aprendizaje: Entrega de informe Competencias evaluadas: Aprendizaje continuo y autónomo Aplicar las nuevas tecnologías Trabajo individual	NO
PC	PRÁCTICAS PC	1	Semana 6	Evidencia de aprendizaje: Práctica Calificada 1 Competencia evaluada: Aprendizaje continuo y autónomo Aplicar las nuevas tecnologías Trabajo Individual	SÍ
EA	EVALUACIÓN PARCIAL	1	Semana 8	Evidencia de aprendizaje: Evaluación escrita Competencias evaluadas: Aprendizaje continuo y autónomo Aplicar las nuevas tecnologías Evaluación individual	SÍ
CL	CONTROL DE LECTURA	2	Semana 11	Evidencia de aprendizaje: Entrega de informe Competencias evaluadas: Aprendizaje continuo y autónomo Aplicar las nuevas tecnologías Trabajo individual	NO
PC	PRÁCTICAS PC	2	Semana 13	Evidencia de aprendizaje: Práctica Calificada 2 Competencia evaluada: Aprendizaje continuo y autónomo Aplicar las nuevas tecnologías Trabajo Individual	SÍ
PA	PARTICIPACIÓN	1	Semana 15	Evidencia de aprendizaje: Participación en clase Competencias evaluadas: Aprendizaje continuo y autónomo Aplicar las nuevas tecnologías Trabajo individual	NO
TF	TRABAJO FINAL	1	Semana 15	Evidencia de aprendizaje Entregables: Presentación, informe ejecutivo y Lab. Competencias evaluadas: Aprendizaje continuo y autónomo Aplicar las nuevas tecnologías Trabajo grupal	NO
EB	EVALUACIÓN FINAL	1	Semana 16	Evidencia de aprendizaje: Evaluación escrita Competencia evaluada: Aprendizaje continuo y autónomo Aplicar las nuevas tecnologías Evaluación individual	SÍ

IX. BIBLIOGRAFÍA DEL CURSO

https://upc.alma.exlibrisgroup.com/leganto/readinglist/lists/6505344530003391?institute=51UPC_INST&auth=LOCAL