I. INFORMACIÓN GENERAL

CURSO	:	Seguridad Informática
CÓDIGO	:	CC66
CICLO	:	202102
CUERPO ACADÉMICO	:	**Abanto Garnique, Jorge Luis**
CRÉDITOS	:	4
SEMANAS	:	16
HORAS	:	4 H (Teoría) Semanal
ÁREA O CARRERA	:	Ciencias de la Computacion

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

El curso de Seguridad Informática realiza una exploración de las buenas prácticas de seguridad que se aplican sobre los activos informáticos basados en tecnologías de la información y comunicaciones (TIC). Aplicando buenas prácticas de gobierno de seguridad, ética en ingeniería, gestión de riesgos, defensa en profundidad, manejo de incidentes, auditoria, regulaciones y análisis forense; para la protección de los activos informáticos. Así como también diseña y desarrolla sistemas de software basados en algoritmos computacionales vinculados con la Seguridad Informática.

El curso busca desarrollar la competencia general de Ciudadanía de nivel 2 y la competencia específica de Diseño y Desarrollo de una Solución de nivel 2 para la carrera Ciencias de la computación.

IV. LOGRO (S) DEL CURSO

Al finalizar el curso, el estudiante aplica prácticas de Seguridad Informática así como también diseña y construye de sistemas de software con código seguro, evidenciando manejo ético y responsable de los derechos de los demás..

Competencia:
Ciudadanía

Nivel de logro:
2

Definición:
Capacidad para valorar la convivencia humana en sociedades plurales, reflexionando acerca de las dimensiones morales de las propias acciones y decisiones, asumiendo la responsabilidad por las consecuencias en el marco

del respeto de los derechos y deberes ciudadanos.

Competencia:
Diseño y Desarrollo de una Solución

Nivel de logro:
2

Definición:
Diseñar, implementar y evaluar una solución basada en la computación para cumplir con un conjunto de requisitos computacionales en el contexto de la disciplina del programa.

V. UNIDADES DE APRENDIZAJE

UNIDAD Nº: 1 Gobierno Seguridad: Seguridad Informática y Seguridad de la Información

LOGRO

Logro de la unidad: Al finalizar la unidad, el estudiante aplica controles de seguridad informática de forma ética, construyendo y diseñando algoritmos basados en seudocódigos y diagramas de flujo para resolver casos de Seguridad Informática.

TEMARIO

Competencia(s):
Ciudadanía,
Diseño y Desarrollo de una Solución

Contenido 1:
¿Gobierno de Seguridad: Seguridad Informática y Seguridad de la Información
¿Ética en Seguridad Informática

Actividades de aprendizaje:
¿Exposición participativa y dinámica
¿Lectura de textos

Evidencias de aprendizaje:
¿Resolución de Casos propuestos en Foros

Bibliografía:
Piattini, M., & Hervada, F. (2007). Gobierno de las Tenologías y los Sistemas de Información

Cano, J. (2011). La Gerencia de la Seguridad de la Information: Evolución y Retos Emergentes

ACM. (1993). Cases: Code of Ethics and Professional Conduct

ACM. (2018). Code of Ethics and Professional Conduct

Contenido 2:
¿Política de Seguridad y Niveles de Madurez en Seguridad

Actividades de aprendizaje:

¿Presentación de Matriz de Madurez en Seguridad
¿Lectura de textos

Evidencias de aprendizaje:
¿Resolución de Casos propuestos en Foros

Bibliografía:
Piattini, M., & Hervada, F. (2007). Gobierno de las Tenologías y los Sistemas de Información

COBIT (2016)

Sinanc, D., & Sagiroglu, S. (2013). A Review on Cloud Security

Odeshina, N. (2013). ISO/IEC 27001:2005 Implementation and Certification¿Doing It Again and Again.

Contenido 3:
¿Objetivos de Control y Controles de Seguridad de la Información y de Seguridad Informática

Actividades de aprendizaje:
¿Presentación de Matriz de Controles de Seguridad
¿Lectura de textos

Evidencias de aprendizaje:
¿CL1 (Control de Lectura)

Bibliografía:
Piattini, M., & Hervada, F. (2007). Gobierno de las Tenologías y los Sistemas de Información

COBIT (2016)

Contenido 4:
¿Diseño y construcción de algoritmos en Seguridad Informática

Actividades de aprendizaje:
¿Presentación de Algoritmos basados en Seudocódigos y Diagramas de flujo
¿Lectura de textos

Evidencias de aprendizaje:
¿Resolución de algoritmos propuestos en Foros

Bibliografía:
Naqvi, F. (2014). Reinspecting Password, Account Lockout and Audit Policies

HORA(S) / SEMANA(S)
Semanas 1, 2, 3 y 4

UNIDAD Nº: 2 Gestión de Riesgos Informáticos

LOGRO
Logro de la unidad: Al finalizar la unidad, el estudiante evalúa los riesgos sobre los activos informáticos en base a aspectos: éticos, legales, principios y prácticas en la ingeniería de seguridad informática.

TEMARIO

Competencia(s):
Ciudadanía,
Diseño y Desarrollo de una Solución

Contenido 5:
¿Fundamentos en la Gestión de Riesgos

Actividades de aprendizaje:
¿Exposición participativa y dinámica
¿Presentación de Matriz de Gestión de Riesgos en Seguridad Informática
¿Lectura de textos

Evidencias de aprendizaje:
¿Resolución de Casos propuestos en Foros

Bibliografía:
Tipton, H. (2009). Information Security Management Handbook

Dahbur, K., Mohammad, B., & Tarakji, A. B. (2011). A Survey of Risks, Threats and Vulnerabilities in Cloud Computing

Gotterbarn, D. (2016). THINKING PROFESSIONALLY: A professional approach to risk management: the missing use case exercise

Contenido 6:
¿Marco de trabajo para la evaluación y análisis de riesgos informáticos

Actividades de aprendizaje:
¿Presentación de Matriz de Controles de Seguridad y Auditoria
¿Lectura de textos

Evidencias de aprendizaje:
¿Resolución de Casos propuestos en Foros
¿CL2 (Control de Lectura)

Bibliografía:
Tipton, H. (2009). Information Security Management Handbook

Lee, J. (2014). An Enhanced Risk Formula for Software Security Vulnerabilities

Contenido 7:
¿Automatización de Controles de Seguridad y Auditoría Informática

Actividades de aprendizaje:
¿Presentación de Algoritmos Codificados en PowerShell o Visual C++.

Evidencias de aprendizaje:
¿TP (Trabajo Parcial)

Bibliografía:

Tipton, H. (2009). Information Security Management Handbook

Contenido 8:
AEvidencias de aprendizaje:
¿EA (Examen Parcial)

HORA(S) / SEMANA(S)
Semanas 5, 6, 7 Y 8

UNIDAD Nº: 3 Programa de Seguridad basado en Defensa en profundidad (Defense in depth)

LOGRO

Logro de la unidad: Al finalizar la unidad, el estudiante aplica prácticas de seguridad basado en Defensa en profundidad sobre los activos informáticos; construyendo y diseñando algoritmos basados en seudocódigos y diagramas de flujo para resolver casos de Seguridad Informática.

TEMARIO

Competencia(s):
Ciudadanía,
Diseño y Desarrollo de una Solución

Contenido 9:
¿Fundamentos de Seguridad basado en Defensa en profundidad (Defense in depth)

Actividades de aprendizaje:
¿Exposición participativa y dinámica
¿Lectura de textos

Evidencias de aprendizaje:
¿Resolución de Casos propuestos en Foros

Bibliografía:
Piattini, M., Peso, E. d., & Peso, M. d. (2008). Auditoría de Tenologías y Sistemas de Información

Townsend, M. (2009). Managing a Security Program in a Cloud Computing

Saleem, S. (2006). Ethical hacking as a risk management technique

Contenido 10:
¿Principios de Diseño de Seguridad: Programación Defensiva

Actividades de aprendizaje:
¿Exposición participativa y dinámica
¿Lectura de textos

Evidencias de aprendizaje:
¿Resolución de Casos propuestos en Foros

Bibliografía:
Piattini, M., Peso, E. d., & Peso, M. d. (2008). Auditoría de Tenologías y Sistemas de Información

Acosta, E. (2013). Defensive Strategic Posture in the Field of Information Security

Mavroeidakos, T., Michalas, A., & Vergados, D. (2016). Security Architecture based on Defense in Depth for Cloud Computing Environment

Contenido 11:
¿Prácticas para diseño y construcción de Código Seguro en Seguridad Informática

Actividades de aprendizaje:
¿Presentación de Algoritmos basados en Seudocódigos
¿Lectura de textos

Evidencias de aprendizaje:
¿Resolución de Casos propuestos en Foros

Bibliografía:
Tipton, H. (2009). Information Security Management Handbook

Yu, H., Jones, N., Bullock, G., & Yuan, X. Y. (2011). Teaching secure software engineering: Writing secure code

Straub, K. (2013). Information Security: Managing Risk with Defense in Depth. SANS.

Contenido 12:
¿Diseño y construcción de algoritmos basado en Código Seguro

Actividades de aprendizaje:
¿Presentación de Algoritmos basados en Seudocódigos y Diagramas de flujo
¿Lectura de textos

Evidencias de aprendizaje:
¿Resolución de algoritmos propuestos en Foros

Bibliografía:
Tipton, H. (2009). Information Security Management Handbook

Mahalkari, A., Tailor, A., & Shukla, A. (2016). Cloud Computing Security, Defense In Depth Detailed Survey. IJCSIT.

Vibhandik, R., & Bose, A. K. (2015). Vulnerability assessment of web applications - a testing approach

HORA(S) / SEMANA(S)
Semanas 9, 10, 11 y 12

UNIDAD Nº: 4 Incidentes de Seguridad de la Información, Prácticas de Auditoría y Análisis Forense y Diseño y Desarrollo de una Solución

LOGRO
Logro de la unidad: Al finalizar la unidad, el estudiante aplica la gestión de incidentes de Seguridad de la Información, construyendo y diseñado sistemas software para de detectar, investigar, responder y recuperarse de incidentes de seguridad

TEMARIO

Competencia(s):
Ciudadanía,
Diseño y Desarrollo de una Solución

¿Fundamentos de la Gestión de Incidentes, Procedimientos de Investigación y Plan de Respuesta

Actividades de aprendizaje:
¿Exposición participativa y dinámica
¿Lectura de textos

Evidencias de aprendizaje:
¿Resolución de Casos propuestos en Foros

Bibliografía:
Council, E. (2107). COMPUTER FORENSIC: Investigation Procedures and Response

Saleem, S. (2006). Ethical hacking as a risk management technique

Contenido 14:
¿Análisis Forense Digital, y su automatización usando algoritmos basados en seudocódigos

Actividades de aprendizaje:
¿Exposición participativa y dinámica
¿Lectura de textos

Evidencias de aprendizaje:
¿Resolución de Casos propuestos en Foros
¿LB1 (Práctica de Laboratorio)

Bibliografía:
Council, E. (2017). COMPUTER FORENSIC: Investigating File and Operating Systems, Wireless, Networks and Storage

Ariu, D., Giacinto, G., & Roli, F. (2011). Machine Learning in Computer Forensics (and the Lessons Learned from Machine Learning in Computer Security)

Contenido 15:
- Diseño y construcción de software para de detectar, investigar, responder y recuperarse de incidentes de seguridad
-Diseño y Desarrollo de una Solución

Actividades de aprendizaje:
- Presentación de Algoritmos basados en Seudocódigos y Diagramas de flujo
- Presentación de Algoritmos Codificados en PowerShell o Visual C++.

Evidencias de aprendizaje:
- Resolución de Casos propuestos en Foros
- PA (Participación)
- TF (Trabajo Final)

Bibliografía:
Doswell, F. (2008). A Case Study on Computer Security for Non-Expert Computer Use

Gardiner, J., & Nagaraja, H. (2016). On the Security of Machine Learning in Malware C&C Detection: A survey

HORA(S) / SEMANA(S)
Semanas 13, 14, 15

UNIDAD Nº: 5 Outcome ABET: Diseño y Desarrollo de una Solución

LOGRO
Competencia(s):
Diseño y Desarrollo de una Solución

Logro de la unidad: Al finalizar la unidad, el estudiante aplica la gestión de incidentes de Seguridad de la Información, construyendo y diseñado sistemas software para de detectar, investigar, responder y recuperarse de incidentes de seguridad

TEMARIO
Contenido 15:
- Diseño y Desarrollo de una Solución

Actividades de aprendizaje:
- Presentación participativa de diapositvas

Evidencias de aprendizaje:
- TF (Trabajo Final)

Contenido 16:
Evidencias de aprendizaje:
- EB (Examen Final)

HORA(S) / SEMANA(S)
Semana 15 y 16

VI. METODOLOGÍA

El Modelo Educativo de la UPC asegura una formación integral, la cual tiene como pilar el desarrollo de competencias. Estas son promovidas a través de un proceso de enseñanza-aprendizaje donde el estudiante cumple un rol activo en su aprendizaje. En este proceso dinámico, las competencias son construidas a partir de la reflexión crítica, el análisis, la discusión, la evaluación, la exposición y la interacción con sus pares, y conectándolas con sus experiencias y conocimientos previos. Por ello, cada sesión está diseñada para ofrecer al estudiante diversas maneras de apropiarse y poner en práctica el nuevo conocimiento en contextos reales o simulados, reconociendo la importancia que esto tiene para su éxito profesional.

El curso se desarrolla en dos sesiones en total de 4 horas semanal, una de 2 horas de teoría y la segunda de 2 horas de laboratorio, que otorgan la base conceptual y práctica para que el estudiante logre las competencias del curso, en el laboratorio se utilizará software tales como: C++, JAVA, Power Shell, DEV++ y Visual Estudio
La metodología a utilizarse en el curso, es una Metodología Activa. Como parte de su aplicación, se fomentará la participación de los alumnos mediante dinámicas grupales, durante las clases, y a través del Blackboard o aula virtual mediante los foros virtuales. De igual modo, se desarrollará un trabajo aplicativo, el cual implicará

el análisis y profundización de los temas del curso. El profesor cumplirá el rol de facilitador y compartirá sus experiencias en clase contribuyendo al crecimiento profesional del estudiante.

VII. EVALUACIÓN

FÓRMULA

10% (CL1) + 10% (CL2) + 5% (TP1) + 15% (EA1) + 10% (LB1) + 5% (PA1) + 20% (TF1) + 25% (EB1)

TIPO DE NOTA	PESO %
CL - CONTROL DE LECTURA	10
CL - CONTROL DE LECTURA	10
TP - TRABAJO PARCIAL	5
EA - EVALUACIÓN PARCIAL	15
LB - PRACTICA LABORATORIO	10
PA - PARTICIPACIÓN	5
TF - TRABAJO FINAL	20
EB - EVALUACIÓN FINAL	25

VIII. CRONOGRAMA

TIPO DE PRUEBA	DESCRIPCIÓN NOTA	NÚM. DE PRUEBA	FECHA	OBSERVACIÓN	RECUPERABLE
CL	CONTROL DE LECTURA	1	Semana 3		NO
CL	CONTROL DE LECTURA	2	Semana 6		NO
TP	TRABAJO PARCIAL	1	Semana 7		NO
EA	EVALUACIÓN PARCIAL	1	Semana 8		SÍ
LB	PRACTICA LABORATORIO	1	Semana 14		NO
PA	PARTICIPACIÓN	1	Semana 15		NO
TF	TRABAJO FINAL	1	Semana 15		NO
EB	EVALUACIÓN FINAL	1	Semana 16		SÍ

IX. BIBLIOGRAFÍA DEL CURSO

https://upc.alma.exlibrisgroup.com/leganto/readinglist/lists/6503209460003391?institute=51UPC_INST&auth=LOCAL