I. INFORMACIÓN GENERAL

CURSO	:	Principios de Seguridad de Información
CÓDIGO	:	SI368
CICLO	:	201801
CUERPO ACADÉMICO	:	**Chinchay Celada, Milton Enrique** **Dávila Ramírez, Juan Ramón**
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

Curso electivo de Principios de Seguridad de Información, en la carrera de Ingeniería de Sistemas de Información, de carácter teórico-práctico dirigido a los estudiantes del octavo ciclo, que busca desarrollar las competencias general de comunicación oral y la especifica de diseñar sistemas, componentes o procesos para encontrar
soluciones en la atención de necesidades teniendo en cuenta restricciones económicas, sociales, políticas, éticas , de salud y seguridad y otras propias del entorno empresarial acorde al ABET Student Outcome (c).

Dada la relevancia e importancia de la aplicación de tecnologías de información (TI) en las organizaciones, se requiere utilizarlas y explotarlas en forma segura a fin de preservar la generación de valor esperada. En este contexto, se requieren profesionales con capacidades en el gobierno y la gestión de la seguridad de las infraestructuras de TI en beneficio de las organizaciones y la sociedad.

IV. LOGRO (S) DEL CURSO

Al finalizar el curso, el estudiante asimila las competencias y habilidades básicas para la gestión del proceso de seguridad de las TI que soportan procesos de negocio en las organizaciones.

V. UNIDADES DE APRENDIZAJE

UNIDAD Nº: 1 Gobierno y gestión de la seguridad de TI
LOGRO Al finalizar la unidad, el estudiante comprende los dominios del gobierno y la gestión de la seguridad en las TI, así como los procesos necesarios para su implementación.

TEMARIO

Gobierno de la seguridad de TI.
Gestión de la seguridad de las TI.
Indicadores y reportes de soporte al gobierno y la gestión de las seguridad d las TI.
Principios de Seguridad de Información.

HORA(S) / SEMANA(S)

6 horas / Semanas 1 y 2

UNIDAD Nº: 2 Estrategias de seguridad de TI

LOGRO

Identificar y comprender los elementos a considerar en la planificación estratégica de la Seguridad de Información.

Además, al finalizar la unidad, el estudiante, a partir de un estudio auto dirigido y guiado remotamente por el profesor, será capaz de alcanzar el PRIMER hito del trabajo final del curso

TEMARIO

Estrategias de seguridad de las TI.
Alineamiento con los objetivos organizacionales.
Roles y responsabilidades de los stakeholders.
Marco normativo.

TEMARIO DE ESTUDIO AUTO DIRIGIDO 1
-Estructuras organizativas para seguridad de información.
-Programas de concientización en seguridad de información.
-Indicadores y métricas en seguridad de información

REFERENCIA DE ESTUDIO AUTO DIRIGIDO
ENTREGABLE DE ESTUDIO AUTO DIRIGIDO
Hito 1: ¿Diseñar un programa de concientización en seguridad de información¿ ¿ Trabajo Parcial del curso

HORA(S) / SEMANA(S)

6 horas / semanas 3 y 4

UNIDAD Nº: 3 Gestión de riesgos

LOGRO

Comprender los procesos de gestión de riesgos y su impacto en la organización.

TEMARIO

TEMARIO DE CLASE
Gobierno y Gestión de Riesgos.
Proceso de Gestión de Riesgos.
Evaluación, respuesta y monitoreo de riesgos.

REFERENCIA DE ESTUDIO AUTO DIRIGIDO
OGC (Office of Government Commerce, UK Government), ITIL Service Operation v3, ITIL Service Management Practices ¿ Risk Management.

HORA(S) / SEMANA(S)
9 horas / semanas 5, 6 y 7

UNIDAD Nº: 4 Desarrollo y gestión del programa de Seguridad de Información

LOGRO
Analizar y comprender el marco de desarrollo y gestión de un programa de Seguridad de Información.

TEMARIO
Desarrollo del plan de Seguridad de Información.
Arquitectura de Seguridad de Información.
Entrenamiento y capacitación en Seguridad de Información.
Programas de concientización.
Estándares, procedimientos y desarrollo de líneas base.
Desarrollo de métricas e indicadores de Seguridad de Información.
Monitoreo, reporte y mejora continua de la Seguridad de Información.
Gestión de incidentes de Seguridad de Información

HORA(S) / SEMANA(S)
21 horas / semanas 9, 10, 11, 12, 13, 14 y 15

VI. METODOLOGÍA

El curso combina la entrega de contenidos teóricos y la utilización de modelos, estándares, plantillas, indicadores y reportes prácticos que brindan un contexto completo del manejo de las competencias y habilidades requeridas para gestionar la seguridad de la información para las organizaciones.

VII. EVALUACIÓN

FÓRMULA

10% (CL1) + 15% (CL2) + 20% (EA1) + 15% (CL3) + 5% (PA1) + 15% (TF1) + 20% (EB1)

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

VIII. CRONOGRAMA

TIPO DE PRUEBA	DESCRIPCIÓN NOTA	NÚM. DE PRUEBA	FECHA	OBSERVACIÓN	RECUPERABLE
CL	CONTROL DE LECTURA	1	Semana 3	individual	NO
CL	CONTROL DE LECTURA	2	Semana 7	individual	NO
EA	EVALUACIÓN PARCIAL	1	Semana 8	individual	SÍ
CL	CONTROL DE LECTURA	3	Semana 13	individual	NO
PA	PARTICIPACIÓN	1	Semana 15	individual	NO
TF	TRABAJO FINAL	1	Semana 15	grupal	NO
EB	EVALUACIÓN FINAL	1	Semana 16	individual	SÍ

IX. BIBLIOGRAFÍA DEL CURSO

BÁSICA

UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS, Centro De Información Catálogo en línea: http://bit.ly/2D16ne6.

RECOMENDADA

(No necesariamente disponible en el Centro de Información)

EUROPEAN COMISSION (2014) Cybersecurity Strategy of the European Union.,

GLOBAL THREAT, Intelligence Report (2014) NTT Group,