Información General del curso

Nombre del curso	PRINCIPIOS DE CIBERSEGURIDAD
Código del curso	CLV-048
Duración	20 horas

Descripción del curso

Este curso brinda el conocimiento necesario para que los estudiantes conozcan los principios y fundamentos entorno a la temática de la seguridad en las tecnologías de información, los introduce al conocimiento sobre la teoría y habilidades relacionadas en un mundo globalizado donde el valor de la información y el aseguramiento de esta es el activo intangible más importante para las organizaciones actuales.

Como futuros profesionales, indistintamente del área, es importante conocer el entorno de las tecnologías como un todo, en el sentido de cómo nos ayudan en nuestro diario hacer y que tan importante es la seguridad de los sistemas, equipos y datos generados desde ellos.

El curso tiene una naturaleza virtual utilizando los altos estándares establecidos por la universidad apoyados en las diferentes herramientas para una adecuada ejecución, comprensión y análisis de los diferentes tópicos entre ellos: la comprensión de los conceptos sobre ciberseguridad, estándares y regulaciones sobre TI, tecnologías de ataques utilizados sobre los sistemas y el descubrimiento de los rastros forenses. Además el curso ofrece la posibilidad de analizar el contexto nacional e internacional sobre las diferentes regulaciones, procesos y procedimientos a seguir en los temas antes mencionados, enriqueciendo el contenido con diferentes actividades a ejecutar por parte de los estudiantes.

Objetivos generales y específicos

Objetivo General

Brindar al estudiante los conceptos, fundamentos y procedimientos necesarios para la comprensión de la temática global de seguridad sobre las tecnologías de información a través de la plataforma virtual ofrecida por la universidad.

Objetivos específicos

- Comprender los conceptos sobre ciberseguridad.
- Identificar los estándares y regulaciones entorno a la seguridad de la tecnologías e información.
- Conocer sobre las tecnologías de ataque utilizadas sobre los sistemas tecnológicos
- Entender los procesos de descubrimiento de huellas forenses tecnológicas.

Contenidos

- Conceptos sobre Ciberseguridad
- Definición de estándares y regulaciones sobre seguridad en TI
- Tecnologías de ataque a los sistemas - hacking ético
- Procedimientos para descubrir la huella del intruso - informática forense

Metodología

El curso se desarrolla con una metodología virtual, donde los estudiantes analizan y desarrollan su aprendizaje a su propio ritmo, por medio de los videos y los recursos digitales disponibles, mientras que el 70% de su tiempo se dedica a realizar actividades prácticas, lo que los lleva a una comprensión más profunda de los contenidos, mediante una metodología de aprendizaje basada en proyectos ABP-STEM, la cual supone una manera concreta de aprender críticamente tomando elementos y problemas del contexto.

Esta experiencia de aprendizaje constituye un modelo de instrucción auténtico en el que los estudiantes planean, implementan y evalúan proyectos que tienen aplicación en el mundo real más allá del aula de clase. En ella se recomiendan actividades interdisciplinarias, de largo plazo y centradas en el estudiante, en lugar de lecciones cortas y aisladas, más importante aún, los estudiantes encuentran los proyectos divertidos, motivadores y

retadores, porque desempeñan en ellos un papel activo tanto en su escogencia como en todo el proceso de concepción, diseño, implementación y operación.

Estrategias de aprendizaje

El profesor escogerá los recursos que utilizará para la mediación pedagógica en el curso. Puede utilizar varios y/o todos los recursos que la plataforma Moodle tiene a su disposición, así como otros recursos que el profesor decida a conveniencia del curso. A continuación, se mencionan algunos:

- Foros: espacios de discusión donde los participantes pueden compartir sobre una temática o comunicarse y aclarar consultas. Esta herramienta propicia el debate, genera discusiones para desarrollar habilidades de argumentación.
- Videos explicativos: son animaciones que cuentan de forma fácil y breve una idea, un producto o un servicio, transformando un mensaje complicado en un discurso entendible para todos.
- Cuestionarios: se utiliza para realizar evaluaciones iniciales, exámenes tipo test, pruebas de nivel

Evaluación

El curso se aprueba con una nota mínima de 70 puntos y se le hará entrega de un certificado emitido por la Universidad al finalizar el curso.

Para este curso el estudiante debe completar las actividades asignadas cada semana correspondientes a la visualización y comprensión de los videos explicativos como material didáctico que fundamentan las bases y posterior completar la actividad evaluativa correspondiente, donde se pretende abrir espacios para un sano debate de algún tema en particular así como la comprensión de definiciones a través de cuestionarios o pruebas cortas, los porcentajes de evaluación para las actividades se desglosan a continuación:

Foros (2 de 10% cada uno)	20%
Cuestionario (2 de 45% cada uno)	80%

Rúbricas

La siguiente información presenta los criterios o rúbricas para la evaluación de los foros, donde en general se pretende que los aportes sean de valor bajo un lenguaje respetuoso sobre las diferentes opiniones, sustentando los conocimientos adquiridos por la explicación a través de los videos o con fuentes adicionales a las suministradas respetando los derechos de autor y copyright.

	Criterios	5	4	3	2	1
1	Los aportes al foro se hacen a tiempo y contienen una discusión completa y relevante para el tema					
2	Las ideas desarrolladas están completas. No se observan errores de gramática u ortografía					
3	Se citan correctamente referencias relevantes. Incorpora aprendizajes previos en la discusión.					
4	Ofrece recursos relacionados con el tema que no se encuentran en las lecturas asignadas o en los textos guía del curso					
5	El aporte demuestra una reflexión seria y combina múltiples ideas relacionadas con el tema.					
Total	**El puntaje se calcula sobre 25 puntos. Ningún trabajo se aprueba con valoraciones de 1 en cualquiera de los criterios.**					

Recursos

Se cuenta con diversos medios tecnológicos para fomentar el aprendizaje según las estrategias de enseñanza que se puedan utilizar.

Se tienen plataformas virtuales propias (Campus Virtual de la Universidad) y de terceros (EBSCO, youtube, y facebook) para fomentar el aprendizaje según las estrategias de enseñanza. Las plataformas virtuales proveen de herramientas importantes como lo son foros, wikis, videos, portafolios y chats, para fomentar presentaciones y medios modernos de comunicación de la información. Particularmente en el curso se tiene acceso a:

- Campus Virtual de la Universidad
- EBSCO
- E-Libro

- Equipos colocados en la Nube con diferentes programas para la realización de ejercicios prácticos. Los mismos estarán debidamente seleccionados e identificados en el campus virtual de la Universidad Fidélitas en la sección de avisos generales.

Cada estudiante de Fidélitas tiene acceso a la licencia de Office 365 donde pueden descargar Office, Stream.

Bibliografía

- Engebretson, P. (2013), The Basics of Hacking and Penetration Testing, Second Edition: Ethical Hacking and Penetration Testing Made Easy. (2da Ed.) Syngress
- Koop, E (2011). Business Continuity Plan (BCP) Template With Instructions and Example. (2da Ed.) EK Publications.
- Calder, A., y Watkins, S. (2012). IT Governance: An International Guide to Data Security and ISO27001/27002 (5ta Ed.). Kogan Page Limited
- Nelson, B., Phillips, A., & Steuart, C. (2010). Guide to Computer Forensics and Investigations. Boston: Cengage Learning.

Cronograma

Semana	Contenidos	Actividades de Evaluación / Entregable
1	• Conceptos sobre Ciberseguridad ○ Generalidades de la seguridad informatica ○ El valor de la informacion ○ Definicion y tipos de seguridad informática ○ Objetivos de la seguridad informática ○ Gestion y evaluacion del riesgo	**Cuestionario 1 Conceptos Básicos**
2	• Estandares y regulaciones sobre seguridad en TI ○ ISO27001 ○ COBIT ○ ITIL ○ Entes éticos reguladores ○ Ley en CR	**Foro 1 Discusión sobre un caso ético y aplicación de la legislación de Costa Rica**
3	• Tecnologias de ataque a los sistemas - Hacking Etico ○ Amenazas a la seguridad ○ Que es el Hacking Etico ○ Quien es el Ethical Hacker	**Cuestionario 2 Conceptos sobre Hacking Ético.**

	○ Fases de ejecucion y herramientas de penetracion ○ Ejemplos de informe	
4	• Descubrir la huella del intruso - informática forense ○ Importancia ○ Problema ○ Solución ○ Que es Informática Forense? ○ Fosensia en Redes ○ Forensia Digital ○ Objetivos ○ Usos ○ Procesos ○ Herramientas ○ Casos ○ Video	**Foro 2 Discusión sobre caso donde se aplicó la informática forense y sus resultados.**