DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

<table>
<tr><td colspan="2"></td><td colspan="3">PROGRAMA</td></tr>
<tr><td colspan="2"></td><td>Código
en SIPE</td><td colspan="2">Descripción en SIPE</td></tr>
<tr><td colspan="2">TIPO DE CURSO</td><td>028</td><td colspan="2">Tecnólogo</td></tr>
<tr><td colspan="2">PLAN</td><td colspan="3">2023</td></tr>
<tr><td colspan="2">ORIENTACIÓN</td><td>88F</td><td colspan="2">Ciberseguridad</td></tr>
<tr><td colspan="2">MODALIDAD</td><td colspan="3">Presencial</td></tr>
<tr><td colspan="2">AÑO</td><td colspan="3">1</td></tr>
<tr><td colspan="2">SEMESTRE/ MÓDULO</td><td colspan="3">1</td></tr>
<tr><td colspan="2">ASIGNATURA</td><td></td><td colspan="2">Taller de Introducción a la Seguridad Informática</td></tr>
<tr><td colspan="2">CRÉDITO EDUCATIVO</td><td colspan="3">6</td></tr>
<tr><td colspan="2">DURACIÓN DEL CURSO</td><td>Horas totales:
64</td><td>Horas semanales:
4</td><td>Cantidad de semanas:
16</td></tr>
<tr><td>Fecha de Presentación:
6/3/2023</td><td>Nº Resolución de la DGETP</td><td>Exp. Nº</td><td>Res. Nº</td><td>Acta Nº</td><td>Fecha __/__/____</td></tr>
</table>

Objetivos:

Este curso se concibe como una aproximación inicial a la seguridad informática, para que los estudiantes que comienzan la carrera adquieran conceptos fundamentales de la ciberseguridad, reconozcan las características principales de esta disciplina y experimenten métodos y herramientas para la resolución de problemas concretos.

Saberes estructurantes de la unidad curricular:

1. Fundamentos de la Seguridad Informática:
    a) Motivación.
    b) Definiciones (confidencialidad, integridad y disponibilidad).
    c) Algunos tipos de ataques comunes y mecanismos de protección.
    d) Introducción a la privacidad y protección de datos personales.

2. Talleres:
    Ejes temáticos:
    a) Conceptos básicos de criptografía, motivación, definiciones y algunas herramientas.
    b) Manejo elemental de consola y comandos básicos, scripting.
    c) Programación web básica (HTML, CSS, javascript)
    d) Uso básico de algunas herramientas de seguridad (nmap, tcpdump, ettercap, netcat, curl/wget, john the ripper, zap, etc).

Sugerencias metodológicas:

El curso cubre los fundamentos y propiedades básicas de seguridad informática (como confidencialidad, integridad y disponibilidad), y los principales tipos de ataques de los que puede ser objeto un sistema informático, así como los posibles métodos de protección, detección y políticas de seguridad que permitan evitar el daño al sistema o minimizar sus consecuencias. Complementando el contenido teórico, se brindarán una serie de talleres durante los cuales los estudiantes realizarán actividades en equipo que ilustren y permitan experimentar técnicas y herramientas de ciberseguridad concretas. Estos talleres tendrán una metodología de enseñanza activa y con sesgo lúdico. Se pueden realizar actividades

competitivas, como capturas de bandera en escenarios sencillos, en donde los propios equipos pueden esconder cierta bandera en un ambiente, y a la vez descubrir la de otros grupos, lo que permite desempeñar roles tanto ofensivos como defensivos. El objetivo principal de este taller es motivar a los estudiantes en el estudio de la ciberseguridad, por lo que se recomienda que las actividades de taller (y por lo tanto los temas que se aborden en esta segunda parte del curso) sean elegidas contemplando en la medida de lo posible los intereses de los estudiantes.

Bibliografía

Básica

W. Stallings, L. Brown; Computer Security: Principles and Practice, Pearson, 4th Edition, (2018).

Complementaria

Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy), AGESIC; Materiales Didácticos (videos, afiches, juegos y otras actividades) de la campaña “Seguro te conectás”; https://www. gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/ ciudadania.