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" rowspan="2">2</td></tr>
<tr><td colspan="2">SEMESTRE/ MÓDULO</td></tr>
<tr><td colspan="2">UNIDAD CURRICULAR</td><td colspan="3">Criptografía aplicada</td></tr>
<tr><td colspan="2">CRÉDITO EDUCATIVO</td><td colspan="3">13</td></tr>
<tr><td colspan="2">DURACIÓN DEL CURSO</td><td>Horas totales:
128</td><td>Horas semanales:
8</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:

El objetivo de esta unidad curricular es que el estudiante conozca los fundamentos matemáticos de la criptografía, las principales primitivas criptográficas, identifique conceptos y propiedades fundamentales de la criptografía aplicada así como algunas malas prácticas que las hacen vulnerables en el uso.

Resultados de aprendizaje:

- Explica el funcionamiento básico de los algoritmos de cifrado de bloques simétricos.
- Compara y contrasta el cifrado de bloques y el cifrado de secuencias.
- Discute el uso de funciones hash seguras para la autenticación de mensajes.
- Lista otras aplicaciones de funciones hash seguras.
- Explica el funcionamiento básico de los algoritmos de cifrado de bloques asimétricos.
- Presenta una descripción general del mecanismo de firma digital y explica el concepto de sobres digitales.
- Explica la importancia de los números aleatorios y pseudoaleatorios en criptografía.

Saberes estructurantes de la unidad curricular:

1. Confidencialidad con cifrado simétrico:
a) Cifrado simétrico.
b) Algoritmos de cifrado de bloques simétricos.
c) Cifrados de flujo.

2. Autenticación de mensajes y funciones hash:
a) Autenticación mediante cifrado simétrico.
b) Autenticación de mensajes sin cifrado de mensajes.
c) Funciones hash seguras.
d) Otras aplicaciones de las funciones hash.

3. Cifrado de clave pública:
a) Estructura de cifrado de clave pública.
b) Aplicaciones para criptosistemas de clave pública.
c) Requisitos para criptografía de clave pública.

d) Algoritmos de cifrado asimétrico.

4. Firmas digitales y gestión de claves:

a) Firma digital.

b) Certificados de clave pública.

c) Intercambio de claves simétricas utilizando cifrado de clave pública.

d) Sobres digitales.

5. Números aleatorios y seudoaleatorios:

a) El uso de números aleatorios.

b) Aleatorio versus pseudoaleatorio.

Bibliografía

Básica

W. Stallings; Criptography and Network Security, Prentice Hall, (2006).

Complementaria

1. W. Stallings, L. Brown; Computer Security: Principles and Practice, Pearson, 4th Edition, (2018). 2. R. Anderson; Security Engineering: A Guide to Building Dependable Distributed Systems, Ed. Wiley, 3rd. Edition, (2020).