DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		1			
SEMESTRE/ MÓDULO		2			
UNIDAD CURRICULAR			Sistemas Operativos		
CRÉDITO EDUCATIVO		8			
DURACIÓN DEL CURSO		Horas totales: 80	Horas semanales: 5		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	Nº Resolución de la DGETP	Exp. Nº	Res. Nº	Acta Nº	Fecha __/__/____

Objetivos:

El objetivo de este curso es introducir conceptos fundamentales de seguridad en Sistemas Operativos. Se presentan tanto amenazas específicas y tipos de ataque como mecanismos de identificación y autenticación. Se pone particular énfasis en la gestión de contraseñas y en la implementación de los mecanismos de control de acceso y de auditoría provistos por los sistemas operativos. Se presenta el concepto de computación confiable y de seguridad multinivel.

Resultados de aprendizajes:

- Discute los cuatro métodos generales para autenticar la identidad de un usuario.
- Explica el mecanismo mediante el cual se utilizan contraseñas hash para la autenticación de usuarios.
- Presenta una descripción general de la autenticación de usuarios basada en tokens.
- Explica cómo se ubica el control de acceso en el contexto más amplio que incluye autenticación, autorización y auditoría.
- Distingue entre sujetos, objetos y derechos de acceso.
- Discute los conceptos principales del control de acceso basado en roles y el basado en atributos. Enumerar los pasos necesarios en el proceso de aseguramiento de un sistema.
- Enumera los pasos básicos utilizados para asegurar el sistema operativo base.
- Explica algunos aspectos específicos de la seguridad de los sistemas Unix/Linux.
- Explica algunos aspectos específicos de la seguridad de los sistemas Windows.
- Enumera los pasos necesarios para mantener la seguridad en los sistemas virtualizados.
- Explica el modelo Bell-LaPadula y su relevancia para la computación confiable.
- Resume otros modelos formales de seguridad informática.
- Comprende el concepto de sistemas confiables.
- Enumera y explica las propiedades de un monitor de referencia y las relaciones entre un monitor de referencia y una base de datos del kernel de seguridad.
- Logra presentar una descripción general de la aplicación de la seguridad multinivel al control de acceso basado en funciones.

Saberes estructurantes de la unidad curricular:

1. Autenticación:
    a) Principios de autenticación de usuario.
    b) Autenticación de usuarios basada en secretos y en tokens.
    c) Mecanismos biométricos.
    d) Autenticación remota.
2. Control de acceso:
    a) Principios de control de acceso.
    b) Sujetos, objetos y permisos.
    c) Control de acceso discrecional (DAC).
    d) Control de acceso basado en roles (RBAC).
    e) Control de acceso basado en atributos (ABAC).
    f) Gestión de identidades, credenciales y de acceso.

3. Seguridad de Sistemas Operativos:
    a) Planificación de la seguridad de SO y Hardening.
    b) Mantenimiento: Logging y Backup.
    c) Seguridad Linux/Unix.
    d) Seguridad Windows.
    e) Seguridad de sistemas de virtualización.

4. Computación confiable y Seguridad Multinivel:
    a) El modelo Bell-LaPadula para seguridad computacional.
    b) Otros modelos.
    c) El concepto de modelo confiable.
    d) Aplicaciones de seguridad multinivel.

Bibliografía

Básica

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

Complementaria

Gollman, Dieter (2009), Computer Security, Wiley Computing Publishing, 3rd. Editon. J.6.