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		2			
SEMESTRE/ MÓDULO		4			
ASIGNATURA		Gestión de la Seguridad de la Información			
CRÉDITO EDUCATIVO		13			
DURACIÓN DEL CURSO		Horas totales: 128	Horas semanales: 8		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	Nº Resolución de la DGETP	Exp. Nº	Res. Nº	Acta Nº	Fecha __/__/____

Objetivos:

Introducir a los estudiantes en los principales conceptos y metodologías asociadas a la gestión de la ciberseguridad, contemplando el marco normativo internacional y nacional existente. Llevar a la práctica una metodología de rápida aplicación para la implementación de un Sistema de Gestión de Seguridad de la Información. Presentar metodologías y buenas prácticas concretas para la gestión de riesgos, gestión de incidentes, gestión de la continuidad de la seguridad y gestión de vulnerabilidades. Se abarcarán las principales conceptos entorno a la familia de normas ISO/IEC 27000 y el marco de ciberseguridad de NIST.

Saberes estructurantes de la unidad curricular:

1. Introducción:
    a) Definiciones y conceptos de gestión de ciberseguridad.
    b) Confidencialidad, Integridad y Disponibilidad.
    c) Marco normativo nacional e internacional.
2. Sistema de Gestión de Seguridad de la Información:
    a) Metodologías de implantación.
    b) Principales desafíos a enfrentar.
    c) Herramientas disponibles que faciliten la implantación.
3. Gestión de Riesgos:
    a) Introducción al proceso de gestión de riesgos.
    b) Metodologías de análisis de riesgo.
    c) Tratamiento de riesgos.
4. Gestión de incidentes:
    a) Definición de incidentes.
    b) Procesos de clasificación, análisis, tratamiento, resolución y cierre.
    c) Control de flujos de información y procesos.
    d) Modelos organizacionales de Centros de Respuesta y Centros Operativos de Seguridad
5. Gestión de la continuidad operativa:
    a) Componentes del negocio.
    b) Tipos de desastres que deben considerarse.c
    c) Análisis de Impacto del Negocio.
    d) Desarrollo de estrategias de mitigación.

Bibliografía:

H. Tipton, M. Krause, Information Security Management Handbook 6th, 2008.

Thomas Peltier, Information Security Policies, Procedures and Standards, 2002.

L. Hayden, IT Security Metrics. A Practical Framework for Measuring Security and Protecting Data, 2010.

Proyecto AMPARO, Manual básico de Gestión de Incidentes de Seguridad Informática, 2012.

Susan Snedaker, Business Continuity and Disaster Recovery for IT professionals, 2007.

Complementaria:

NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018.

AGESIC, Marco de Ciberseguridad, 2019.

H. Allen et al, Structuring the Chief Information Security Officer Organization, CERT Division, Software Engineering Institute, Carnegie Mellon University.

C. Zimmerman, Ten Strategies of a World-Class Cybersecurity Operations Center, MITRE Corporation.