MATERIA
Optativa IV

CIBERSEGURIDAD APLICADA A LAS TECNOLOGÍAS DE INFORMACIÓN

Nivel de formación	Maestría en Tecnologías de Información				
Área de formación	Optativa abierta	**Orientación**	Gestión estratégica de Tecnologías de Información y Diseño e Implantación de Tecnologías de Información		
Modalidad	Presencial	**Carga horaria**	**48** hrs.	**Créditos**	7

Objetivo General

El estudiante desarrollará los conocimientos, las habilidades y destrezas en materia de Ciberseguridad con la finalidad de entender escenarios reales y como prevenir y blindar de ataques a las organizaciones. Podrá evaluar la seguridad de los sistemas de tecnologías de información establecidos para conocer su situación de riesgo y vulnerabilidad.

Objetivo Particular

Este curso tiene como objetivo particular el brindar al estudiante los conocimientos básicos en materia de ciberseguridad focalizada en las tecnologías de información, las diferentes técnicas que auxilien a las organizaciones y a las direcciones de tecnologías de información en el uso adecuado de las diferentes herramientas que existen para este fin.

Competencia y sub-competencia a desarrollar

Competencia genérica

Desarrollar habilidades para analizar las vulnerabilidades y escenarios en materia de ciberseguridad a las organizaciones y desarrollar un plan de trabajo

que proteja y mitigue el riesgo para llevar una la gestión de la información de los centros de datos de las organizaciones.

Sub-competencia genérica

- Definir Analice e integre el estatus de los insumos de información de las organizaciones en materia de ciberseguridad
- Ejecutar auditorias de ciberseguridad y lleve a cabo un análisis forense de seguridad de la información
- Diseñe un plan de acción en materia de ciberseguridad para los centros de datos de las organizaciones

Producto esperado del curso

- Diseñe y ejecute un plan de ciberseguridad conforme a los estándares de la industria.

Campo de aplicación profesional

Definir los campos profesionales en los cuales aplica el contenido de la unidad de aprendizaje

Logros esperados	
Conocimientos	El estudiante entenderá el concepto ciberseguridad en un entorno de las tecnologías de información las arquitecturas de seguridad, estándares de la industria en esta materia. El estudiante aprenderá a implementará soluciones de ciberseguridad en entornos de centros de datos
Habilidades	Trabajo colaborativo, respeto, inclusión y adaptación de ideas
Actitudes	Adaptabilidad, trabajo de equipo, versatilidad, liderazgo
Valores	Honestidad, prudencia, ética, respeto y responsabilidad

CONTENIDO

Módulo / Unidad	Contenido	Producto o resultado esperado
Módulo I. Introducción a la Ciberseguridad	1. Importancia de la ciberseguridad 2. Introducción a los ciberataques 3. Objetivos de Ciberataques a. Confidencialidad b. Disponibilidad c. Integridad	Identificar escenarios de infraestructura e insumos de información a proteger
Módulo II. Tipos de Ciberataques	1. Negación del servicio (DoS) 2. Negación del servicio distribuido (DDoS) 3. Ataques Man-in-the-Middle (MITM) 4. Inyección SQL 5. Ciberterrorismo 6. Phishing 7. Ciber Fraudes	Escenarios e implementación de laboratorios y casos de uso
Módulo III. Tipos de Malware Computacional	1. Virus 2. Trojan Horse 3. Rootkit 4. Spyware 5. Worms 6. Adware 7. Browser Hijacker	Escenarios e implementación de laboratorios y casos de uso
Módulo IV. Seguridad Computacional	1. Firewalls 2. Antivirus Software 3. Anti-Spyware Software 4. Anti-Spam Software 5. Security Updates 6. Secure Browsing Settings 7. Scan Devices before data transfer 8. Social Enginnering Attack Percautions 9. Password Management	Escenarios e implementación de laboratorios y casos de uso
Módulo V. Prevención de Ciberataques	1. Algoritmos y técnicas a. Detección de ciberataques b. Predicción de ciberataques c. Prevención de ciberataques 2. Firewalls a. Windows 10 Firewalls b. MacOS Firewalls c. iOS, Android Firewalls d. Monitoreo de trafico e. Análisis de trafico f. Sistemas de Detección y prevención de	Escenarios e implementación de laboratorios y casos de uso

Módulo / Unidad	Contenido	Producto o resultado esperado
	intrusos g. Sistemas de detección de intrusos (IDS) h. Sistemas de Prevención de intrusos (IPS) i. Autenticación mediante Hash j. Autenticación Multi-factor k. Sockets Seguros SSL l. Redes Virtuales Privadas	
Módulo VI. Seguridad de Redes Inalámbricas y computo móvil	1. Vulnerabilidades LAN 2. Vulnerabilidades Inalámbricas WAN 3. Vulnerabilidades IoT 4. HTTPS 5. Certificados de Seguridad 6. Encriptación SSL 7. Sistemas de Detección de fraudes WEB 8. Administración y actualización del navegador cache 9. Análisis de espectros inalámbricos WLAN 10. Importancia de la seguridad móvil	Escenarios e implementación de laboratorios y casos de uso
Módulo VII Estándares de Ciberseguridad y la nube computacional	1. Estándares ISO/IEC 27001 & 27002 2. Estándar Fórum de Seguridad de la Información (ISF) 3. Norma Británica BSI-7799 4. Framework de Ciberseguridad del NIST 5. Certificación de Hackeo Ético (CEH)	Diseño de una política básica de ciberseguridad

BIBLIOGRAFÍA

Libros:

- CEH V11 Certified Ethical Hacker, Sybex-Wiley, ISBN: 9781119800309, 2021
- Cybersecurity: The Beginner´s Guide, Packt, Dr Erdal Ozkaya, ISBN: 9781789616194, 2019.
- Cybersecurity Threats, Malware Trends, and Strategies - Second Edition, Packt, Tim Rains, ISBN: 9781804613672, 2023
- Cybersecurity – Attack and Defense Strategies - Third Edition, Packt, Yuri Diogenes, ISBN: 9781803248776, 2022.
- ISO/IEC 27001 & 27002
- Norma Británica BSI-7799
- Framework de Ciberseguridad del NIST

Artículos: IEEE, ACM y Springer.

Criterios de Evaluación	Porcentaje / Puntaje
Actividades Semanales de Investigación entregables en formato PDF en Plataforma Classroom	30 %
Casos de Uso Prácticos Semanales, entregables en formato PDF en plataforma Classroom	30 %
Proyecto Integrador y Articulo de Revisión final	40 %
Total	100 %

Elaboró y actualizó el programa: **Dr. José Antonio Orizaga Trejo**
Última Revisión, actualización: **2 de diciembre del 2022**

Aprobación de la Junta Académica
Programa de la Maestría en Tecnologías de Información

Revisores:	**Firma:**
Dr. José Antonio Orizaga Trejo Presidente de la Junta Académica	
Dr. Sergio Roberto Dávalos García Secretario	
Dr. Víctor Manuel Larios Rosillo Consejero	
Dr. Cuauhtémoc López Martín Consejero	
Dra. María Elena Meda Campaña Consejero	
Mtro. Alejandro López Rodríguez Consejero	