LICENCIATURA EN

CIBERSEGURIDAD

CUGDL

CENTRO UNIVERSITARIO DE GUADALAJARA

LICENCIATURA EN

CIBERSEGURIDAD

En la era digital contemporánea, la ciberseguridad se ha convertido en una de las principales preocupaciones para gobiernos,industrias y organizaciones académicas. Con el advenimiento de tecnologías avanzadas, especialmente la inteligencia artificial (IA), los riesgos asociados con la seguridad de la información han crecido exponencialmente.

La IA presenta oportunidades y desafíos para la ciberseguridad. Mientras la IA puede mejorar la seguridad a través de la detección automática de amenazas y la respuesta en tiempo real, los ciberdelincuentes también pueden utilizar la misma IA para mejorar la eficacia de sus ataques. Además, con la creciente adopción de servicios en la nube, se están generando vastas cantidades de datos,creando a su vez nuevos vectores de ataque.

Es por ello, que esta preocupación ha incitado que las Instituciones Educativas innoven en su oferta educativa para su atención.

OBJETIVO GENERAL

Formar profesionales altamente cualificados en el ámbito de la seguridad de la información, capaces de identificar, abordar y solucionar problemas globales en este campo. Este programa tiene como meta dotar que los estudiantes desarrollen competencias avanzadas en auditoría, gestión de seguridad de la información,técnicas de hackeo ético y protección de datos. Asimismo, se promoverá la aplicación de la inteligencia artificial en el ámbito de la ciber seguridad para anticipar y mitigar riesgos, equipando a los estudiantes con las habilidades necesarias para diseñar, implementar y gestionar sistemas de seguridad robustos y eficaces.

Objetivos específicos

» Capacitar a los estudiantes para analizar problemas de seguridad de la información de manera crítica e identificar vulnerabilidades en sistemas de información y redes, utilizando métodos y herramientas de hackeo ético y proponer medidas correctivas.

»Formar a los estudiantes en técnicas de investigación forense digital para recopilar, preservar y analizar evidencia digital de actividades maliciosas o incidentes de seguridad, siguiendo procedimientos legales y éticos.

» Enseñar a los estudiantes los principios y estándares de protección de datos, incluyendo la regulación GDPR y otras leyes de privacidad aplicables, y cómo aplicarlos en el diseño, implementación y gestión de sistemas de información seguros.

» Fomentar la conciencia sobre la importancia de la privacidad de los usuarios y la información personal, e integrar consideraciones de privacidad desde el diseño en todos los aspectos de la ciberseguridad y el desarrollo de software.

» Fomentar la innovación y la creatividad en la protección de datos a través del diseño e implementación de soluciones innovadoras y creativas para proteger los datos y mitigar los riesgos de seguridad, adaptándose a las nuevas amenazas y desafíos en un entorno tecnológico en constante evolución.

PERFIL DEL ESTUDIANTE

» Comprensión sólida de las matemáticas, especialmente en álgebra, cálculo y estadísticas.

» Conocimientos básicos de informática, incluyendo comprensión de sistemas operativos, software de oficina y programación básica.

» Habilidades de investigación y capacidad para analizar y sintetizar información de diversas fuentes.

» Familiaridad con conceptos de redes y sistemas de comunicación.

» Comprensión básica de los principios de programación y desarrollo de software.

» Capacidad para comunicarse efectivamente de forma verbal y escrita.

» Capacidad para trabajar de manera colaborativa.

» Habilidades para la autogestión y el aprendizaje auto dirigido.

» Interés en la ciberseguridad y la tecnología de la información.

» Compromiso con la ética profesional y la responsabilidad social, especialmente en relación con la privacidad y seguridad de la información.

PERFIL DEL EGRESADO

La Licenciatura en Ciberseguridad, contempla un conjunto de competencias, habilidades blandas y conocimientos, que lo calificarán para una variedad de roles en el campo profesional, tales como:

» Serán profesionales altamente capacitados y comprometidos con la protección de la información y los sistemas digitales.

» Dominarán las técnicas y herramientas necesarias para proteger activos digitales, identificar vulnerabilidades y responder eficazmente a incidentes de seguridad.

» Enfrentarán los desafíos emergentes en el ámbito de la ciberseguridad y estarán capacitados para aplicar principios éticos en todas sus actividades.

» Analizarán y abordarán los problemas de seguridad cibernética en un contexto global, considerando las implicaciones políticas, económicas y sociales de las amenazas cibernéticas y diseñando estrategias adaptativas para mitigar riesgos.

» Desarrollarán conocimientos especializados en técnicas de hackeo ético.

» Estarán comprometidos con la protección de datos y la privacidad, aplicando principios éticos en todas sus actividades relacionadas con la ciberseguridad.

CAMPO PROFESIONAL

» Consultor y asesor de organizaciones sobre cómo mejorar sus posturas de seguridad, realizar evaluaciones de riesgos y desarrollar estrategias de seguridad.

» Como especialistas en hackeo ético, los licenciados en ciberseguridad pueden desempeñarse como Licenciado de Pruebas de Penetración, para realizar pruebas éticas para identificar y corregir vulnerabilidades en sistemas y aplicaciones, así como diseñar arquitecturas de seguridad para garantizar que los sistemas estén protegidos desde su concepción, como Analista de Inteligencia de Amenazas.

» En la figura de Ingeniero Forense Digital en las organizaciones, los licenciados en ciberseguridad serán capaces de investigar incidentes de seguridad, recuperar y analizar evidencia digital para entender la naturaleza y el alcance de un ataque, y podrán ser responsables de supervisar y coordinar las estrategias de seguridad de toda la organización, asegurándose de que las políticas y controles estén alineados con los objetivos comerciales, etc.

LICENCIATURA EN

CIBERSEGURIDAD

S1	PENSAMIENTO CRÍTICO	INNOVACIÓN TECNOLÓGICA	INTELIGENCIA COLECTIVA	MATEMÁTICAS I	ALGEBRA LINEAL	ANÁLISIS DE PROBLEMAS GLOBALES DE SIGLO XXI	INTRODUCCIÓN A LA CIENCIA DE DATOS
S2	PROGRAMACIÓN I	STORYTELLING	GESTIÓN SOCIOEMOCIONAL O COGNITIVA	ÉTICA Y RESPONSABILIDAD SOCIAL	GESTIÓN DE PROYECTOS	PROBABILIDAD Y ESTADÍSTICA	MATEMÁTICAS II
S3	PROGRAMACIÓN II	HACKIN ÉTICO (FUNDAMENTOS)	SISTEMAS OPERATIVOS DISTRIBUIDOS	FUNDAMENTOS DE REDES Y TELE-COMUNICACIONES	GESTIÓN DE RIESGOS Y RECUPERACIÓN DE DESASTRES	LA NUBE COMPU-TACIONAL Y LA CIBERSEGURIDAD	ARQUITECTURA DE SISTEMAS DE SEGURIDAD
S4	PRIVACIDAD Y PROTECCIÓN DE TDATOS	ANÁLISIS Y VISUA-LIZACIÓN DE DATOS PARA CIBERSEGURIDAD	ORIENTACIÓN A-1	ORIENTACIÓN A-2	ORIENTACIÓN B-1	ORIENTACIÓN B-2	MICROCREDENCIAL 1
S5	INVESTIGACIÓN Y ANÁLISIS FORENSE DIGITAL	CRIPTOGRAFÍA Y SEGURIDAD DE LA INFORMACIÓN	ORIENTACIÓN A-3	ORIENTACIÓN A-4	ORIENTACIÓN B-3	ORIENTACIÓN B-4	MICROCREDENCIAL 3
S6	PRÁCTICAS PROFESIONALES	PROYECTO INTEGRADOR	ORIENTACIÓN A-5	ORIENTACIÓN B-5	MICROCREDENCIAL 3	DISEÑO Y ANÁLISIS DE ALGORITMOS SEGUROS	BASES DE DATOS

ORIENTACIÓN A Y B / PUEDES ELEGIR 2 DE LAS SIGUIENTES ORIENTACIONES

INTELIGENCIA APLICADA A LA CIBERSEGURIDAD / INTELIGENCIA ARTIFICIAL EN CIBERSEGURIDAD **/** MACHIE Y DEEP LEARNNG PARA CIBERSEGURIDAD **/** NPL EN CIBERSEGURIDAD **/** SEGURIDAD EN IOT (INTERNET DE LAS COSAS) **/** CHATGPT EN CIBERSEGURIDAD

AUDITORÍA Y GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN / TÓPICOS AVANZADOS EN PRIVACIDAD DE DATOS **/** DESARROLLO E IMPLEMENTACIÓN DE POLÍTICAS DE CIBERSEGURIDAD **/** RESPUESTA A INCIDENTES Y ANÁLISIS DE AMENAZAS **/** CONTROLES Y ASEGURAMIENTO EN CIBERSEGURIDAD **/** ESTÁNDARES Y NORMATIVIDAD NACIONAL E INTERNACIONAL A INCIDENTES DE CIBERSEGURIDAD

HACKEO ÉTICO Y PROTECCIÓN DE LOS DATOS / HACKING ÉTICO Y RESPUESTA A INCIDENTES **/** SIMULACIÓN Y MODELADO DE AMENZAS CIBERNÉTICAS **/** PLANIFICACIÓN Y CONDUCCIÓN DE AUDITORÍAS DE CIBERSEGURIDAD **/** TÉCNICAS AVANZADAS DE HACKEO ÉTICO **/** SEGURIDAD DE APLICACIONES WEB Y MÓVILES

MICROCREDENCIALES

CONJUNTO DE MATERIAS PERTENECIENTES A OTRO PROGRAMA EDUCATIVO (CONSULTAR EL CATÁLOGO DISPONIBLE)

CUGDL
CENTRO UNIVERSITARIO DE GUADALAJARA

PLAN DE ESTUDIOS

Áreas de Formación	Créditos	%
Área de Formación Básica Común	60	17
Área de Formación Básica Particular Obligatoria	56	16
Área de Formación Especializante Obligatoria	129	37
Área de Formación Especializante Selectiva	80	23
Área de Formación Optativa Abierta	24	7
Número mínimo de créditos para obtener el Título:	**349**	**100**

Área de formación básico común

Unidad de Aprendizaje	Tipo	Horas Teoría	Horas Práctica	Horas Totales	Créditos	Prerequisitos
Pensamiento crítico	CT	40	40	80	8	
Innovación Tecnológica	CT	40	40	80	8	
Inteligencia Colectiva	CT	40	40	80	8	
Storytelling	CT	40	40	80	8	
Gestión Socioemocional y Cognitivo	CT	40	40	80	8	
Análisis de Problemas Globales del Siglo XXI	-	-	-	80	8	
Gestión de Proyectos	CT	40	40	80	8	
Formación Integral	-	-	60	60	4	
Totales:		**240**	**300**	**620**	**60**	

Área de formación básico particular obligatoria

Unidad de Aprendizaje	Tipo	Horas Teoría	Horas Práctica	Horas Totales	Créditos	Prerequisitos
Algebra Lineal	CT	40	40	80	8	
Introducción a la Ciencia de Datos	CT	40	40	80	8	
Matemáticas I	CT	40	40	80	8	
Programación I	CT	40	40	80	8	
Probabilidad y Estadística	CT	40	40	80	8	
Ética y Responsabilidad Social	CT	40	40	80	8	
Matemáticas II	CT	40	40	80	8	Matemáticas I
Totales:		**280**	**280**	**560**	**56**	

Área de formación especializante obligatoria

Unidad de Aprendizaje	Tipo	Horas Teoría	Horas Práctica	Horas Totales	Créditos	Prerequisitos
Programación II	CT	40	40	80	8	Programación I
Hacking ético (Fundamentos)	CT	40	40	80	8	
Sistemas Operativos Distribuidos	CT	40	40	80	8	
Fundamentos de Redes y Telecomunicaciones	CT	40	40	80	8	
Gestión de Riesgos y Recuperación de Desastres	CT	40	40	80	8	
La Nube Computacional y la Ciberseguridad	CT	40	40	80	8	
Arquitectura de Sistemas de Seguridad	CT	40	40	80	8	
Privacidad y Protección de Datos	CT	40	40	80	8	
Análisis y Visualización de Datos para Ciberseguridad	CT	40	40	80	8	
Criptografía y Seguridad de la Información	CT	40	40	80	8	
Investigación y Análisis Forense Digital	CT	40	40	80	8	
Diseño y Análisis de Algoritmos Seguros	CT	40	40	80	8	
Bases de Datos	CT	0	80	80	8	
Prácticas Profesionales	PP	0	260	260	17	
Proyecto Integrador	CT	40	40	80	8	
Totales:		**520**	**860**	**1,380**	**129**	

Área de formación especializante Selectiva Orientación A

Unidad de Aprendizaje	Tipo	Horas Teoría	Horas Práctica	Horas Totales	Créditos	Prerequisitos
Orientación A-1 para ciberseguridad	CT	40	40	80	8	
Orientación A-2 para ciberseguridad	CT	40	40	80	8	
Orientación A-3 para ciberseguridad	CT	40	40	80	8	
Orientación A-4 para ciberseguridad	CT	40	40	80	8	
Orientación A-5 para ciberseguridad	CT	40	40	80	8	
Totales:		**200**	**200**	**400**	**40**	

Área de formación especializante Selectiva Orientación B

Unidad de Aprendizaje	Tipo	Horas Teoría	Horas Práctica	Horas Totales	Créditos	Prerequisitos
Orientación B-1 para ciberseguridad	CT	40	40	80	8	
Orientación B-2 para ciberseguridad	CT	40	40	80	8	
Orientación B-3 para ciberseguridad	CT	40	40	80	8	
Orientación B-4 para ciberseguridad	CT	40	40	80	8	
Orientación B-5 para ciberseguridad	CT	40	40	80	8	
Totales:		**200**	**200**	**400**	**40**	

Área de formación optativa abierta

Unidad de Aprendizaje	Tipo	Horas Teoría	Horas Práctica	Horas Totales	Créditos	Prerequisitos
Optativa I	CT	40	40	80	8	
Optativa II	CT	40	40	80	8	
Optativa III	CT	40	40	80	8	
Optativa IV	CT	40	40	80	8	
Optativa V	CT	40	40	80	8	
Optativa VI	CT	40	40	80	8	


CUGDL
CENTRO UNIVERSITARIO DE GUADALAJARA