

Certificación en **Ciberdefensa Avanzada** + **Microcredencial en** **Criptografía Postcuántica**



A DISTANCIA

Sesiones sincrónicas en vivo,
no incluye grabaciones



**MICROCREDENCIAL
POR MÓDULO**





¿POR QUÉ ESTUDIAR ESTE PROGRAMA?

Prepárate para defender la infraestructura digital de hoy y anticipar los riesgos del futuro

Desarrollarás una visión integral de la seguridad, desde la protección de redes y aplicaciones hasta la gestión de incidentes y entornos cloud. Como elemento diferenciador, estudiarás los límites de la criptografía clásica y los fundamentos de las soluciones postcuánticas, un campo emergente para la preparación tecnológica de las organizaciones

OBJETIVO DEL PROGRAMA

Desarrolla habilidades técnicas, analíticas y estratégicas para proteger activos digitales, gestionar riesgos y cumplimiento normativo, asegurar entornos híbridos y en la nube, responder ante incidentes y comprender los desafíos de seguridad de la era postcuántica.

¿PARA QUIÉN ES ESTE PROGRAMA?

¿Te reconoces en alguno de estos *perfiles*?

Dirigido a:

Profesionales de tecnologías de la información, ingeniería informática, seguridad informática, administración de sistemas y campos afines, así como a personas interesadas en adquirir conocimientos en ciberseguridad.

REQUISITOS

Contar con conocimientos básicos de informática y redes.

¿Qué aprenderás?

- ✓ Diseñar arquitecturas de red seguras y configurar mecanismos de protección perimetral
- ✓ Evaluar riesgos tecnológicos mediante estándares y normativas de seguridad
- ✓ Integrar controles criptográficos y prácticas de desarrollo seguro en aplicaciones
- ✓ Estructurar protocolos para detectar, contener y atender incidentes cibernéticos
- ✓ Proteger servicios, contenedores e infraestructuras en entornos cloud e híbridos
- ✓ Reconocer los límites de la criptografía clásica y los fundamentos de la criptografía postcuántica



ESTRUCTURA DEL PROGRAMA

Todo lo que necesitas saber antes de inscribirte.

MODALIDAD



A distancia

Sesiones sincrónicas en vivo,
no incluye grabaciones

NIVEL



Intermedio

DURACIÓN



120 horas

• 6 meses | 6 módulos

HORARIOS

Viernes de 18:00 a 22:00 hrs y sábados de 09:00 a 13:00 hrs

SOLICITAR INFORMACIÓN →

INVERSIÓN

Inscripción: \$4,000 MXN

Colegiaturas: 6 pagos de \$4,000 MXN



ANÁHUAC MAYAB
Educación Continua

SISTEMA DE RECONOCIMIENTO

Proceso de **certificación oficial** y obtención de **insignias digitales verificables**.



PASO 1

Entregable

¿QUÉ ES?

La evidencia de que aplicaste lo aprendido. Es el producto, proyecto o ejercicio que desarrollas al cierre de cada módulo para demostrar la competencia adquirida — no un examen, sino una muestra real de lo que ya sabes hacer.



¿CÓMO SE ENTREGA?

Cada módulo define su propio entregable y se envía en la plataforma del programa dentro del plazo indicado por el facilitador. Su aprobación es requisito para obtener la microcredencial del módulo.



PASO 2

Microcredencial

¿QUÉ ES?

Una microcredencial es una insignia digital que obtienes al aprobar cada módulo individualmente. Certifica una competencia concreta y es verificable y compartible en tus redes y plataformas de empleo desde el momento en que la recibes.



¿CÓMO SE OBTIENE?

Cumpliendo con la asistencia y entregando la evidencia de cada módulo. Al finalizar el programa, habrás acumulado una colección de insignias que documenta tu aprendizaje paso a paso.



PASO 3

Certificación

¿QUÉ ES?

Una certificación es el reconocimiento formal de las competencias que desarrollaste y demostraste a lo largo del programa. Al concluirlo, recibirás un documento oficial emitido por la Universidad Anáhuac Mayab —y en programas seleccionados*, respaldado por un organismo aliado— que acredita tu perfil ante el mercado profesional.



¿CÓMO SE OBTIENE?

Aprobando todos los módulos con asistencia mínima del 80% y entregando las evidencias de aprendizaje de cada etapa.

SISTEMA DE NIVELES
5 niveles de competencia

01



FUNDAMENTOS
SABER

02



HERRAMIENTAS
SABER HACER

03



METODOLOGÍAS
SABER CÓMO

04



APLICACIÓN PROFESIONAL
SABER RESOLVER

05



INNOVACIÓN
SABER TRANSFORMAR



ANÁHUAC MAYAB
Educación Continua

SISTEMA DE RECONOCIMIENTO

Tu ruta hacia la certificación



MÓDULO 1

FUNDAMENTOS DE CIBERDEFENSA Y ARQUITECTURA DE REDES SEGURAS

1.1. Introducción a la ciberseguridad

1.2. Conceptos básicos de ciberseguridad

1.3. Amenazas y riesgos cibernéticos

1.4. Marco legal y regulaciones en ciberseguridad

1.5. Seguridad de redes y sistemas

1.5.1. Fundamentos de redes y protocolos

1.5.2. Topologías de red segura

1.5.3. Configuración y gestión de firewalls y sistemas de detección de intrusos (IDS/IPS)

FUNDAMENTOS



MICROCREDENCIAL

Arquitectura de Redes Blindadas

Establece defensas perimetrales e internas robustas mediante el diseño de arquitecturas de red seguras y protocolos de protección para mitigar riesgos de intrusión y salvaguardar los activos organizacionales tradicionales.

 **ENTREGABLE:**
Diseño de Topología de Red Segura: esquema técnico descriptivo que incluya la configuración lógica de perímetros, firewalls y sistemas de detección (IDS/IPS) para mitigar riesgos identificados

MÓDULO 2

GOBERNANZA DIGITAL: GESTIÓN DE RIESGOS Y CUMPLIMIENTO NORMATIVO

2.1. Evaluación de riesgos

2.2. Normativas y estándares de seguridad cibernética (ISO 27001, NIST, GDPR, etc.)

2.3. Planificación y gestión de la seguridad de la información

HERRAMIENTAS



MICROCREDENCIAL

Auditor de Riesgos y Cumplimiento Normativo

Evalúa el riesgo tecnológico y el nivel de exposición de los activos críticos de una entidad mediante la aplicación de normativas y estándares internacionales (ISO 27001, NIST, GDPR) para estructurar planes organizacionales de cumplimiento y gobernanza digital.

 **ENTREGABLE:**
Matriz de Gestión de Riesgos Institucionales: documento de planificación que identifique activos críticos y proponga controles de seguridad alineados con el marco legal vigente

MÓDULO 3

DEVSECOPS Y BLINDAJE DE DATOS: DESARROLLO Y CRIPTOGRAFÍA APLICADA

3.1. Criptografía y seguridad de la información

3.1.1. Principios de criptografía

3.1.2. Gestión de claves

3.1.3. Seguridad en el almacenamiento y transmisión de datos

3.2. Seguridad en aplicaciones y desarrollo seguro

3.2.1. Principios de desarrollo seguro

3.2.2. Pruebas de penetración y evaluación de seguridad de aplicaciones

3.2.3. Mitigación de vulnerabilidades en aplicaciones web y móviles

METODOLOGÍAS



MICROCREDENCIAL

Desarrollo Seguro y Blindaje de Datos

Integra controles criptográficos avanzados y prácticas de desarrollo seguro en el ciclo de vida del software a través del análisis de vulnerabilidades y la gestión de claves para blindar aplicaciones web y móviles contra fugas o alteraciones de información.



ENTREGABLE:
Reporte de Pentesting y Mitigación en Aplicaciones: informe técnico de evaluación de vulnerabilidades en una aplicación web o móvil con una propuesta formal de cifrado y gestión de claves

MÓDULO 4

OPERACIONES DE CIBERSEGURIDAD: MONITOREO Y RESPUESTA A INCIDENTES

4.1. Monitorización de seguridad

4.2. Identificación y gestión de incidentes de seguridad

4.3. Recuperación y respuesta ante incidentes cibernéticos

APLICACIÓN PROFESIONAL



MICROCREDENCIAL

Operador de Respuesta a Incidentes Cibernéticos

Gestiona operaciones de monitoreo continuo y protocolos de respuesta a incidentes (IRP) mediante el diseño de flujos tácticos de detección, contención y erradicación para mitigar ciberataques de forma ágil y efectiva bajo escenarios de alta presión.



ENTREGABLE:
Protocolo de Respuesta a Incidentes (IRP): manual operativo que detalle minuciosamente los pasos de identificación, contención, erradicación y recuperación ante un ataque cibernético simulado

MÓDULO 5

CLOUD SECURITY:
PROTECCIÓN A ENTORNOS
VIRTUALES E HÍBRIDOS

- 5.1. Seguridad en entornos de nube pública, privada e híbrida
- 5.2. Despliegue seguro de servicios en la nube
- 5.3. Virtualización segura y contenedores

APLICACIÓN PROFESIONAL



MICROCREDENCIAL

Seguridad Cloud y
Virtualización

Implementa estrategias de protección e infraestructuras seguras en entornos de nube pública, privada e híbrida mediante la definición de políticas IAM, hardening de contenedores y blindaje virtual para neutralizar vectores de compromiso en ecosistemas virtualizados.



ENTREGABLE:
Plan de Despliegue Seguro en la Nube:
configuración documentada de un entorno cloud con políticas de acceso, seguridad en contenedores y blindaje de infraestructura virtual

MÓDULO 6

CRIPTOGRAFÍA
POSTCUÁNTICA

- 6.1. Complejidad computacional y límites de la criptografía clásica
- 6.2. Elementos básicos de computación cuántica
- 6.3. El algoritmo de Shor
- 6.4. Criptografía postcuántica: criptografía basada en retículos

FUNDAMENTOS



MICROCREDENCIAL

Fundamentos de Criptografía
Postcuántica (Especialidad)

Describe los principios teóricos de la computación cuántica, las limitaciones de la criptografía clásica y los esquemas basados en retículos mediante la identificación conceptual de sus algoritmos y alcances para fundamentar planes organizacionales de concientización y prevención de riesgos tecnológicos futuros.



ENTREGABLE:
Reporte de Análisis Conceptual y Mapeo de Amenazas Cuánticas





MTRO.

Miguel Antonio Guirao Aguilera

Ingeniero en Sistemas Computacionales, con Maestría en Gestión de Tecnologías de la Información, actualmente se encuentra cursando un doctorado en Ciencias de la Computación por la Universidad Estatal de Nuevo México, USA, con la especialidad en Seguridad y Privacidad en Machine Learning.

En cuanto a su experiencia profesional, se ha desempeñado como Analista de Servicio en Sistemas Integrales de Automatización, analista de Logística y analista de datos. Fundó Futura Soluciones Libres, a través de la cual proporciona servicios de consultoría a PYMES para implementar servicios de TI basados en software libre, así como también consultoría para la valoración de la seguridad en la infraestructura de TI. Es miembro profesional de la Association for Computing Machinery (ACM).

Ha participado en diversos congresos nacionales de Seguridad Informática, así como conferencias internacionales como DEFCON en Las Vegas, Nevada, donde actualmente es parte del equipo de liderazgo de la Crypto and Privacy Village.





DR.

José Gabriel Urzaiz Lares

Ingeniero en Computación por la Universidad Nacional Autónoma de México (UNAM) y Doctor en Tecnologías Informáticas Avanzadas por la Universidad de Castilla-La Mancha, España. Cuenta con más de veinte años de experiencia profesional tanto en puestos técnicos como gerenciales, y más de cuarenta años de experiencia docente en el ámbito de la ingeniería y las ciencias computacionales.

En la Universidad Anáhuac Mayab ha desempeñado diversos cargos académicos y de liderazgo, entre ellos director de las Escuelas de Informática y de Ingeniería en Sistemas Estratégicos de Información, profesor investigador y coordinador académico de posgrado. Su labor ha estado orientada al fortalecimiento de la formación tecnológica, la innovación educativa y la consolidación de programas académicos con enfoque en desarrollo de software, gestión de sistemas y tecnologías emergentes.

Actualmente se desempeña como profesor universitario en la División de Ingeniería y Ciencias Exactas de la Universidad Anáhuac Mayab, donde continúa contribuyendo al desarrollo académico de nuevas generaciones de ingenieros y profesionales en el área de tecnologías de la información.





ING.

Walter Medina Puy

Ingeniero en Sistemas Computacionales con especialidad en ciberseguridad y experiencia en pentesting, gestión de vulnerabilidades y seguridad en la nube.

Cuenta con más de nueve años de trayectoria en desarrollo de software y seguridad informática, combinando docencia, consultoría y participación en proyectos corporativos. Posee experiencia en la identificación y mitigación de riesgos, implementación de controles basados en ISO 27001 y NIST, y diseño de arquitecturas seguras en entornos cloud y DevSecOps.

Actualmente se desempeña como Backend Software Engineer en Htech, donde desarrolla microservicios seguros en C#, Python y Golang bajo arquitectura DDD, integra servicios distribuidos mediante Docker y despliegues en AWS, y participa en proyectos con certificación PCI DSS Nivel 1.



MTRO.

Edgar Antonio Palma de la Cruz

Ingeniero en Computación por la Universidad Autónoma de Yucatán. Posee certificaciones de alto nivel, incluyendo Professional Cloud Security Engineer y Professional Cloud Architect por Google Cloud, así como certificaciones en seguridad, como Offensive Security Web Expert, OffSec Experienced Penetration Tester y Offensive Security Certified Professional.

Actualmente se desempeña como Lead Security en EPAM Systems. Previamente, trabajó como consultor en sistemas de desarrollo y soporte de plataformas, y como consultor de seguridad de TI en Estratel y en The Ksquare. Ha ampliado sus conocimientos y experiencia en seguridad informática y tecnologías de la información a través de proyectos en diferentes ámbitos empresariales.

SOBRE LA UNIVERSIDAD ANÁHUAC MAYAB

MÁS DE 40 AÑOS FORMANDO LÍDERES EN EL SURESTE.

Una institución con vocación de excelencia, acreditaciones internacionales y una comunidad que impulsa el desarrollo profesional y humano de cada alumno.

En la **Universidad Anáhuac Mayab** hemos trabajado de manera constante para ofrecer los mejores programas educativos en la región, diseñando contenidos que responden a las demandas actuales de nuestra sociedad.

Nuestros programas integran conocimientos técnicos especializados con el desarrollo de habilidades de liderazgo, comunicación y trabajo en equipo, asegurando que cada egresado cuente con herramientas de alto valor y conexiones que impulsarán su crecimiento.

Miembros de:

uni>ersia

RECLA
Red de Educación Continua
de Latinoamérica y Europa

edx

Acreditados por:



FIMPES



Comunidad de impacto

Claustro académico con experiencia real en la industria y una red de egresados con presencia nacional e internacional.



Formación integral

Programas diseñados para desarrollar profesionales con visión estratégica, valores sólidos y habilidades para transformar su entorno.



ANÁHUAC MAYAB
Educación Continua

PROCESO DE INSCRIPCIÓN

01

Entra a nuestra página

merida.anahuac.mx/educacion-continua 

02

Encuentra el programa de tu preferencia

Y ubica el botón “Solicitar información”

03

Llena el formulario de contacto

Encuétralo al final de la página del programa.

04

Espera tu correo de confirmación

Recibirás un mail con los pasos para completar tu inscripción. Síguelos y confirma tu lugar.

CONTACTO

Continúa tu crecimiento profesional



TU ASESOR

MARTIN CAN

TEL (999) 942 48 00 Ext. 1615

MAIL martin.sabido@anahuac.mx

WEB merida.anahuac.mx/educacion-continua