

# Licenciatura en Ingeniería en Ciberseguridad

Modalidad

**Semipresencial/Online**

Duración

**4 años**





## 01. Introducción

Modalidad semipresencial

Nuestro modelo educativo

Nuestra área académica

---

## 02. Programa académico

El programa universitario en Ciberseguridad

Campus virtual, recursos y docencia

Evaluación y exámenes online

Prácticas presenciales

---

## 03. Itinerario académico

Plan de estudios

---

## 04. Acompañamiento académico

Tutor académico asignado

Clases en directo y seguimiento

---

## 05. Admisión y reconocimiento

Reconocimiento de créditos

Admisión

# ¿Qué significa estudiar Ciberseguridad en Mundae?

En la **Universidad Internacional Mundae** entendemos la educación como un proceso activo que conecta la teoría con la práctica y la formación universitaria con la realidad tecnológica y digital contemporánea. Apostamos por una enseñanza que se construye en diálogo con entornos reales, con una visión global de la ingeniería y con un uso avanzado de la tecnología educativa aplicada a la ciberseguridad.

La **Licenciatura en Ingeniería de Ciberseguridad** responde plenamente a esta misión. Ofrecemos una formación superior basada en fundamentos científicos y técnicos sólidos, orientada al desarrollo del pensamiento analítico y crítico, a la aplicación progresiva del conocimiento y a la integración de experiencias prácticas en entornos profesionales vinculados a la protección de sistemas, redes y datos, con posibilidad de acceder a un itinerario de proyección internacional.

En la universidad, situamos al estudiante en el centro del proceso formativo y garantizamos un acompañamiento académico continuo en cada etapa del aprendizaje, favoreciendo una formación rigurosa, aplicada y alineada con los estándares internacionales del sector tecnológico.

Duración

4 años

Modalidad

Semipresencial  
/Online

## Modalidad semipresencial

La formación se estructura bajo un modelo semipresencial que integra, de manera equilibrada y coherente, el **rigor académico con la aplicación práctica**.

La **parte teórica** se desarrolla íntegramente a través del **campus virtual**, una plataforma de aprendizaje avanzada, accesible **24/7**, que permite al estudiante gestionar su ritmo de estudio con total flexibilidad y acompañamiento docente continuo.

La parte práctica, de carácter obligatorio, se desarrolla de forma presencial, garantizando una experiencia formativa aplicada, inmersiva y alineada con los más altos estándares profesionales en **entornos reales**.

# Nuestro modelo educativo

Nuestro modelo educativo combina trabajo académico riguroso, actividades aplicadas, resolución de problemas reales y formación práctica desde etapas tempranas del itinerario formativo. En el ámbito de la Ingeniería de Ciberseguridad, este enfoque conecta los fundamentos científicos y técnicos con la realidad operativa de los sistemas, redes y entornos digitales contemporáneos.

Según la **Metodología Mundae**, estructuramos el aprendizaje en tres ejes:

---

## 01 Aprendizaje a través de experiencias reales

Integramos prácticas formativas, actividades de simulación, análisis de casos y proyectos aplicados vinculados a contextos profesionales de la ciberseguridad, tales como la administración de sistemas, la protección de infraestructuras digitales, el análisis de amenazas y la gestión de incidentes en entornos reales y simulados.

---

## 02 Construcción progresiva de competencias

Organizamos el desarrollo académico en fases que avanzan desde la comprensión de los fundamentos matemáticos, lógicos y computacionales, hasta el diseño, implementación y auditoría de soluciones de seguridad en escenarios tecnológicos complejos, conforme a los estándares del sector.

---

## 03 Uso intensivo de tecnología educativa

Aplicamos recursos digitales avanzados, laboratorios virtuales, entornos de simulación, plataformas de análisis y herramientas especializadas para reforzar la comprensión de arquitecturas, algoritmos, redes y sistemas seguros, y para preparar al estudiante para la práctica profesional en contextos digitales reales.

---

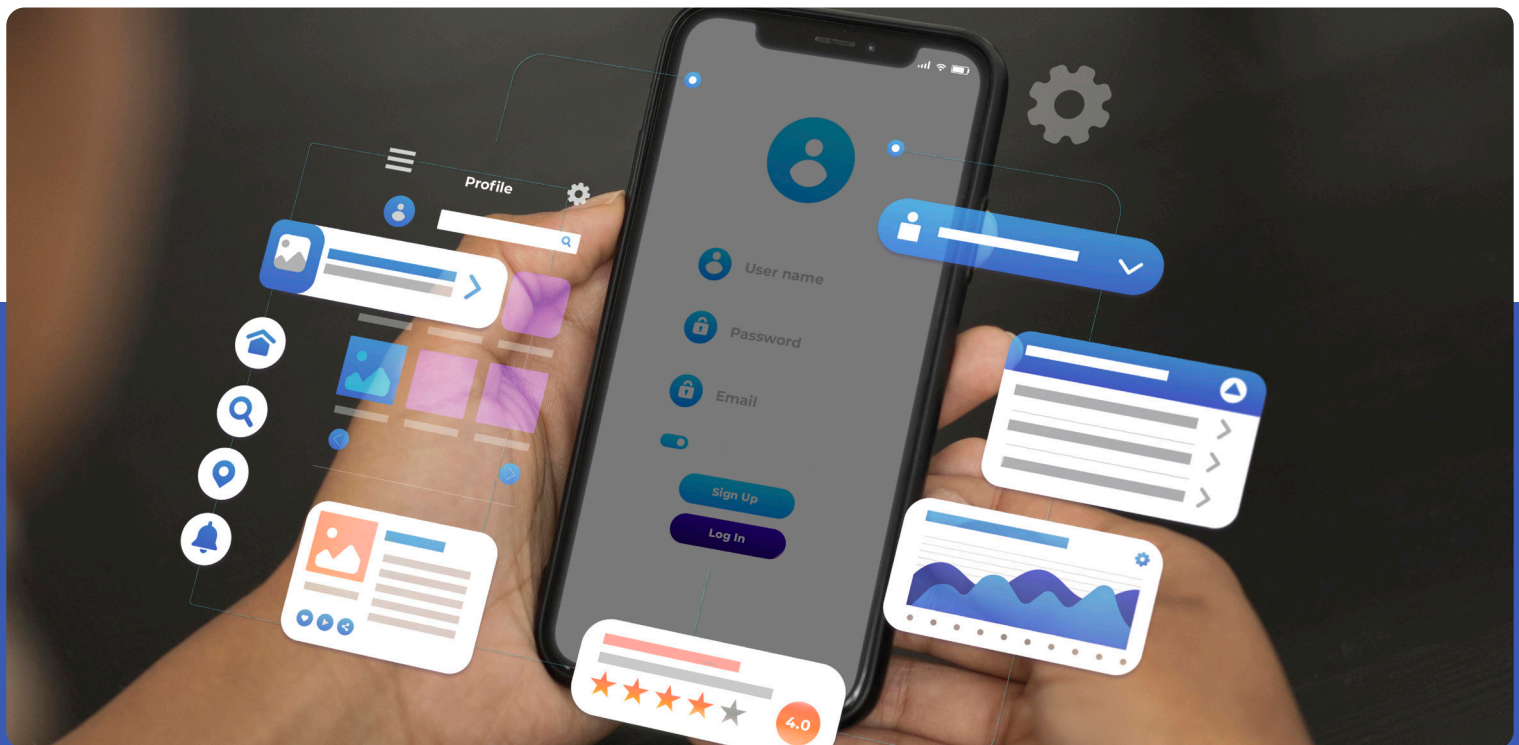
Este modelo nos permite formar profesionales de la ciberseguridad capaces de analizar, diseñar, proteger y auditar sistemas tecnológicos, actuando con solvencia técnica en situaciones reales desde etapas tempranas de su formación.

# Nuestra área académica

La Licenciatura en Ingeniería en Ciberseguridad se integra en el área académica de **Ingeniería, Ciencia y Tecnología**, que articula programas universitarios orientados al estudio, diseño y desarrollo de sistemas técnicos y tecnológicos desde una perspectiva científica, aplicada e interdisciplinar.

Esta área reúne titulaciones vinculadas a las distintas ramas de la ingeniería, las ciencias tecnológicas y las ciencias experimentales. Todas ellas comparten fundamentos matemáticos, físicos y tecnológicos que permiten comprender, diseñar y gestionar sistemas complejos en entornos industriales, científicos y digitales.

En este marco académico, la Ingeniería en Ciberseguridad se sitúa como una disciplina especializada en la protección de infraestructuras tecnológicas, sistemas informáticos y redes de comunicación frente a amenazas digitales. La formación integra conocimientos técnicos y metodológicos orientados al análisis de vulnerabilidades, la gestión de riesgos tecnológicos y el desarrollo de sistemas seguros, contribuyendo a la protección de los entornos digitales contemporáneos. El área cuenta con plataformas tecnológicas avanzadas y un claustro docente con sólida trayectoria académica y profesional en ingeniería y tecnología.



# El Programa Universitario en Ciberseguridad

El programa universitario en Ingeniería de Ciberseguridad está orientado a la formación de profesionales capaces de diseñar, analizar, proteger y auditar sistemas, redes y entornos digitales, desde una base científica y técnica sólida y con criterios profesionales actualizados. La titulación ofrece una estructura formativa progresiva que combina **campus virtual, actividades aplicadas, formación práctica y experiencias en entornos profesionales reales y simulados**.

El diseño del programa se sustenta en los siguientes **pilares académicos**:

---

Fundamentos matemáticos, lógicos y computacionales aplicados a la ingeniería

---

Arquitectura de computadores, sistemas operativos y bases de datos

---

Redes de ordenadores y servicios de red

---

Programación estructurada, orientada a objetos, concurrente y distribuida

---

Seguridad de sistemas, redes y aplicaciones

---

Criptografía y protección de la información

---

Análisis de amenazas, hacking ético y pentesting

---

Legislación, gobernanza y gestión del riesgo en ciberseguridad

---

Metodologías de ingeniería, proyectos tecnológicos e investigación aplicada

---

Prácticas profesionales progresivas y supervisadas

---

Este enfoque integral garantiza una formación rigurosa, aplicada y alineada con los estándares universitarios y profesionales internacionales, preparando al estudiante para integrarse con solvencia en los distintos ámbitos de ejercicio profesional de la ciberseguridad y la ingeniería informática.

# Campus virtual, recursos y docencia

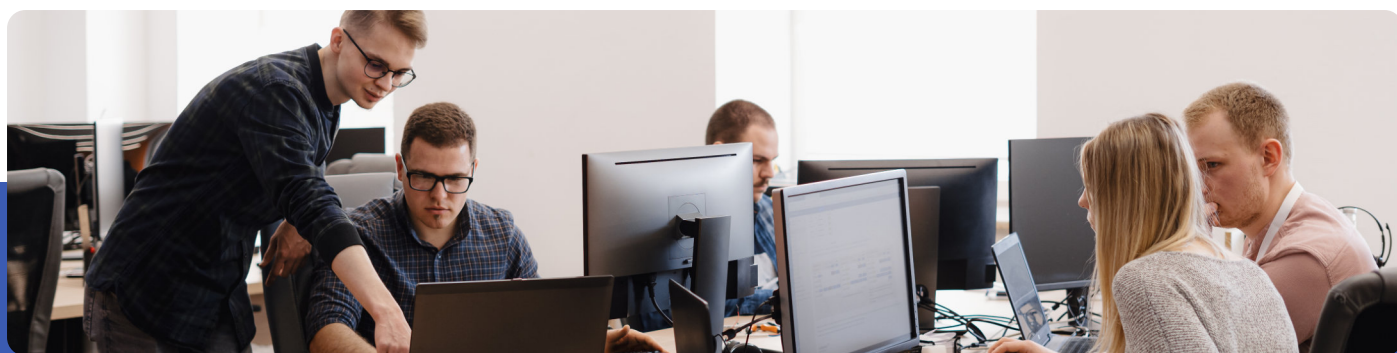
La docencia se imparte en **modalidad online** a través de un campus virtual que constituye el eje central del proceso formativo. El estudiante dispone de **acceso permanente a los contenidos académicos**, organizados por asignaturas, así como a los materiales docentes y recursos audiovisuales elaborados por el equipo académico.

El modelo docente se complementa con sesiones en directo orientadas a la ampliación de contenidos, la interacción académica y la resolución de dudas.

## Evaluación y exámenes online

La evaluación se desarrolla íntegramente en **modalidad online**, conforme a la planificación académica del programa. Este sistema permite un **seguimiento riguroso y continuo del progreso académico**, garantizando la trazabilidad del aprendizaje y el cumplimiento de criterios universitarios de calidad.

# Prácticas presenciales o telemáticas



El programa incorpora un periodo de **prácticas presenciales o telemáticas**, diseñado para aplicar los conocimientos adquiridos y consolidar competencias profesionales en entornos digitales reales y simulados. Esta etapa formativa permite al estudiante integrarse en contextos profesionales del ámbito de la ciberseguridad, participando en actividades relacionadas con la protección de sistemas, redes y datos desde una modalidad plenamente alineada con la realidad del sector tecnológico.

Durante el desarrollo de las prácticas, el estudiante cuenta con **orientación y seguimiento académico continuos**, garantizando la coherencia entre la experiencia práctica y los objetivos formativos del programa, así como el cumplimiento de los estándares universitarios y profesionales vigentes.

# Plan de estudios

| Curso Académico | Código         | Nombre de la asignatura                                 | Horas | Créditos CR | Equiv. ECTS |
|-----------------|----------------|---------------------------------------------------------|-------|-------------|-------------|
| 1               | CR-LIC-ICI0305 | Inglés técnico                                          | 90    | 2           | 4           |
|                 | CR-LIC-ICI0102 | Fundamentos de hardware                                 | 135   | 3           | 5           |
|                 | CR-LIC-ICI0103 | Gestión de bases de datos                               | 225   | 5           | 9           |
|                 | CR-LIC-ICI0202 | Lenguaje de marcas y sistemas de gestión de información | 180   | 4           | 7           |
|                 | CR-LIC-ICI0302 | Administración de sistemas operativos                   | 180   | 4           | 7           |
|                 | CR-LIC-ICI0104 | Planificación y administración de redes                 | 225   | 5           | 9           |
|                 | CR-LIC-ICI0201 | Implantación de sistemas operativos                     | 315   | 7           | 13          |
|                 | CR-LIC-ICI0101 | Empleabilidad I - FOL                                   | 90    | 2           | 4           |
|                 | CR-LIC-ICI0303 | Empleabilidad II - EIE                                  | 90    | 2           | 4           |
|                 | CR-LIC-ICI0401 | Servicios de red e internet                             | 180   | 4           | 7           |
|                 | CR-LIC-ICI0301 | Administración de sistemas gestores de bases de datos   | 180   | 4           | 7           |
|                 | CR-LIC-ICI0203 | Seguridad y alta disponibilidad                         | 180   | 4           | 7           |
|                 | CR-LIC-ICI0304 | Implantación de aplicaciones web                        | 135   | 3           | 5           |
|                 | CR-LIC-ICI0402 | Proyecto de Administración de Sistemas Informáticos     | 90    | 2           | 4           |
|                 | CR-LIC-ICI0403 | Formación en entornos laborales                         | 405   | 9           | 16          |

| Curso Académico | Código         | Nombre de la asignatura                                    | Horas | Créditos CR | Equiv. ECTS |
|-----------------|----------------|------------------------------------------------------------|-------|-------------|-------------|
| 2               | CR-LIC-ICI0802 | Arquitectura de computadores                               | 90    | 2           | 4           |
|                 | CR-LIC-ICI0502 | Análisis matemático                                        | 180   | 4           | 7           |
|                 | CR-LIC-ICI0602 | Fundamentos de programación                                | 180   | 4           | 7           |
|                 | CR-LIC-ICI0701 | Principios Jurídicos básicos aplicados a la ciberseguridad | 180   | 4           | 7           |
|                 | CR-LIC-ICI0803 | Criptografía                                               | 135   | 3           | 5           |
|                 | CR-LIC-ICI0504 | Sistemas operativos                                        | 135   | 3           | 5           |
|                 | CR-LIC-ICI0705 | Bases de datos                                             | 135   | 3           | 5           |
|                 | CR-LIC-ICI0603 | Estadística y optimización                                 | 180   | 4           | 7           |
|                 | CR-LIC-ICI0703 | Dimensiones de la seguridad                                | 180   | 4           | 7           |
|                 | CR-LIC-ICI0501 | Álgebra Lineal                                             | 180   | 4           | 7           |
|                 | CR-LIC-ICI0503 | Lógica                                                     | 180   | 4           | 7           |
|                 | CR-LIC-ICI0903 | Ingeniería del software                                    | 135   | 3           | 5           |
|                 | CR-LIC-ICI0704 | Programación con estructuras lineales                      | 135   | 3           | 5           |
|                 | CR-LIC-ICI0901 | Diseño y análisis de algoritmos                            | 135   | 3           | 5           |

| Curso Académico | Código         | Nombre de la asignatura                  | Horas | Créditos CR | Equiv. ECTS |
|-----------------|----------------|------------------------------------------|-------|-------------|-------------|
| 3               | CR-LIC-ICI0604 | Programación orientada a objetos         | 135   | 3           | 5           |
|                 | CR-LIC-ICI0804 | Metodologías de gestión de proyectos     | 180   | 4           | 7           |
|                 | CR-LIC-ICI0601 | Empresa y legislación                    | 180   | 4           | 7           |
|                 | CR-LIC-ICI1005 | Seguridad en redes                       | 135   | 3           | 5           |
|                 | CR-LIC-ICI1003 | Inteligencia artificial                  | 135   | 3           | 5           |
|                 | CR-LIC-ICI1002 | Proyecto de Ingeniería I                 | 135   | 3           | 5           |
|                 | CR-LIC-ICI0801 | Programación concurrente y distribuida   | 135   | 3           | 5           |
|                 | CR-LIC-ICI0702 | Redes de ordenadores                     | 180   | 4           | 7           |
|                 | CR-LIC-ICI0904 | Grandes Volúmenes de Datos               | 135   | 3           | 5           |
|                 | CR-LIC-ICI0905 | Redes Avanzadas y Computación en la Nube | 135   | 3           | 5           |
|                 | CR-LIC-ICI0902 | Técnicas de Hacking                      | 135   | 3           | 5           |
|                 | CR-LIC-ICI0805 | Técnicas de programación avanzada        | 135   | 3           | 5           |
|                 | CR-LIC-ICI1001 | Desarrollo Seguro de Web y Apps          | 135   | 3           | 5           |
|                 | CR-LIC-ICI1101 | Pentesting                               | 135   | 3           | 5           |
|                 | CR-LIC-ICI1103 | Análisis y Gestión del Riesgo            | 90    | 2           | 4           |

| Curso Académico | Código         | Nombre de la asignatura                 | Horas | Créditos CR | Equiv. ECTS |
|-----------------|----------------|-----------------------------------------|-------|-------------|-------------|
| 4               | CR-LIC-ICI1004 | Seguridad en Base de datos              | 135   | 3           | 5           |
|                 | CR-LIC-ICI1102 | Proyecto de Ingeniería II               | 90    | 2           | 4           |
|                 | CR-LIC-ICI1203 | Prácticas Externas                      | 180   | 4           | 7           |
|                 | CR-LIC-ICI1105 | Auditoría                               | 90    | 2           | 4           |
|                 | CR-LIC-ICI1202 | Regulación y Gobernanza de la Seguridad | 180   | 4           | 7           |
|                 | CR-LIC-ICI1106 | Metodologías de desarrollo seguro       | 90    | 2           | 4           |
|                 | CR-LIC-ICI1107 | Investigación                           | 90    | 2           | 4           |
|                 | CR-LIC-ICI1201 | Proyecto de Ingeniería III              | 135   | 3           | 5           |
|                 | CR-LIC-ICI1104 | Malware y amenazas dirigidas            | 90    | 2           | 4           |
|                 | CR-LIC-ICI1204 | Trabajo Final de Graduación             | N/A   | N/A         | N/A         |



# Acompañamiento académico

## Tutor académico asignado

Cada estudiante dispone de un **tutor académico de referencia**, responsable de orientar su proceso formativo, apoyar la planificación del estudio y realizar un seguimiento personalizado del progreso académico a lo largo de todo el programa. Este acompañamiento facilita la correcta integración de los contenidos técnicos y el desarrollo progresivo de las competencias propias de la ingeniería en ciberseguridad.

## Clases en directo y seguimiento

La docencia se complementa con **clases en directo**, concebidas como espacios de interacción académica, ampliación de contenidos técnicos y resolución de dudas. Estas sesiones refuerzan la comprensión de los conceptos complejos propios del ámbito tecnológico y permiten un seguimiento continuo del aprendizaje, con posibilidad de acceso posterior en diferido.

# Reconocimiento de créditos

El estudiante podrá solicitar el **reconocimiento de créditos** en función de su formación previa, de acuerdo con la normativa académica vigente. Podrán ser objeto de reconocimiento los estudios oficiales universitarios u otras titulaciones y programas de educación superior previamente cursados, tales como diplomaturas, formación profesional, Técnicos Superiores Universitarios (TSU), tecnologías superiores u otras titulaciones equivalentes, siempre que exista correspondencia académica y competencial con los contenidos del programa.

Este procedimiento permite optimizar el recorrido formativo del estudiante, respetando en todo momento los criterios académicos y los estándares universitarios establecidos.

# Admisión

El proceso de admisión se realiza íntegramente en modalidad online y está diseñado para facilitar el acceso al programa de manera clara y flexible.

Desde el inicio, el estudiante cuenta con **orientación académica especializada** para la correcta planificación de su itinerario formativo.

Formamos ingenieros en Ciberseguridad **capaces de proteger infraestructuras digitales en entornos reales, preparados para responder a los desafíos tecnológicos de sistemas informáticos modernos** y con oportunidades de vivir experiencias internacionales para fortalecer su desarrollo académico y profesional.

Proud  
to be.



Universidad  
Mundaë

(+34) 911 23 80 70  
info@mundauniversidad.com  
mundauniversidad.com

## Nuestros campus

### Costa Rica

Edificio Odessa XR26+C4F Unnamed Road,  
San José, Pozos, Costa Rica.

### México

Avenida Insurgentes N.º 64, Colonia Juárez, Alcaldía  
de Cuauhtémoc, Ciudad de México, C.P. 06600.

### Miami

475 Half Day Rd Ste 500  
Lincolnshire, IL 60069.

### Suiza

Rte de Meyrin 123,  
1219 Vernier, Ginebra. Suiza.

### Colombia (Corporación Universitaria Rafael Núñez)

Centro Calle 35, Calle del Coliseo #5-35,  
Cartagena de Indias, Bolívar, Colombia.