

MAESTRÍA EN

CIBERSEGURIDAD

RVOE 20250385



Estudia
100%
en línea



Modalidad:
No escolarizado



Opción educativa:
100% en línea

Clave del plan de estudios: 2025

Diseño curricular: Flexible cuatrimestral

Total de ciclos: 6 cuatrimestres

Carga horaria a la semana: 3 hrs de clase
1 día a la semana. (Sábado)

Objetivos generales del plan de estudios

Al finalizar el plan de estudios de la Maestría en Ciberseguridad, el egresado:

Contará con los elementos que constituyen el desarrollo y análisis de los procedimientos asociados con la seguridad de redes y comunicaciones en el contexto tecnológico actual, considerando los parámetros de estudio de la criptografía y de los perfiles de ciberdelincuente y de la víctima, con la finalidad de intervenir en los procesos de gestión de riesgos, respuesta a incidentes, penetración testing y la denominada seguridad biométrica, así como en el desarrollo de las estrategias de ciberseguridad en la web, dispositivos móviles, tecnologías 5G e inteligencia artificial.



CIBERSEGURIDAD

Plan de estudios **cuatrimestral**

Primer cuatrimestre

- Fundamentos de ciberseguridad
- Ciberdefensa y ciberataques
- Criptografía y seguridad de la información

Segundo cuatrimestre

- Seguridad en redes y sistemas
- Gestión de riesgos y análisis de vulnerabilidades
- Forense digital y respuesta a incidentes

Tercer cuatrimestre

- Seguridad en aplicaciones web y móviles
- Cloud computing y seguridad en la nube
- Tecnologías emergentes y su seguridad

Cuarto cuatrimestre

- Ciberseguridad en la industria 4.0
- Inteligencia artificial y ciberseguridad
- Ciberseguridad en entornos de trabajo remoto

Quinto cuatrimestre

- Psicología del ciberdelincuente y de la víctima
- Seguridad en tecnologías 5G
- Metodologías de penetración testing

Sexto cuatrimestre

- Tecnología inversa en ciberseguridad
- Programación en python para la ciberseguridad
- Biohacking y seguridad biométrica

PERFIL DE EGRESO

Al finalizar el plan de estudios de la Maestría en Ciberseguridad, el alumno obtendrá los siguientes conocimientos, habilidades, destrezas y actitudes:

Conocimientos



Principios y prácticas fundamentales de la ciberseguridad, incluyendo la identificación de amenazas y vulnerabilidades, así como la implementación de medidas de protección esenciales.



Estrategias avanzadas de defensa cibernética y técnicas utilizadas en ciberataques, permitiendo anticipar y contrarrestar tácticas maliciosas de manera efectiva.



Métodos criptográficos y protocolos de seguridad para proteger la confidencialidad, integridad y disponibilidad de los datos en diversas plataformas.



Seguridad en entornos de computación en la nube, protegiendo datos y aplicaciones alojadas en servicios de terceros mediante la implementación de medidas adecuadas.



Utilización de técnicas de inteligencia artificial para mejorar la detección y respuesta a amenazas, aplicando soluciones avanzadas a problemas complejos de seguridad.



Adopción de un enfoque proactivo y preventivo en la protección de sistemas esenciales, asegurando la continuidad y seguridad operativa de las organizaciones.



Exploración de la intersección entre biotecnología y seguridad, implementando soluciones innovadoras para proteger datos biométricos.

Habilidades



Implementar medidas de seguridad en entornos de computación en la nube, asegurando la integridad y disponibilidad de los datos.



Evaluar y gestionar riesgos de seguridad, implementando planes de mitigación para reducir vulnerabilidades.



Implementar medidas de seguridad en entornos de computación en la nube, asegurando la integridad y disponibilidad de los datos.



Asegurar la continuidad operativa de sistemas industriales críticos, protegiendo infraestructuras y procesos de manufactura.



Liderar proyectos de ciberseguridad, coordinando equipos y recursos para implementar soluciones de seguridad.



Diseñar y ejecutar medidas de seguridad para redes y dispositivos 5G, asegurando su protección.



Implementar soluciones de biohacking y seguridad biométrica, protegiendo datos sensibles y mejorando la autenticación.



Destrezas



Desarrollar enfoques innovadores en la creación de métodos y técnicas de ciberseguridad.



Actualizar y mejorar continuamente las prácticas de seguridad informática según las amenazas actuales.



Gestionar programas de ciberseguridad en entornos industriales, asegurando la continuidad operativa.



Ajustar las medidas de seguridad a las necesidades específicas de diversas organizaciones.



Coordinar proyectos de ciberseguridad, supervisando desde la planificación hasta la implementación.



Aplicar soluciones de inteligencia artificial para fortalecer las defensas contra ciberamenazas.



Implementar técnicas de seguridad biométrica para mejorar la autenticación y protección de datos.



Actitudes



Actitudes

Empatía hacia las necesidades y preocupaciones de los usuarios en entornos digitales.



Respeto por la privacidad y derechos de los usuarios en plataformas digitales.



Perseverancia en la resolución de problemas complejos relacionados con la ciberseguridad.



"La ciberseguridad no se trata de proteger sistemas, se trata de proteger personas."

– Kevin Mitnick