

# Maestrías en ciberseguridad



## PROCEDIMIENTO DE INSCRIPCIÓN

### Objetivo de General de la Maestría en Ciberseguridad

Desarrollar, formar y actualizar profesionales quienes, por medio del conocimiento de las medidas de seguridad informática, sus riesgos y legislación aplicable; puedan salvaguardar la información empresarial y personal. De igual manera, ser capaces de proponer medidas y planes para asegurar la continuidad de la operación de los negocios

### Modalidad

- Duración: 4 semestres.
- Modalidad: clases virtuales sincrónicas.
- Horario: lunes a viernes de 20 a 22 horas (tiempo del Centro).
- Inicio de ciclo: lunes 31 de agosto de 2026.
- Nuestro ecosistema digital potencia el aprendizaje en línea con plataformas como Eduscore, Discord y Google Workspace.

### Perfil de Ingreso

Profesionistas con experiencia en:

- Administración de sistemas.
- Industrias relacionadas vertical u horizontalmente con las TICs.
- Conocimiento de conceptos fundamentales de Bases de datos, Programación, Programación orientada a objetos, Redes y Redes inalámbricas.
- Nociones de hackeo y de planificación en recuperación de desastres.
- Gusto por el manejo de computadoras y paquetes de comunicación digital.
- Alta comprensión de texto técnico en inglés.
- El/la aspirante a la Maestría en Ciberseguridad deberá ser egresado de cualquier licenciatura o ingeniería afines a la programación, el diseño y/o desarrollo de redes, seguridad informática, sistemas informáticos;
- bien, tener un desempeño laboral en alguna de estas áreas y las correspondientes en seguridad cibernética, entorno legal de la seguridad informática, fraudes cibernéticos, etc., con posibles perfiles en derecho, criminología y criminalística, entre otras.

# Maestrías en ciberseguridad



## Perfil de Egreso

- Capacidad de analizar los riesgos digitales a los que están sometidos las instituciones y organizaciones y proceder contra aquellas conductas tipificadas como delito informático.
- Conocimiento de la legislación y regulación de cumplimiento obligatorio para implementar las medidas técnicas adecuadas que permitan salvaguardar la reputación de la institución y evitar sanciones.
- Conocimientos y análisis de las demandas técnicas que permitan que la utilización de datos personales se vuelva un proceso cada vez más integrado y seguro.
- Uso de protocolos de seguridad y sistemas de gestión de seguridad de la información (SGSI).
- Manejo de técnicas criptográficas de protección para evitar la filtración de datos sensibles.
- Análisis y protección de redes, aplicaciones, sistemas operativos y dispositivos móviles.
- Mecanismos de seguridad para el desarrollo de código, sitios web y bases de datos seguros.
- Estandarizar y aplicar prácticas de auditoría de la seguridad y análisis forense digital.

## Procedimiento de inscripción

1.- Para el alta y generación de matrícula es necesario:

- Llenar esta ficha de inscripción: <https://forms.gle/cJXcXzXQ9EtW4Cqv7>
- Enviar CV y carta de motivos al correo [rosalinda.galvez@uniat.edu.mx](mailto:rosalinda.galvez@uniat.edu.mx).
- Presentar un examen diagnóstico de perfil idóneo y tener una entrevista con la Coordinación Académica de Posgrado - UNIAT.

En caso de aspirantes sin el perfil apropiado, se tendrá que acreditar el manejo de lenguajes de programación Python y C++, o en su defecto, tomar un curso propedéutico en UNIAT con mínimo de 30 horas de duración. Puede ser con profesorado propio de UNIAT o con algún socio académico, como CISCO Networking Academy.

# Maestrías en ciberseguridad



**2.-** En caso de admisión aprobada, antes del inicio de clases se requiere entregar la siguiente documentación completa a Control Escolar a más tardar el 15 de agosto de 2026 :

- Título universitario y/o cédula profesional. En caso de no tener ambos, certificado total de estudios.
- Acta de nacimiento y CURP (con QR)
- Credencial del INE (PDF por ambos lados)

Todo en original y tres copias en el domicilio: Calle Chimalhuacán #20, Col. Ciudad del Sol, Zapopan, Jalisco, México. C.P. 45050.

Tel: (33) 3122 7458. Atención a: Asesor educativo.