

**CERTUS**

**Especialización**

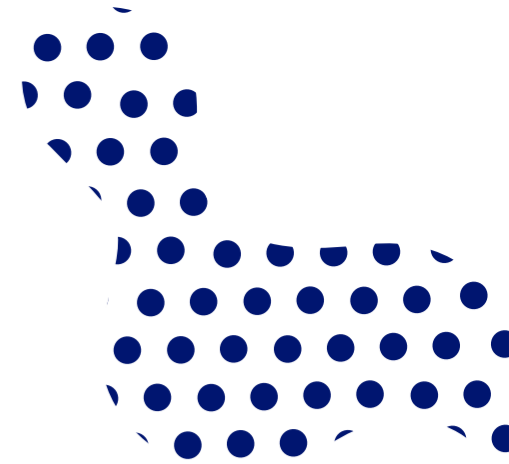
# **Gestión en Ciberseguridad**

---

 **5 meses**

 **Online**





## Gestión en Ciberseguridad

El uso de la tecnología dentro de las organizaciones se ha incrementado exponencialmente en estos últimos años y la creciente necesidad de contar con profesionales capacitados en protección y defensa de la información en entornos tecnológicos también. El programa de Ciberseguridad que ofrece Certus, busca proporcionar a los profesionales las habilidades y competencias necesarias para enfrentar los desafíos actuales y futuros en materia de ciberseguridad.

El programa brinda conocimientos sólidos en gobierno, gestión, auditoría, ciberseguridad y riesgos de TI, centrándose en la aplicación práctica de estrategias y soluciones efectivas.



**Duración:**  
**5 meses**



**160 horas**  
**académicas**

### ¿A quién está dirigido?

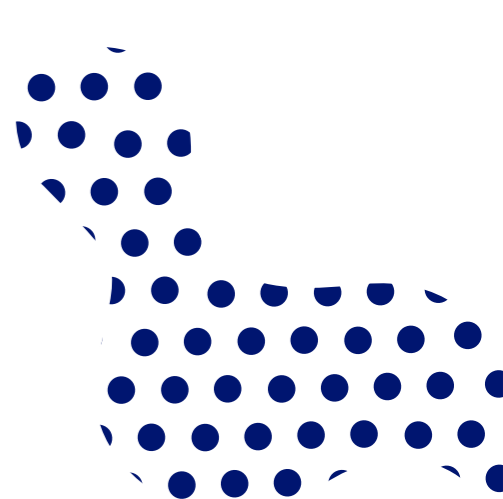


- Especialistas en seguridad de la información.
- Analistas o profesionales en auditoría, seguridad o riesgos tecnológicos.
- Personas interesadas en incrementar y mejorar sus habilidades en ciberseguridad con conocimientos previos de programación e informática.

### ¿Qué certificado obtengo?



Certificado de Especialización en **Gestión en Ciberseguridad**  
a nombre de Certus



## Gestión en Ciberseguridad

Módulo	Tema	Contenido
Módulo 1	Introducción a la ciberseguridad	<ul style="list-style-type: none"> <li>- Contexto Problemática.</li> <li>- Historia de la Seguridad.</li> <li>- Requerimientos de seguridad.</li> <li>- Amenazas, vulnerabilidades y tipos de Ataque en la actualidad.</li> <li>- Principios de la seguridad de la información.</li> <li>- Roles en Seguridad.</li> <li>- Niveles de la ciberseguridad (red team, blueteam, etc).</li> </ul>
Módulo 2	Buenas prácticas en seguridad de redes y sistemas	<ul style="list-style-type: none"> <li>- Concepto general de Arquitectura y protocolos de redes locales y empresariales.</li> <li>- Concepto de Seguridad perimétrica.</li> <li>- VPN y túneles seguros.</li> <li>- Firewalls y sistemas de detección de intrusiones.</li> <li>- Monitoreo y análisis de tráfico de red.</li> <li>- Administración de sistemas operativos en servidores.</li> <li>- Técnicas de protección malware y ransomware.</li> <li>- Plan de recuperación ante desastres.</li> <li>- Administración de plataformas distribuidas.</li> </ul>
Módulo 3	Buenas prácticas en seguridad de aplicaciones	<ul style="list-style-type: none"> <li>- Fundamentos de seguridad en el desarrollo de aplicaciones.</li> <li>- Pruebas de penetración y vulnerabilidades.</li> <li>- Codificación segura y buenas prácticas.</li> <li>- Autenticación y autorización en aplicaciones.</li> <li>- Protección contra ataques de inyección y XSS.</li> <li>- Seguridad en APIs y servicios web.</li> <li>- Seguridad en aplicaciones móviles.</li> <li>- Gestión de vulnerabilidades en aplicaciones.</li> </ul>
Módulo 4	Auditoría y gestión de riesgos	<ul style="list-style-type: none"> <li>- Normas y estándares de seguridad.</li> <li>- Auditorías de seguridad y cumplimiento.</li> <li>- Gestión de logs y registros.</li> <li>- Monitoreo y detección de intrusiones.</li> <li>- Plan de gestión de riesgos.</li> <li>- Gestión de incidentes y respuesta a brechas.</li> <li>- Análisis forense digital.</li> <li>- Pruebas de penetración y auditoría de sistemas.</li> <li>- Informes y recomendaciones de seguridad.</li> </ul>
Módulo 5	Ética y legislación en ciberseguridad	<ul style="list-style-type: none"> <li>- Aspectos éticos en ciberseguridad.</li> <li>- Responsabilidad y confidencialidad de la información.</li> <li>- Marco legal y regulaciones de ciberseguridad.</li> <li>- Responsabilidad legal de los profesionales de la ciberseguridad.</li> <li>- Regulaciones Nacionales y por sector.</li> <li>- Legislación de privacidad y protección de datos.</li> <li>- Regulaciones internacionales general y por sector.</li> <li>- Ética en el uso de tecnologías de ciberseguridad.</li> </ul>

### Conocimientos previos

Para llevar con éxito el curso, el estudiante debe tener:

- Conocimientos básicos de programación e informática.
- Comprensión de conceptos básicos de seguridad de la información.
- Motivación para aprender y mantenerse actualizado en el campo de la ciberseguridad.
- Familiaridad con los fundamentos de redes y sistemas operativos.
- Habilidades de análisis y resolución de problemas.

### Requerimientos del curso

Para poder llevar la especialización en Ciberseguridad, se requieren los siguientes requisitos mínimos técnicos:

- Software: Se espera que los estudiantes tengan acceso a un sistema operativo actualizado, así como a las herramientas específicas mencionadas en cada curso, como Wireshark, VirtualBox, Burp Suite, Nessus.
- Conexión a internet estable y de alta velocidad (recomendado: al menos 10 Mbps de velocidad de descarga).
- Conexión a Internet con velocidad mínima de 10 megas.
- Computadora o laptop con sistema operativo actualizado.
- Navegador web actualizado (recomendado: Google Chrome, Mozilla Firefox).
- Micrófono y altavoces integrados o auriculares con micrófono para participar en sesiones de audio.
- Cámara web para participar en sesiones de video.

### Te acompañamos en tu ruta de aprendizaje



¿Qué es meidei? Un sistema digital de acompañamiento personalizado, que orienta al estudiante a resolver dudas de forma inmediata durante su programa de capacitación. Asimismo, el estudiante tendrá una guía permanente llamada Lucía y recibirá pistas o microcontenidos que mejorará su experiencia de aprendizaje.

### ¿Por qué elegir Certus?



Más de 27 años de experiencias



Clases en vivo que se quedan grabadas



Docentes expertos de primer nivel



Horarios flexibles



Material adicional para complementar tu aprendizaje