



# MAESTRÍA EN CIBERSEGURIDAD

**100% Virtual**



“

Transforma tu pasión

EN ÉXITO”

GRADO  
ACADÉMICO

Maestro en Ciberseguridad

# PRESENTACIÓN

## Bienvenidos a la Autónoma

### DR. ENRIQUE VÁSQUEZ HUAMÁN Rector

En la actualidad la seguridad informática es una preocupación cada vez mayor para las organizaciones, es por ello, que cada vez se requieren más profesionales especializados capaces de anticipar, prevenir, detectar y responder amenazas cibernéticas para garantizar la protección de los datos y sistemas. En ese sentido, la Escuela de Posgrado de la Universidad Autónoma del Perú asume un rol protagónico en la formación de profesionales que contribuyan a proteger los sistemas de información y las infraestructuras tecnológicas de organizaciones públicas y privadas. Con la Maestría en Ciberseguridad, la Autónoma busca que sus estudiantes sean capaces de diseñar y aplicar soluciones de seguridad efectivas para proteger los activos de información de las organizaciones.



## ¿POR QUÉ ESTUDIAR NUESTRA MAESTRÍA 100% VIRTUAL?

1

Conseguirás tu grado de maestro desde cualquier parte del país o del mundo

2

Aprenderás de manera autónoma y con acompañamiento de tu docente

3

Accederás a clases en vivo con tu docente (síncronas)

4

Accederás permanentemente a contenidos y materiales para una mejor organización de tu tiempo

5

Interactuarás con una plataforma digital diseñada para tu aprendizaje

# PERFIL DEL ESTUDIANTE



❖ **Pensamiento sistémico:**  
Posee una visión integral para desarrollar propuestas de solución a la problemática del contexto



❖ **Capacidad crítica para transferir el conocimiento académico a las diferentes situaciones reales acorde a las necesidades**



❖ **Comunicación:** Procesa información de textos escritos y se expresa con coherencia



❖ **Investigación:** Desarrolla investigaciones y realiza innovaciones en su práctica profesional con creatividad



❖ **Competencias digitales:** demuestra el manejo de herramientas digitales orientadas al aprendizaje



❖ **Ética y responsabilidad social:** Comprende la responsabilidad ética de las tareas y proyectos de responsabilidad social asumidas contribuyendo con la transformación de la sociedad

## CAMPO LABORAL

- ❖ **Gerente de Ciberseguridad:** Lidera equipos multidisciplinarios para diseñar y supervisar estrategias de ciberseguridad, asegurando la protección de activos digitales y la alineación con los objetivos estratégicos de la organización.
- ❖ **Consultor en Ciberseguridad:** Asesora a empresas e instituciones en la identificación y mitigación de riesgos cibernéticos, implementación de políticas de seguridad y cumplimiento normativo.
- ❖ **Especialista en Respuesta a Incidentes de Seguridad:** Identifica, evalúa y gestiona incidentes cibernéticos, minimizando el impacto y garantizando la continuidad del negocio mediante planes de respuesta y recuperación.
- ❖ **Analista de Amenazas Cibernéticas:** Recopila y analiza información de inteligencia de amenazas para identificar patrones de ataque y desarrollar estrategias defensivas proactivas.





# METODOLOGÍA

## 2EXA

### EXPLORA

Promovemos el aprendizaje activo mediante lluvia de ideas, videos enriquecidos, lecturas, preguntas motivadoras y retos educativos, fomentando la reflexión y el intercambio de perspectivas con tus pares

### EXPERIMENTA

Fomentamos la interacción entre estudiantes y docentes, aplicando el contenido de estudio en situaciones propias del entorno laboral, con actividades grupales o individuales, uso de simuladores y recursos digitales

### APLICA

Impulsamos el aprendizaje autónomo y la reflexión sobre las formas de aprender, por medio de acciones de metacognición, resúmenes, actividades de divulgación y evaluación que consolidan el conocimiento y permiten aplicar el aprendizaje en situaciones reales y cercanas a tu ejercicio profesional

## RECURSOS PARA TUS CLASES



#### ❖ Sesión ONLINE vía Zoom con el docente

El docente imparte en vivo la sesión de clases y podrás en ella intercambiar experiencias y realizar consultas



#### ❖ Lecturas digitales

Archivos en formato digital especialmente preparados para enriquecer la clase y las actividades de aprendizaje



#### ❖ Podcast

Grabaciones de audio para explicar y ayudar a desarrollar las actividades y uso de los servicios en la universidad



#### ❖ Enlaces web

Información relevante seleccionada para complementar el aprendizaje



#### ❖ Bases de datos

Herramientas de acceso exclusivo para reforzar el aprendizaje de todas las materias impartidas como ebooks, revistas especializadas, ecosistemas de aprendizaje y audiolibros



#### ❖ Recursos de Autoaprendizaje

Para consolidar el conocimiento de lo aprendido y de los recursos disponibles de la clase



#### ❖ Tutoriales

Videos multimedia creados exclusivamente para aprender de manera sencilla el tema de la clase

# NUESTROS BENEFICIOS



## ❖ Plana Docente de Primer Nivel

Con destacada experiencia profesional en el campo de la Ciberseguridad, así como en la enseñanza en entornos virtuales de aprendizaje



## ❖ Misión Académica Internacional

Tendrás la opción de realizar una visita académica al extranjero



## ❖ Horarios Flexibles

Frecuencia de clases síncronas semanales y asíncronas según tu disponibilidad



## ❖ Clases Internacionales

Podrás interactuar en clases virtuales con docentes extranjeros



## ❖ Certificación

Especialízate mientras obtienes tu grado de maestro y obtén dos certificaciones



## ❖ Programa de Empleabilidad

Participarás en actividades y talleres que potenciarán tus competencias empleables



## ❖ Acompañamiento Personalizado

Contarás con acompañamiento permanente para asegurar que alcances tus objetivos académicos y profesionales de manera efectiva



## ❖ Conversatorios con Expertos

Se realizarán encuentros con expertos nacionales e internacionales de destacadas empresas o entidades para que aprendas de sus experiencias



## ❖ Seminario Internacional

Participarás de un seminario internacional al año para ampliar tus conocimientos en el área



## ❖ Cursos y Taller de Nivelación

Tendrás a tu disposición el taller de normas APA y los cursos de nivelación en Estadística, Contabilidad y Finanzas y Habilidades para la Investigación



**Maestría respaldada  
por SUNEDU**







**SUNEDU**  
SUPERINTENDENCIA  
NACIONAL DE EDUCACIÓN  
SUPERIOR UNIVERSITARIA





# MAPA CURRICULAR

 **Duración:** 15 meses





## CICLO I





-  Fundamentos de Ciberseguridad
-  Seguridad en Redes, Sistemas en la Nube y Dispositivos Móviles
-  Detección y Respuesta a Incidentes
-  Investigación I

## CICLO II

-  Gestión de Riesgos y Cumplimiento en Ciberseguridad
-  Gobierno y Políticas en Ciberseguridad
-  Inteligencia de Amenazas y Seguridad
-  Investigación II

## CICLO III

-  Criptografía, Protección de Datos y Privacidad
-  Arquitectura y Diseño de Seguridad
-  Electivo
-  Investigación III

Investigación  Identificar y proteger los activos empresariales  Detectar y responder a evento de ciberseguridad  Recuperación de las capacidades empresariales impactadas en un evento de ciberseguridad 

### Nota:

- La Universidad Autónoma del Perú, se reserva la atribución de realizar cambios que mejoren esta malla curricular en función de los avances tecnológicos, tendencias del sector y mercado laboral.

- Para la obtención del grado de maestro de acuerdo a la Ley Universitaria, deberá acreditar el dominio del idioma extranjero o lengua nativa. De no contar con el dominio del idioma, podrá desarrollar la experiencia académica del idioma extranjero en el Centro de Idiomas de la misma universidad o en instituciones externas; este último podrá ser validado a través de un proceso de convalidación (examen de capacidad o presentación del certificado)

- La Universidad Autónoma se reserva el derecho de modificaciones en plana docente y cierre de aulas por no cumplir con el mínimo de estudiantes matriculados requeridos por la institución.

## CERTIFICACIONES PROGRESIVAS



Certificación en Seguridad de Redes y Sistemas (ciclo I)



Certificación en Gestión de Riesgos y Cumplimiento (ciclo II)



### ❖ Fundamentos de Ciberseguridad

Adquirirás una comprensión integral de las amenazas cibernéticas actuales, junto con las medidas y estrategias fundamentales para sistemas, datos e infraestructuras en un entorno digital. Esta asignatura te proporcionará las bases necesarias para estudiar y aplicar de manera efectiva la ciberseguridad en contextos técnicos y de gestión.

### ❖ Seguridad en Redes, Sistemas en la Nube y Dispositivos Móviles

Adquirirás una profunda comprensión de los desafíos y vulnerabilidades en redes, sistemas, servicios en la nube y dispositivos móviles, y aprenderás a aplicar soluciones efectivas para mitigar riesgos. Este curso te proporcionará los conocimientos técnicos y estratégicos necesarios para proteger activos digitales en diversos entornos.

### ❖ Detección y Respuesta a Incidentes

Aprenderás a detectar actividades maliciosas, evaluar su impacto y aplicar estrategias de mitigación. Esta asignatura te enseñará técnicas avanzadas de análisis de datos y te proporcionará conocimientos prácticos para gestionar incidentes en entornos tecnológicos complejos.

### ❖ Investigación I

Obtendrás conocimiento sobre las lógicas de indagación, así como sobre las estrategias y técnicas propias de la investigación cualitativa. Para ello, se proponen dos líneas de trabajo complementarias que te permitirán abordar el material teórico y metodológico en estrecha conexión con investigaciones empíricas.



## CICLO II



### ❖ **Gestión de Riesgos y Cumplimiento en Ciberseguridad**

Adquirirá conocimientos fundamentales sobre el análisis de riesgos, el diseño de planos de mitigación y el establecimiento de políticas de cumplimiento. Este curso te ofrece una visión integral de la gestión de riesgos y el aseguramiento del cumplimiento en el ámbito de la ciberseguridad.

### ❖ **Gobierno y Políticas en Ciberseguridad**

Obtendrás una comprensión profunda de cómo las políticas y regulaciones influyen en las prácticas de seguridad cibernética, y aprenderás a establecer un marco de gobernanza sólido para mitigar riesgos. Este curso abarca los aspectos legales, éticos y estratégicos necesarios para gestionar de manera efectiva la ciberseguridad en organizaciones y gobiernos.

### ❖ **Inteligencia de Amenazas y Seguridad**

Aprenderás a identificar y prevenir ataques cibernéticos interpretando indicadores de compromiso y tendencias. Este curso te enseñará cómo recopilar datos, analizar riesgos y aplicar soluciones defensivas basadas en información de amenazas.

### ❖ **Investigación II**

Ejecutarás tu trabajo de investigación de especialidad. Este proceso incluye desarrollar aspectos clave como el inicio de la ejecución, el seguimiento y control de los objetivos del trabajo de investigación, y la evaluación del cumplimiento.

## CICLO III



### ❖ **Criptografía, Protección de Datos y Privacidad**

Obtendrás conocimientos profundos sobre algoritmos criptográficos, técnicas de cifrado y medidas para garantizar la confidencialidad y la integridad de la información. Esta asignatura aborda tanto los aspectos técnicos como los legales relacionados con la protección de datos y la privacidad.

### ❖ **Arquitectura y Diseño de Seguridad**

Aprenderás a integrar medidas de seguridad en la arquitectura y el diseño, teniendo en cuenta aspectos como la autenticación, la autorización y el control de acceso. Esta asignatura te proporcionará conocimientos técnicos y prácticos para garantizar la robustez de los sistemas de seguridad desde su diseño inicial.

### ❖ **Electivo**

Desarrollarás tus capacidades para gestionar el aprendizaje, analizar problemas y llevar a cabo investigaciones científicas, generando soluciones a problemas sociales y fomentando una actitud.

### ❖ **Investigación III**

Desarrollarás un informe final de tu trabajo de investigación en ingeniería en ciencia de datos, que incluirá los siguientes contenidos: redacción de la introducción del informe, la teoría relacionada y la metodología, los resultados y las conclusiones, así como la exposición y defensa del informe.

# PLANA DOCENTE

---



❖ **Marlon  
Avalos**

Ingeniero de Sistemas titulado y colegiado, con maestrías en Dirección de Tecnologías de Información (ESAN) y en Ingeniería de Sistemas con mención en Gerencia de Sistemas de Información (UPN). Especialista en ciberseguridad con múltiples certificaciones internacionales, incluyendo ISO 27001 Lead Auditor, ITIL v4, y Ciberseguridad bajo el enfoque de ISO 27032. Cuenta con amplia experiencia como supervisor y gestor de incidentes de ciberseguridad en empresas como Neosecure y CANVIA, liderando proyectos estratégicos, elaboración de políticas y procesos, y capacitación en normas como ISO 27001. Ha trabajado en la gestión de incidentes para organizaciones de alto perfil como el BCP y BBVA, y ha desarrollado herramientas y soluciones tecnológicas avanzadas para mitigar riesgos de seguridad. Docente universitario en cursos relacionados con ciberseguridad, transformación digital y auditoría de sistemas, ha sido ponente en eventos nacionales sobre ciberseguridad, destacando su participación en temas relacionados con la protección de datos en tiempos de crisis global. Su liderazgo en ciberseguridad y su capacidad para integrar normas internacionales con soluciones prácticas lo posicionan como un referente en la industria tecnológica.



❖ **Rafael  
Bocanegra**

Ingeniero en Computación y Sistemas por la USMP, con una Maestría en Gerencia y Administración y un MBA Gerencial por la UPC, además de certificaciones internacionales en ISO 27001, ISO 27032 Lead Cybersecurity Manager y COBIT. Especialista en ciberseguridad con más de 15 años de experiencia liderando proyectos estratégicos en gestión de riesgos, protección de datos y seguridad de la información en el sector bancario e industrial. Ha implementado marcos normativos de seguridad, diseñado estrategias de ciberseguridad corporativa y liderado iniciativas como la adecuación a la Ley de Protección de Datos Personales y la implementación de modelos de seguridad gestionada (CyberSOC). Su trayectoria incluye roles de liderazgo en el Grupo Romero y el Banco de la Nación, donde estableció estándares avanzados de seguridad cibernética. Mentor en la Universidad Peruana Alemana y organizador de eventos destacados como el CISOSummit Perú, su enfoque en cultura de seguridad y formación profesional lo posiciona como un referente en el fortalecimiento de la ciberseguridad en América Latina.



❖ **Juan  
Chávez**

Ingeniero Informático y Magíster en Ciberdefensa por la Universidad de Alcalá de Henares, con más de 25 años de experiencia en tecnologías de la información, ciberseguridad y ciencia de datos aplicados a la defensa nacional. Oficial de la Fuerza Aérea del Perú, ha liderado proyectos estratégicos en ciberespacio y telemática, incluyendo la implementación de sistemas de seguridad avanzada y el fortalecimiento de capacidades defensivas cibernéticas. Su experiencia en ciberseguridad incluye certificaciones en Ethical Hacking, formación en normas internacionales de seguridad de la información (ISO 27001) y liderazgo en iniciativas de protección de infraestructuras críticas. Ha ocupado roles clave en la gestión de operaciones de ciberseguridad y en la dirección de proyectos tecnológicos para el sector defensa. Docente y formador de talento en instituciones académicas y militares, contribuye al desarrollo de profesionales especializados en ciberseguridad. Su trayectoria y liderazgo lo posicionan como un referente en la implementación de estrategias tecnológicas y de seguridad en entornos críticos.



**Enrique  
Dobbartin**

Magíster en Ciberseguridad por IMF Smart Education (España) y Oficial de la Fuerza Aérea del Perú, con más de 15 años de experiencia en tecnologías de la información, incluyendo 10 dedicados exclusivamente a la ciberseguridad y ciberdefensa. Actualmente se desempeña como Jefe de Operaciones Ciberespaciales en el Centro de Operaciones en el Ciberespacio de la FAP, liderando equipos especializados en gestión de incidentes, caza de amenazas y evaluación de riesgos. Cuenta con certificaciones internacionales en ISO 27001, ISO 27032 Lead Cybersecurity Manager, y CISSP, además de una sólida formación en hacking ético, seguridad en sistemas Linux y gestión de riesgos cibernéticos. Ha liderado proyectos estratégicos para la implementación de sistemas de seguridad y la protección de infraestructuras críticas en el ámbito nacional. Con una destacada trayectoria académica y profesional, ha diseñado y ejecutado estrategias operativas para la ciberdefensa en el sector público. Su experiencia y liderazgo lo posicionan como un referente en la protección y desarrollo de capacidades defensivas en el ciberespacio.



**Pedro  
Montalván**

Ingeniero Industrial con un Máster en Ciberdefensa por la Universidad de Alcalá de Henares y un MBA por la Universidad Católica de Murcia, además de certificaciones internacionales como CISSP, CISM, ISO 27001 Lead Implementer, ISO 27032 Lead Cybersecurity Manager, e ISO 27035 Incident Response Manager. Posee más de 10 años de experiencia en ciberseguridad, liderando proyectos en instituciones públicas y privadas, así como en eventos internacionales como los Juegos Panamericanos Lima 2019. Ha implementado controles avanzados de ciberseguridad, diseñado SOC's (Centros de Operaciones de Seguridad) y creado políticas de gestión de seguridad de la información basadas en estándares como ISO 27001 e ISO 27032. Su experiencia incluye la dirección de equipos técnicos para proteger infraestructuras críticas y garantizar la continuidad del negocio mediante estrategias de ciberdefensa. Docente en universidades de prestigio, es experto en la formación de profesionales en ciberseguridad y gestión de riesgos. Reconocido por su enfoque en innovación y liderazgo estratégico, contribuye al fortalecimiento de la ciberseguridad en América Latina.



**Manuel  
Pereyra**

Ingeniero de Computación y Sistemas por la USMP, con un Doctorado en Gestión Pública y Gobernabilidad (UCV) y Maestrías en Ingeniería de Sistemas (UNFV) y Gobierno y Políticas Públicas (PUCP). Especialista en ciberseguridad con más de 30 años de experiencia en la Fuerza Aérea del Perú, liderando proyectos tecnológicos y estrategias en ciberdefensa. Cuenta con experiencia en técnicas avanzadas de Ethical Hacking y auditorías de seguridad informática, además de la implementación de sistemas de gestión de seguridad de la información. Ha sido Coordinador del Programa de Gestión Estratégica del Poder Aeroespacial y Ciberespacio, enfocándose en formar profesionales en el ámbito cibernético. También ha asesorado y evaluado investigaciones relacionadas con ciberseguridad y gestión tecnológica. Como docente universitario en reconocidas instituciones nacionales e internacionales, ha dictado cursos de ingeniería, ciberseguridad y gestión tecnológica. Su liderazgo académico y profesional lo posiciona como un referente en la integración de tecnología y seguridad en el ámbito público y privado.

# MISIÓN ACADÉMICA INTERNACIONAL\* (Opcional)



**Colombia**

❖ Universidad Católica de Colombia



\*La Universidad Autónoma del Perú se reserva el derecho de modificar las sedes de las misiones académicas y de cancelar viajes en caso de no alcanzar el número mínimo de inscriptos necesarios.

## INFORMACIÓN



**Inicio  
de clases**

❖ 24 de mayo del 2025



**Horario  
frecuencia semanal**

❖ Sábados de 4:00 p. m. a 8:20 p. m.

## INVERSIÓN

~~Inscripción regular: S/ 150~~

**Inscripción promocional**

**S/ 50**

### Financiamiento

❖ Financia la maestría directamente con nosotros sin pagar intereses

Inversión	Matrícula	N.º Matrícula	Cuotas	N.º Cuotas
Inversión Regular	S/ 350	3	S/ 850	18
Tarifa Promocional	S/ 350	3	S/ 640	18





**Autónoma**  
Universidad Autónoma del Perú

**POSGRADO**

#### Informes

WhatsApp: 934 836 484

E-mail: [posgrado@autonoma.pe](mailto:posgrado@autonoma.pe)

Panamericana Sur Km. 16.3, Villa El Salvador