ESCUELA DE POSGRADO UNI

MAESTRÍA EN GOBIERNO Y GESTIÓN DE LA SEGURIDAD DIGITAL

Escuela de Posgrado UNI

DISEÑADO PARA QUE TE CONVIERTAS EN EL LÍDER DEL FUTURO

PRESENTACIÓN

La Maestría ofrece una especialización de alto nivel para los profesionales de las áreas de seguridad digital y ciberdefensa, seguridad de la información y ciberseguridad, que deseen desarrollar conocimientos, aptitudes y habilidades para la planificación, organización, liderazgo, operación y monitoreo de estrategias de seguridad digital, a escala de toda la organización. La Maestría comprende cursos a distancia y dos cursos de seminario de tesis.

DIRIGIDO A

Profesionales que deseen adquirir conocimientos en la gestión de la seguridad digital, liderazgo estratégico y ciberdefensa, orientados a ocupar roles como CISO, oficial de seguridad digital o jefe de ciberseguridad en las organizaciones.

OBJETIVO

Formar profesionales capaces de asumir roles ejecutivos y directivos en el ámbito de la seguridad digital, desarrollando habilidades estratégicas y técnicas para gestionar y liderar la protección digital.

ESCUELA DE POSGRADO UNI

PLAN CURRICULAR

CICLO I

- **Gobierno Corporativo, Defensa Nacional y Seguridad Digital**
  GSD01 — *4 créditos*
- **Tecnologías Emergentes , Innovación, Transformación Digital y Seguridad Digital**
  GSD02 — *4 créditos*
- **Proyecto de Investigación I**
  GSD03 — *4 créditos*

CICLO II

- **Normatividad y Metodologías de Seguridad Digital**
  GSD04 — *4 créditos*
- **Arquitectura y Diseño de la Seguridad Digital**
  GSD05 — *4 créditos*
- **Seguridad Digital en la Cadena de Suministros**
  GSD06 — *4 créditos*

CICLO III

- **Seguridad Digital en la Industria 4.0 y Activos Críticos Nacionales**
  GSD07 — *4 créditos*
- **Gobierno y Gestión de TI y Seguridad Digital**
  GSD08 — *4 créditos*
- **Proyecto de Investigación II**
  GSD09 — *4 créditos*

CICLO IV

- **Gobierno, Roles y Responsabilidades, Procesos en la Seguridad Digital**
  GSD10 — *4 créditos*
- **Ciberprotección y Ciberdefensa**
  GSD11 — *4 créditos*
- **Gestión de Incidentes, Resiliencia y Gestión de la Continuidad del Negocio**
  GSD12 — *4 créditos*

HORARIO

MIÉRCOLES
7:00 pm a 10:00 pm

SÁBADO
8:00 am a 11:00 am y
11:30 am a 2:30 pm

ESCUELA DE POSGRADO UNI

CICLO I

GSD01

Gobierno Corporativo, Defensa Nacional y Seguridad Digital

Comprende conceptos de gobierno corporativo basado en los esquemas de evaluación de controles internos y gestión del riesgo (COSO), ERM y Basilea, así como la relación entre la seguridad digital y la ciberdefensa. Asimismo, se tratarán tendencias respecto a regulaciones de Fin Tech, Open Finance, entre otros. Es de naturaleza teórico-práctica. Se desarrolla un proyecto de aprendizaje por exploración de casos.

GSD02

Tecnologías Emergentes , Innovación, Transformación Digital y Seguridad Digital

Desarrolla en el participante el conocimiento sobre las tecnologías digitales emergentes y vigentes, así como modelos de innovación, transformación digital y como las oportunidades que nos ofrecen dichas tecnologías y modelos nos exponen riesgos de seguridad digital, los que requieren ser gestionados adecuadamente, a fin que la implementación de dichas tecnologías/prácticas cumplan con los objetivos del negocio. Es de naturaleza teórico-práctica. Se desarrolla un proyecto de aprendizaje por exploración de casos.

GSD03

Proyecto de Investigación I

Del área Formativa de Investigación de carácter práctico. Se propone que los participantes desarrollen un **plan de trabajo de investigación** relacionado a dirección y gobierno de la seguridad digital, que sean retos que aporten soluciones a los problemas identificados. El tema es individual y también puede realizarse en grupo de hasta tres estudiantes. Al final del curso deben presentar su plan de investigación.

CICLO II

GSD04

Normatividad y Metodologías de Seguridad Digital

Desarrolla en el participante la capacidad de conocer y dominar los marcos nacionales e internacionales de ciberseguridad, tanto a escala de gestión como de marcos de control. Asimismo, las metodologías para el inventario y la clasificación de inventarios de activos de información y/o evaluación de riesgos, así como la aplicación a escala de los productos, procesos, cambios importantes y servicios de terceros. Es de naturaleza teórico-práctica. Se desarrolla un proyecto de aprendizaje por exploración de casos.

GSD05

Arquitectura y Diseño de la Seguridad Digital

Desarrolla los principales marcos de arquitectura de seguridad digital y las tecnologías de seguridad digital disponibles para establecer las medidas de protección. Es de naturaleza teórico-práctica. Se desarrolla un proyecto de arquitectura de seguridad digital para una empresa.

GSD06

Seguridad Digital en la Cadena de Suministros

Desarrolla los aspectos de seguridad digital en la cadena de suministros los cuales comprenden desde la confección del bien o servicio contratado hasta la entrega de estos a los clientes. Dichas medidas se apoyan en las prácticas internacionales relacionadas con estos temas. Es de naturaleza teórico-práctica. Se desarrolla un proyecto de aprendizaje por exploración de casos.

CICLO III

GSD07

Seguridad Digital en la Industria 4.0 y Activos Críticos Nacionales

Desarrolla la capacidad de conocer las medidas de la seguridad digital en la industria 4.0, así como en la infraestructura crítica del transporte, energía, petróleo, agua y salud. Es de naturaleza teórico-práctica. Se desarrolla un proyecto de aprendizaje por exploración de casos.

GSD08

Gobierno y Gestión de TI y Seguridad Digital

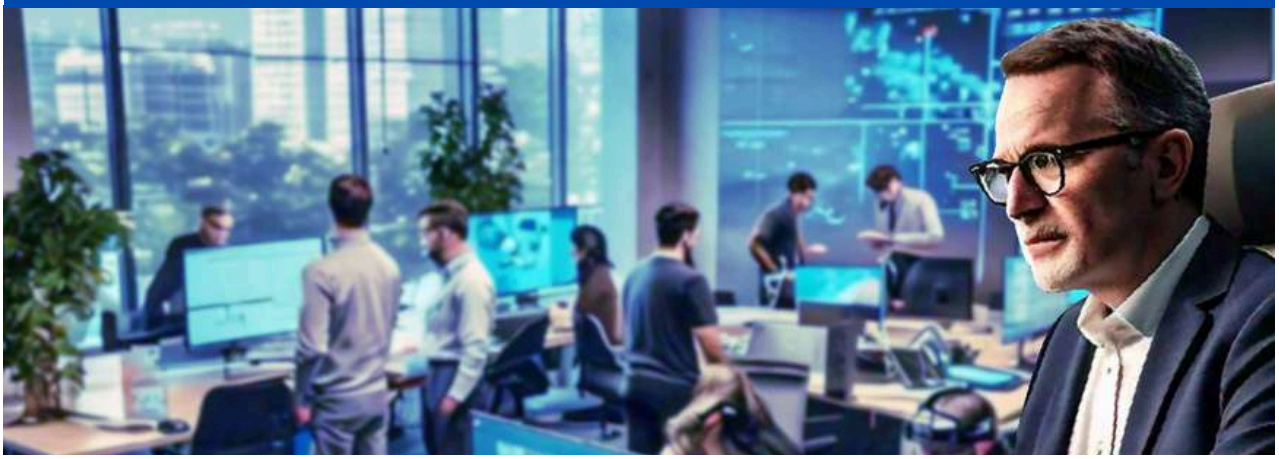
Desarrolla aspectos importantes de la gestión de las tecnologías de información que impactan la seguridad digital, entre ellos el gobierno de TI y gobierno de datos, la gestión de proyectos y los marcos de procesos de TI a escala de desarrollo y la operación de TI, así como los marcos ágiles y de innovación. Es de naturaleza teórico-práctica. Se desarrolla un proyecto de aprendizaje por exploración de casos.

GSD09

Proyecto de Investigación II

Del área Formativa de Investigación de carácter práctico. Se propone que los participantes desarrollen un **trabajo de investigación relacionado** a dirección y gobierno de la seguridad digital que sean retos que aporten soluciones a los problemas identificados. El tema es individual y puede realizarse en grupo de hasta tres estudiantes. Al final del curso deben presentar su plan de investigación.

CICLO IV



GSD10

Gobierno, Roles y Responsabilidades, Procesos en la Seguridad Digital

Desarrolla el concepto de las 3 líneas de defensa sobre las cuales se decantan los modelos de gobierno, roles y responsabilidades, los marcos de procesos de gestión de la seguridad digital en las organizaciones. Es de naturaleza teórico-práctica. Se desarrolla un proyecto de aprendizaje por exploración de casos.

GSD11

Ciberprotección y Ciberdefensa

Desarrolla en el participante los conocimientos y habilidades para comprender los aspectos nacionales de la seguridad digital focalizados en la ciber protección y ciberdefensa. Es de naturaleza teórico-práctica. Se desarrolla un proyecto de aprendizaje por exploración de casos.

GSD12

Gestión de Incidentes, Resiliencia y Gestión de la Continuidad del Negocio

Desarrolla en el participante los conocimientos de la gestión de incidentes de seguridad digital y como se relaciona con los mecanismos de resiliencia y continuidad de negocio, así como el rol del cybersec como unidad organizacional y primera barrera para detectar, detener y responder a los ciberataques. Es de naturaleza teórico-práctica. Se desarrolla un proyecto de aprendizaje por exploración de casos.

PROCEDIMIENTO DIGITAL

1. Registrar los datos de contacto del postulante por medio del formulario virtual.

2. Para iniciar el proceso de admisión, se emitirá la Orden de Pago por derecho de postulación.

3. Una vez que el postulante realiza el pago por el derecho de postulación, se le enviará un correo donde se indica cuál es la documentación requerida a presentar.

4. Para presentar la documentación se facilitará al postulante un formulario virtual.

5. Se evaluará el currículo del postulante, la problemática de investigación presentada (una página) además de una entrevista personal virtual.

6. Posterior a la entrevista, se comunicará al postulante los resultados de la evaluación por correo.

7. Los postulantes admitidos pagarán la matrícula y la cuota inicial.

CRONOGRAMA DE ESTUDIOS

2025		2026	
Ciclo I	Ciclo II	Ciclo III	Ciclo IV

*Cronograma referencial

INVERSIÓN

Derecho de postulación (una sola vez)	4 matrículas (una por ciclo)	16 cuotas (una por mes)
S/ 300.00	S/ 300.00	S/ 1,000.00

Cada nuevo ciclo se paga la matrícula más la primera cuota.
Para matricularse no se debe tener cuotas pendientes de pago.

CRONOGRAMA DE PAGOS

Primer ciclo

1era CUOTA + MATRÍCULA	2da CUOTA + MATRÍCULA	3era CUOTA + MATRÍCULA	4ta CUOTA + MATRÍCULA
S/ 1, 300.00	S/ 1,000.00	S/ 1,000.00	S/ 1,000.00

Segundo ciclo

1era CUOTA + MATRÍCULA	2da CUOTA + MATRÍCULA	3era CUOTA + MATRÍCULA	4ta CUOTA + MATRÍCULA
S/ 1, 300.00	S/ 1,000.00	S/ 1,000.00	S/ 1,000.00

Tercer ciclo

1era CUOTA + MATRÍCULA	2da CUOTA + MATRÍCULA	3era CUOTA + MATRÍCULA	4ta CUOTA + MATRÍCULA
S/ 1, 300.00	S/ 1,000.00	S/ 1,000.00	S/ 1,000.00

Cuarto ciclo

1era CUOTA + MATRÍCULA	2da CUOTA + MATRÍCULA	3era CUOTA + MATRÍCULA	4ta CUOTA + MATRÍCULA
S/ 1, 300.00	S/ 1,000.00	S/ 1,000.00	S/ 1,000.00

PREGUNTAS FRECUENTES

GENERALES

1. ¿Cuáles son los requisitos para postular?

- Grado de bachiller.
- CV
- DNI *(ambos lados).*
- Dos cartas de presentación *(pueden ser docentes, jefes o compañeros de trabajo).*
- Declaración jurada.
- Ficha de datos personales.
- Solicitud dirigida al Director de la Escuela de Posgrado.
- Problemática de investigación en una página.
- Recibo de pago del derecho de postulación.

  Los formularios de los documentos solicitados serán enviados al correo del postulante una vez realizado el pago del derecho de postulación.

2. ¿Puedo aprobar la maestría sin asistir a clases?

No, solo es justificable hasta el **30%** de inasistencia. La maestría desarrolla habilidades en los estudiantes; por lo que se requiere la participación activa en las clases, hacer trabajos en equipo, debates e interacción con los docentes y estudiantes.

COSTOS

3. ¿Cuál es el costo total de la maestría?

Derecho de postulación (una sola vez)	4 matrículas (una por ciclo)	16 cuotas (una por mes)	COSTO TOTAL
S/ 300.00	S/ 300.00	S/ 1,000.00	S/ 17,500.00

4. ¿Cuánto cuesta el Derecho de Grado?

El costo actual del derecho de grado es **S/ 4,375.00** *(Según TUPA 2025, sujeto a cambios)*

5. ¿Hay algún descuento sobre el costo de la maestría?

No, este costo es aproximadamente un **30%** inferior al costo vigente de las maestrías UNI.

6. ¿Por qué se pagan juntas la matrícula y la cuota inicial?

Para garantizar el pago a los docentes.

7. ¿Cuándo se deben hacer los pagos de la segunda, tercera y cuarta cuota?

El primer día del mes según se muestra en el cronograma de pagos.

8. ¿Cuáles son las formas de pago?

- Por medio de los canales de pago del **BCP.** *Se entregará guía de pago.*
- Por medio de los canales de pago del **Scotiabank.** *Se entregará guía de pago.*
- Pago en línea a través de la Plataforma **Niubiz** con la cual se acepta todo tipo de tarjetas. *Se entregará guía de pago.*
- Ir de manera presencial a la caja UNI donde se acepta todo tipo de tarjetas. *(No se acepta efectivo).*

9. ¿Puedo iniciar un nuevo ciclo teniendo cuotas pendientes de pago de otro ciclo?

No, para iniciar un nuevo ciclo; además de haber pagado todas las cuotas del ciclo anterior, pagará la matrícula más la primera cuota del ciclo que comienza.

10. ¿Se puede solicitar la devolución del derecho de postulación?

No hay devolución.

11. ¿Hay devolución por la matrícula y la cuota inicial?

No hay devolución.

PROBLEMÁTICA DE INVESTIGACIÓN

12. ¿Se presenta un examen escrito de admisión?

No se presenta examen escrito de admisión. La evaluación para la admisión del postulante se hace mediante el **análisis de CV, problemática de investigación y entrevista.**

13. ¿Qué temas se tratan en la problemática de investigación?

Los temas pueden estar relacionados con la organización donde esté trabajando, estrategias, negocios y tecnología.

14. ¿La problemática de investigación es individual?

Sí, es individual.

15. ¿Cuántas páginas debe tener la problemática de investigación?

Una página.

INICIO

16. Cuando soy admitido ¿Cuál es el siguiente paso?

El asistente administrativo entrega la orden de pago de la matrícula y la primera cuota que se abona para comenzar el ciclo.

17. Si he sido admitido en la maestría, ¿En qué momento se considera que empiezo el ciclo?

El estudiante podrá asistir a clases únicamente después de haber realizado el pago de la matrícula y la cuota inicial.

LA MAESTRÍA

18. ¿Cuántos créditos tiene la maestría?

48 créditos.

19. ¿Cuántos créditos tiene cada ciclo?

Cada ciclo tiene 12 créditos.

20. ¿A cuántas horas equivale un crédito?

A 16 horas académicas *(45 minutos).*

21. ¿Esta maestría es solo para ingenieros?

No, es válida para profesionales de cualquier especialidad.

22. ¿Los estudiantes de la maestría tienen código y correo UNI?

Sí, a todos los estudiantes de la maestría se les genera el código y correo UNI.

23. ¿La maestría cuenta con una plataforma digital de enseñanza?

Sí, se cuenta con la **Plataforma NEO** y las clases se realizan mediante **ZOOM.**

24. ¿Los estudiantes tienen acceso a las clases grabadas?

Sí, los estudiantes tienen acceso a las clases grabadas a través de la **Plataforma NEO.**

25. ¿La maestría tiene la aprobación de la SUNEDU?

La maestría ha sido creada por la UNI e informada a SUNEDU. Ya no es necesario que SUNEDU apruebe la creación de las maestrías (leer Ley No 31520).
Cuando los egresados obtengan el grado de maestro, este será comunicado a la SUNEDU. Se podrá registrar el grado de maestro en la SUNEDU.

26. ¿Cuál es el nombre del grado de esta maestría?

Maestro en Gobierno y Gestión de la Seguridad Digital.

IDIOMAS

27. ¿Es necesario saber otro idioma para obtención del grado de maestro?

Sí, es necesario saber otro idioma a nivel intermedio. Se aconseja el inglés.
Se le solicita un certificado que acredite su conocimiento del idioma inglés a nivel intermedio. Se debe presentar una copia notariada del certificado de inglés cuando el alumno esté en proceso de sustentación de su tesis.

28. ¿Qué certificados de inglés acepta la Escuela de Posgrado?

Los certificados de conocimiento del idioma inglés son aceptados por la Escuela de Posgrado de la UNI independientemente de su fecha de emisión o la institución certificadora que los haya otorgado.

29. ¿La Escuela de Posgrado UNI brinda cursos de inglés?

No. Sin embargo, el Centro de Idiomas UNI brinda un curso de inglés específicamente para estudiantes de la maestría y doctorado el cual le permitirá certificar su dominio del idioma inglés.

También cuenta con un examen de competencia en el cual usted puede validar su conocimiento del idioma inglés.

PROGRAMA DE INGLÉS

El programa de Inglés para Posgrado Online del Centro de Idiomas UNI está dirigido a maestrandos o doctorandos que necesiten continuar sus trámites para la obtención del grado.

Si no dispone de una constancia o certificado que acredite su conocimiento del idioma inglés, puede tomar el Examen de Competencia por medio del Centro de Idiomas UNI o llevar el curso que consta de 6 Módulos.

EXAMEN DE COMPETENCIA

- Nota mínima es 16 para cumplir con el nivel intermedio.
- Online. Consta de 2 partes:
  - Entrevista
  - Grammar
    Listening
    Reading
- El costo es de S/200.00 (*)
  El alumno puede programar con el centro de idiomas en cualquier momento.

  Certificado S/ 150

CURSO

- Clases sincrónicas Online
  Para que se abra un salón debe haber mínimo 15 alumnos.
  - 3 meses
  - 6 módulos
  - 144 horas
- El costo es de S/1,200.00 (*) en dos cuotas: una al iniciar y la otra al acabar el tercer módulo

  Certificado S/ 120

Sobre el certificado del curso

Se emite como nivel intermedio a nombre de la Universidad, hace mención a la Ley 30220. No tiene caducidad en la Universidad.

Para inscripciones o consultas contactar con el Centro de Idiomas UNI
+51 981 603 043

**Costos a enero del 2025, sujeto a actualización.*

DOCENTES

Víctor Simich

Coordinador de la Maestría

Ingeniero de Sistemas por la Universidad Nacional de Ingeniería. MBA-TEC por UNIR, Diplomado de Seguridad Informática por TEC de Monterrey, Sistemas Integrados de Banca Electrónica por ACI, Digital Transformation – Boston Consunlting Group y SingularityU Custom Program en Singularity University. Creador y Director de la Maestría en Gobierno y Gestión de Seguridad Digital de la UNI. Ejerció durante 15 años labores de CISO en empresas como Interbank, Innovacción-Grupo ACP, Visanet

Félix Jiménez

Ingeniero Industrial de la Universidad Nacional de Ingeniería (UNI), Doctor en Ingeniería de Sistemas por la Universidad Nacional Federico Villarreal, con estudios en Doctorado en Administración de Negocios (DBA) en CENTRUM por la Pontificia Universidad Católica del Perú, Maestría en Ciberseguridad y Ciberdefensa por el Centro de Altos Estudios Nacionales. Posee diplomados en Inteligencia de Negocios, Gerencia de Proyectos, Ciberseguridad y Ciberdefensa, así como Dirección Estratégica de Sistemas. Miembro de Comisión Nacional de Transformación Digital, Innovación e Inteligencia Artificial del Colegio de Ingenieros del Perú, Miembro IEEE, con más de 25 años de experiencia de TI en instituciones públicas y privadas, como Gerente de TI, Redes y Telecomunicaciones y Ciberseguridad, Consultor en Gobierno y Transformación Digital en la PCM, RENIEC, SUNARP, Ministerio Publico y Ministerio del Interior. Reconocido por la UNI y el CIP como uno de los profesionales más destacados en su campo. Especialista en Sistemas de Identificación Biométrica y Ciberseguridad. Actualmente docente en la Escuela de Posgrado de la Universidad Nacional de Ingeniería en Gobierno Digital y Ciberseguridad.

Percy Gonzales

Profesional con amplia experiencia en el ámbito militar y académico, con múltiples diplomas y títulos avanzados en gestión de seguridad, inteligencia y planeamiento estratégico, incluyendo un Magíster en Ciencias Militares y un Doctorado en Desarrollo y Seguridad Estratégica. Destacado por sus estudios de especialización en diversas áreas como operaciones de paz, análisis de informaciones y planeamiento operacional conjunto. Habla inglés y portugués a nivel avanzado. Ha recibido varios méritos, como la Espada de Honor y la Medalla Académica del Ejército, además de felicitaciones por contribuciones en investigación y desarrollo. Ha ejercido roles académicos como docente en instituciones militares y civiles, y ha ocupado cargos administrativos como subdirector de la Escuela de Comunicaciones del Ejército. Recientemente, ha sido docente en la Universidad Nacional Mayor de San Marcos y en la Escuela de Posgrado de la Policía Nacional del Perú.

DOCENTES

Juan Chuquivilca

Ingeniero de Sistemas, Oficial del Ejército Peruano del grado de Teniente Coronel, desempeñándose actualmente como Jefe de Operaciones de Ciberdefensa del Ejército y Director de Innovación y Desarrollo Tecnológico en SITECOM, con experiencia en Seguridad Informática, Inteligencia Estratégica, Innovación Tecnológica, Auditoria de Sistemas, Gestión y Gobierno de TI. Maestro y egresado de diferentes Maestrías y Doctorados, actualmente cursando la Maestría en Dirección de Tecnologías de la Información en ESAN. Desempeño profesional en entidades Públicas y Privadas. Catedrático en universidades en pre y post grado, y actualmente integrando proyectos de innovación tecnológica en SITECOM y en desarrollo el libro “El lado oscuro de la Transformación Digital”. Con amplia predisposición para brindar soluciones, con iniciativa, innovación, trabajo en equipo y compromiso con los objetivos organizacionales

Laura Johanson

MBA en Centrum Católica PUCP y Economista Titulado por la Universidad Nacional de Trujillo, Programa de Directores de Empresas en la Universidad del Pacífico, RIsk Management for Corporate Leaders en Harvard Business School y Digital Transformation en MIT y Columbia Business Schoool ha ocupado cargo gerenciales en Operaciones, ,Riesgo Operacional, Continuidad de negocio, Seguridad de Información, Gerencia de Riesgos, en importantes empresas del sector como Caja Trujillo, Fondo Mivivienda, BNP PARIBAS CARDIF SEGUROS, Grupo Monge, FINTECH Crece Capital. Asimismo, ha trabajado como Supervisor principal de Riesgos en la Superintendencia de Banco y Seguros y como Auditor principal en Grant Thorton. Gerente de Riesgo Operacional y Continuidad de Negocio en Banco Pichincha.

Manuel Caldas

Máster en Ingeniería de Seguridad Informática por la Universidad Tecnológica del Perú (UTP), Bachiller en Administración de Empresas por la Universidad Científica del Sur, Cuenta con diversas certificaciones como PMP, ITIL Expert en sus diferentes niveles por APMG y EXIN, ISO27001, ISO27032, ISO38500 por PECB, Certificate of Cloud Security Knowledge (CCSK) por Cloud Security Alliance. Cuenta con más de 30 años de experiencia profesional habiendo trabajdo en importantes empresas como COSAPI DATA, AirON Group, Adexus Perú, Axcess Financial Perú así como ha realizado actividad de consultoría en instituciones públicas y privadas. Docente en diversas universidades de nuestro país, entre ellas la docente en la carrera de ciberseguridad de la Universidad Nacional de Ingeniería. En la actualidad es IT Security Architect en MIbanco.

Rafael García-Calderón

Máster en Finanzas de la Universidad del Pacífico y Bachiller de Ingeniería Industrial de la Universidad de Lima. Cuenta con amplia experiencia en puestos ejecutivos y directivos en Logística, Operaciones, Estrategia, Gestión de Riesgos no Financieros y Riesgo Operacional en importantes empresas del sector público y privado. Ha sido presidente del Comité de Riesgo Operacional de ASBANC. Es Socio Fundador y CEO de Luken Business Consulting brindando su experiencia en Gestión de Riesgos y Cumplimiento, Gestión de Riesgo Operacional, Gestión de Continuidad de Negocio, Gestión de Seguridad de Información, Ley de Protección de Datos Personales, Gestión de Prevención de Lavado de Activos y Terrorismo. Además, Rafael dirige nuestra práctica de Aseguramiento de Ingresos y Reducción de Pérdidas para empresas de Servicios.

DOCENTES

Danilo Pomalaza

Ingeniero de Sistemas UNI, con MBA en ESAN. Ha tenido experiencias en el sector financiero trabajando en empresas líderes del sector como Especialista de Seguridad de Información en el BBVA, Especialista de Seguridad de Información en Interbank y Subgerente de Arquitectura de TI en el Banco de Crédito del Perú (BCP). En la actualidad es jefe de Arquitecturas de Ciberseguridad en Minera Antamina. Es Docente de Postgrado en Ciberseguridad en el Centro de Altos Estudios Nacionales y en la Universidad Tecnológica del Perú (UTP).

Joseph Valenzuela

Maestría en Ciencias de Tecnologías de Información concentrado en Ciberseguridad de la Universidad de Texas en San Antonio (USA), Bachiller de Ingeniería de Sistemas de la Universidad Nacional de Ingeniería (PERÚ), Certificado Profesional de Seguridad en Sistemas de Información (CISSP), Implementador Líder ISO/IEC 27001. Experiencia laboral en el sector privado y público como Futurex-USA, VIsanet Perú., Procesos MC -Perú, Banco Ripley, Financiera Compartamos, Ministerio de Desarrollo e Inclusión Social, PromPerú, Ministerio de Cultura entre otros. Consultor en temas de Ciberseguridad.

Leslye Sihuay

Master of Public Affairs (MPA) por la Universidad de California, Berkeley, Master of Science (MSc) Corporate and Financial Risk Management por la Universidad de Sussex. Diploma, Cambridge FinTech and Regulatory Innovation Fintech innovation and regulation por la Universidad de Cambridge, Bachiller de Ingeniería de Sistemas por la Universidad Nacional de Ingeniería. Con más de 15 años de experiencia en el sector financiero, se especializa en la combinación de políticas, finanzas digitales, gestión de riesgos tecnológicos y cumplimiento normativo para navegar por el cambiante panorama financiero. Ha desempeñado funciones clave en el Foro Económico Mundial, CITRIS Policy Lab de la Universidad de California - Berkeley y la Superintendencia de Bancos, Seguros y AFP. Además, ha colaborado con organizaciones globales en diversos foros, incluyendo grupos de trabajo de la Alianza del Pacifico, Alliance for Financial Inclusion y el Banco Mundial. En la actualidad es Especialista Senior en SupTech en Cambridge SupTech Lab, una organización global que impulsa la innovación en supervisión tecnológica, donde lidera colaboraciones internacionales y asistencia técnica con autoridades financieras del mundo para acelerar la innovación a través políticas y tecnología de vanguardia.

Julio Núñez

Doctor en Derecho y Ciencia Política por la Universidad Nacional Mayor de San Marcos (2017) y Magister en Derecho Empresarial por la Universidad de Lima (1997). Abogado por la Universidad de Lima (1988), cuenta con formación en Derecho Informático y Ciberdelitos, participando en programas del Ilustre Colegio de Abogados de Lima, Harvard e INDECOPI, OEA, y APEC. Publicó extensamente sobre identidad digital y derecho informático. Tiene experiencia docente en la UPC, UNMSM, Universidad de Lima, y Universidad ESAN, enseñando derecho informático y regulación de servicios públicos. En RENIEC, fue Especialista Legal en Protección de Datos Personales y consultor en TMB Asesores y Consultores SCRL. Además, asesoró tesis y coordinó académicamente en la Universidad de Lima, participando en comités de autoevaluación y como auditor interno de ISO 9000. Es miembro de diversas asociaciones relacionadas con la informática jurídica.

DOCENTES

Martín Blas

Ingeniero de Sistemas (UNI) colegiado (CIP), con Maestría en Administración de Negocios (MBA-ESAN) y Diplomado Internacional en Gestión de Riesgos y Administración de la Seguridad. Ejecutivo con más de 25 años de experiencia profesional en proyectos de Seguridad de la Información, Continuidad del Negocio, Tecnologías de Información, Protección de Datos Personales, Gestión de Riesgos Tecnológicos y Auditoria de Sistemas, en los sectores Banca, Finanzas, Energía, Salud y Gobierno. Con certificaciones internacionales en CISM, CRISC, CDPSE, ISO 27001 Lead Auditor, ISO 22301 Senior Lead Implementer. Cargos relevantes como Gerente de Sistemas, Oficial de Seguridad de Información (CISO), Coordinador de Continuidad del Negocio, Oficial de Datos Personales, Oficial de Gobierno de Datos y Auditor de Sistemas. Catedrático universitario e instructor en Centros de Capacitación Especializada.

Yuri Aldoradin

Maestría en Gestión Pública en la Universidad Nacional de Seúl (Corea del Sur), bachiller en Ingeniería de Sistemas por la Universidad Nacional de Ingeniería (UNI), bachiller en Administración de Empresas por la Universidad de Piura (UDEP); con estudios en España, Corea del Sur, Estados Unidos y Japón en gobierno digital, ciberseguridad y transformación digital. Actualmente especialista en regulación digital y coordinador del Centro de Cooperación en Gobierno Digital Perú-Corea (DGCC). Más de diez (10) años de experiencia en diseño y regulación de políticas en materia de gobierno digital, seguridad digital y transformación digital. Expositor sobre aplicación de la regulación digital en el sector público.

Carlos Soto

Ingeniero de Sistemas por la Universidad Nacional de Ingeniería y Magíster en Administración Estratégica de Empresas (MBA) por Centrum PUCP. Docente en programas de posgrado, pregrado y educación ejecutiva. Experto en innovación, transformación digital y ciberseguridad, con más de 14 años de experiencia en gestión de productos financieros, canales digitales y seguridad de la información. Ha desempeñado roles como Gerente de Innovación y Transformación Digital, Líder de Proyectos Digitales e Innovación, y Subgerente de Seguridad de la Información en organizaciones como Caja Trujillo, Banco Falabella, Mibanco y EY. Especializado en Innovación Estratégica por ESADE Business School, en Transformación Digital e Innovación por IE Business School y certificaciones CISA, CISM, CRISC e ISO 27001 Lead Implementer.

Henry Gómez

Ingeniero Electrónico por la Universidad Nacional de Ingeniería, Magister en Administración de Empresas (MBA) por ESAN y Master en Marketing Science por ESIC; con múltiples certificaciones de la industria LPT, CEH, ECSA, CHFI, ISO27K, ITIL RCV, IBM. Actualmente vendedor técnico senior de soluciones de ciberseguridad de IBM para Perú, Ecuador y Bolivia; habiendo antes desempeñado roles de vendedor para Perú y Ecuador, y arquitecto de servicios LA, siempre de seguridad en IBM durante los últimos 10 años. Con 18+ años de experiencia en ciberseguridad asociada a ventas, preventa, diseños de arquitecturas y costeo, consultorías, SOC, outsourcing, liderazgo de operaciones, análisis de vulnerabilidades, PCI, ISO27K e ISO20K; en grandes proyectos para múltiples empresas en Perú y otros países de la región.

Luis Gastulo

Magíster en Dirección de Tecnologías de la Información por la Universidad LaSalle y la Universidad Ramon Llull, España, con más de 15 años de experiencia en ciberseguridad, gestión de riesgos y liderazgo de proyectos estratégicos en el sector financiero, gubernamental y privado. Actualmente es Jefe de Seguridad de la Información en el Banco Central de Reserva del Perú, donde lidera equipos de seguridad ofensiva y defensiva, además de la implementación de SGSI (ISO 27001) y estrategias de protección de datos sensibles. Docente universitario desde 2012 en Seguridad Informática y Forense Digital, ha participado en el Cybersecurity Summer Bootcamp de la Universidad de León y la OEA. Posee certificaciones internacionales como CEH, CHFI, ISO 27001, ISO 27032 y COBIT 5. Reconocido por su liderazgo y visión estratégica, ha desarrollado controles avanzados de ciberseguridad en entornos híbridos y multinube. Su perfil combina excelencia académica, experiencia docente y certificaciones para formar profesionales con alto impacto en el sector.

Edgar Ramos Palomino

El Dr. Edgar Ramos es profesor en la Universidad Peruana de Ciencias Aplicadas (UPC) y en la Universidad Nacional de Ingeniería (UNI), donde imparte cursos de tesis e investigación en ingeniería industrial. Es ingeniero industrial por la UNI, con una maestría en Administración por la Universidad del Pacífico (UP) y un Ph.D. por la Universidad Nacional Mayor de San Marcos (UNMSM). Tiene más de 20 años de experiencia en operaciones, servicios, logística y gestión de la cadena de suministro en la industria peruana. Sus publicaciones internacionales abordan estos temas, con más de 20 artículos en revistas indexadas en Q1 en Scopus y Web of Science, además de más de 40 artículos en conferencias internacionales.

Angélica Castillo

Ingeniera Informática con Magíster en Ciencias (UNI) y Master en Ciberseguridad (España). Cuenta con más de 24 años de experiencia profesional en transformación digital, ciberseguridad, ciberinteligencia, inteligencia artificial y big data. Ha ocupado cargos como Gerente de Tecnologías de la Información en diversas instituciones del gobierno peruano, incluyendo la Presidencia del Consejo de Ministros y el Ministerio de Relaciones Exteriores. Ha sido consultora TIC para el Banco Interamericano de Desarrollo y el Banco Mundial. Actualmente, es Consultora en Ciberseguridad en Telefónica Tech y en el Banco Mundial. Ha sido becada en diversas universidades internacionales y ha recibido múltiples premios, destacando los premios internacionales "Cybersecurity Woman of the World – 2024" y "Cybersecurity Woman of the Year – 2023". Además, ha sido reconocida como "Top Women in Cybersecurity" por la organización WOMCY.