



UNIVERSIDAD
NACIONAL
DE INGENIERÍA

ESCUELA DE
POSGRADO

ADMISIÓN
hasta el
11 de
octubre



*Análisis de casos reales
con profesionales de la
empresa privada, del
Estado y las FF.AA.*

MAESTRÍA

**EN GOBIERNO Y GESTIÓN
DE LA SEGURIDAD DIGITAL**

OBJETIVOS EDUCACIONALES

La Maestría en Gobierno y Gestión de la Seguridad Digital, de tipo *Especialización*, ofrece una educación de alto nivel para los profesionales en áreas de seguridad digital y ciberdefensa, seguridad de la información y ciberseguridad, que deseen desarrollar aptitudes, conocimientos 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.

PERFIL DEL GRADUADO Y/O EGRESADO

El perfil de un egresado de la Maestría en Gobierno y Gestión de la Seguridad Digital es de un profesional altamente calificado, con los conocimientos de gestión de la seguridad digital a escala organizacional (CISO), técnico, de procesos y de gestión del talento. Se desempeñará en posiciones estratégicas y de dirección de seguridad digital y ciberdefensa en las organizaciones, como oficial de seguridad y confianza digital, jefe de Seguridad Informática/ciberseguridad, entre otros.

Se espera que un egresado de la Maestría en Gobierno y Gestión de Seguridad Digital esté preparado para desarrollar roles ejecutivos y directivos en el campo de la seguridad digital; entre ellas, se destacan las siguientes características:

Capacidad de desarrollar medidas de seguridad digital en la cadena de suministros.

Explorar las tecnologías emergentes y metodologías de innovación y su impacto en la seguridad digital.

Capacidad para diseñar la estructura organizacional, roles y responsabilidades en seguridad digital.

Capacidad de diseñar los mecanismos de respuesta a incidentes.

Capacidad para implementar planes estratégicos y operativos de seguridad digital.

Capacidad para definir una arquitectura de seguridad digital.

Conocer los aspectos de gestión de TI y su relación con la seguridad digital.

Capacidad para diseñar, definir y desplegar las metodologías de seguridad digital.

Habilidades de comunicación efectiva y capacidad para presentar los resultados de la investigación de manera concisa.



UNIVERSIDAD
NACIONAL
DE INGENIERÍA

ESCUELA DE
POSGRADO

 Teléfono central:
481-1070, Anexo 5223

 Escuela de Posgrado UNI

 979 038 521

PLAN CURRICULAR



■ Sumillas de cursos en la siguiente página.

CRONOGRAMA DE ESTUDIOS



HORARIO



Viernes de 7:00 pm a 10:00 pm
Sábado de 8:00 am a 11:00 am y de 11:30 am a 2:30 pm



UNIVERSIDAD NACIONAL DE INGENIERÍA

ESCUELA DE POSGRADO

Teléfono central: 481-1070, Anexo 5223

Escuela de Posgrado UNI

979 038 521

ESTRUCTURA CURRICULAR / CURSOS

CICLO I

➔ GSD-01 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 refuerzo.

➔ GSD-02 TECNOLOGÍAS EMERGENTES, INNOVACIÓN TRANSFORMACIÓN DIGITAL Y SEGURIDAD DIGITAL

Desarrolla en el estudiante 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 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 refuerzo.

➔ GSD-09 PROYECTO DE INVESTIGACIÓN I

Del área Formativa de Investigación de carácter analítica-descriptiva y práctica. Se propone que los estudiantes 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

➔ GSD-04 NORMATIVIDAD Y METODOLOGÍAS DE SEGURIDAD DIGITAL

Desarrolla en el estudiante la capacidad de conocer y dominar los marcos nacionales e internacionales de ciberseguridad, tanto a escala de gestión como de marcos de control. Así como las metodologías para el inventario y la clasificación de inventarios de activos de información y evaluación de riesgos y como ellos se aplican a nivel de los productos, procesos, cambios importantes y servicios de terceros. Es de naturaleza teórico-práctica. Se desarrolla un proyecto de aprendizaje por refuerzo.



➤ **GSD-05 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.

➤ **GSD-06 SEGURIDAD DIGITAL EN LA CADENA DE SUMINISTROS**

Desarrolla los aspectos de seguridad digital en la cadena de suministros los cuales pueden comprender desde la confección del bien o servicios contratados hasta la entrega de estos a los clientes. Dichas medidas se apoyan en las prácticas internacionales más importantes en este tema. Es de naturaleza teórico-práctica. Se desarrolla un proyecto de aprendizaje por refuerzo.

CICLO III

➤ **GSD-07 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 como transporte, energía, petróleo, agua y salud. Es de naturaleza teórico-práctica. Se desarrolla un proyecto de aprendizaje por refuerzo.

➤ **GSD-08 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 refuerzo.

➤ **GSD-12 PROYECTO DE INVESTIGACIÓN II**

Del área Formativa de Investigación de carácter analítica-descriptiva y práctica. Se propone que los estudiantes desarrollen un proyecto 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 puede realizarse en grupo de hasta tres estudiantes. Al final del curso deben presentar su plan de investigación.



CICLO IV

➔ GSD-03 GOBIERNO, ROLES Y RESPONSABILIDADES, PROCESOS Y 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 refuerzo.

➔ GSD-10 CIBERPROTECCIÓN Y CIBERDEFENSA

Desarrolla en el estudiante los conocimientos y habilidades para entender 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 refuerzo.

➔ GSD-11 GESTIÓN DE INCIDENTES, RESILIENCIA Y GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Desarrolla en el estudiante 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 esfuerzo.



INICIO

CICLO I

➔ **Inicio:**
Lunes 21 de octubre del 2024



UNIVERSIDAD
NACIONAL
DE INGENIERÍA

ESCUELA DE
POSGRADO

☎ Teléfono central:
481-1070, Anexo 5223

f Escuela de Posgrado UNI

📞 979 038 521

INVERSIÓN

Derecho de postulación
(una sola vez).

S/ 300.00

4 matrículas
(una por ciclo)

S/ 300.00

16 cuotas
(una por mes)

S/ 1,000.00

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

CRONOGRAMA DE PAGOS

CICLO I

OCT 2024 - ENE 2025

Hasta 20 de septiembre 2024	1 de nov 2024	1 de dic 2024	1 de ene 2025
S/ 1,300.00	S/ 1,000.00	S/ 1,000.00	S/ 1,000.00

CICLO II

MAR-JUN 2025

Hasta 07 de febrero 2025	1 de abr 2025	1 de may 2025	1 de jun 2025
S/ 1,300.00	S/ 1,000.00	S/ 1,000.00	S/ 1,000.00

CICLO III

AGO-NOV 2025

Hasta 07 de julio 2025	1 de sep 2025	1 de oct 2025	1 de nov 2025
S/ 1,300.00	S/ 1,000.00	S/ 1,000.00	S/ 1,000.00

CICLO IV

ENE-ABR 2026

Hasta 07 de diciembre 2025	1 de feb 2026	1 de mar 2026	1 de abr 2026
S/ 1,300.00	S/ 1,000.00	S/ 1,000.00	S/ 1,000.00

PROCEDIMIENTO

Inscripción

1 Registro de datos del postulante por medio de formulario.

Pago por derecho de postulación

2 Emisión de orden de pago por derecho de postulación.

3 Pago por derecho de postulación.

Envío de documentos

4 Envío de correo al postulante con la documentación y formularios requeridos.

5 El postulante entrega la documentación y formularios requeridos.

Evaluación

6 Evaluación del postulante mediante el CV, Problemática de Investigación (una página) y entrevista.

Notificación y matrícula

7 Comunicación del resultado de la entrevista al postulante.

8 El postulante admitido abona la matrícula más la cuota inicial.



UNIVERSIDAD
NACIONAL
DE INGENIERÍA

ESCUELA DE
POSGRADO



Teléfono central:
481-1070, Anexo 5223



Escuela de Posgrado UNI



979 038 521

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).

S/ 300.00

4 matrículas
(una por ciclo)

S/ 300.00

16 cuotas
(una por mes)

S/ 1,000.00

Costo total

S/ 17,500.00

Estos costos no incluyen derecho de grado.

4 ¿Cuánto cuesta el Derecho de Grado?

El costo actual del derecho de grado es S/ 4,375.00

5 ¿Cuál es el cronograma de pagos?

Derecho de Postulación de la Maestría: S/ 300.00

CICLO I OCT 2024 - ENE 2025

Hasta 20 de
septiembre 2024

1 de nov
2024

1 de dic
2024

1 de ene
2025

S/ 1,300.00

S/ 1,000.00

S/ 1,000.00

S/ 1,000.00

CICLO II MAR-JUN 2025

Hasta 07 de
febrero 2025

1 de abr
2025

1 de may
2025

1 de jun
2025

S/ 1,300.00

S/ 1,000.00

S/ 1,000.00

S/ 1,000.00

CICLO III AGO-NOV 2025

Hasta 07 de
julio 2025

1 de sep
2025

1 de oct
2025

1 de nov
2025

S/ 1,300.00

S/ 1,000.00

S/ 1,000.00

S/ 1,000.00

CICLO IV ENE-ABR 2026

Hasta 07 de
diciembre 2025

1 de feb
2026

1 de mar
2026

1 de abr
2026

S/ 1,300.00

S/ 1,000.00

S/ 1,000.00

S/ 1,000.00

6 ¿Hay algún descuento sobre el costo de la maestría?

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

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

Para garantizar el pago a los docentes.

8 ¿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.



UNIVERSIDAD
NACIONAL
DE INGENIERÍA

ESCUELA DE
POSGRADO



Teléfono central:
481-1070, Anexo 5223



Escuela de Posgrado UNI



979 038 521

9 ¿Cuáles son los requisitos para postular?

- 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).*

10 ¿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.

11 ¿Se puede solicitar la devolución del derecho de admisión?

Solo es devuelto a los postulantes que se retiren antes de realizar la entrevista para la admisión; en ese caso, se devolverá lo pagado menos un **15%** por gastos administrativos.

12 ¿Hay devolución por la matrícula y la cuota inicial?

Si el estudiante pagó la matrícula más la primera cuota y se retira de la maestría antes de haber iniciado el ciclo, se le devolverá lo pagado menos un **15%** por gastos administrativos. Si se retira luego de haber comenzado el ciclo, no se hará la devolución.

PROBLEMÁTICA DE INVESTIGACIÓN

13 ¿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.**

14 ¿Qué temas se tratan en la problemática de investigación?

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

15 ¿La problemática de investigación es individual?

Sí, es individual.

16 ¿Cuántas páginas debe tener la problemática de investigación?

Una página.

INICIO

17 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.

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

Una vez que haya pagado la matrícula y la cuota inicial.

LA MAESTRÍA

19 ¿Qué duración tiene la maestría?

19 meses.

20 ¿Cuántos créditos tiene la maestría?

48 créditos.

21 ¿Cuántos créditos tiene cada ciclo?

Cada ciclo tiene 12 créditos.

22 ¿A cuántas horas equivale un crédito?

A 16 horas académicas (45 minutos).



23 ¿Esta maestría es solo para ingenieros?

No, es válida para profesionales de cualquier especialidad.

24 ¿La modalidad de la maestría es 100% digital?

Sí.

25 ¿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.

26 ¿La maestría cuenta con una plataforma digital de enseñanza?

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

27 ¿Los estudiantes tienen acceso a las clases grabadas?

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

28 ¿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.

29 ¿Cuál es el nombre del grado de esta maestría?

Maestro en Gobierno y Gestión de la Seguridad Digital.

30 ¿Se menciona en el diploma que la maestría es online?

No se menciona.

31 ¿Es necesario saber otro idioma para graduarse de maestro?

Sí, es necesario saber otro idioma a nivel intermedio. Se aconseja el inglés.



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 Consulting 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, Innovación-Grupo ACP, Visanet Perú y Banco Pichincha y 5 años como Gerente de Consultoría en Seguridad de Información y Ciberseguridad. Ha sido 3 veces miembro ganador de premios de creatividad empresarial por innovaciones en el sector bancario, y ha liderado el mayor proyecto de seguridad de información de protección de datos de tarjeta en nuestro país. Fue director del Instituto de Software de la UNI, Gerente de Startup UNI y ha sido miembro del equipo de Competisofit, proyecto de mejora de procesos de software para PYME, el cual desde el 2013 es la norma ISO29110. Gerente de Consultoría en Luken Business Consulting, empresa especializada en Gestión de Riesgos No financieros, entre ellos Seguridad de Información y Ciberseguridad.



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 Público 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.



UNIVERSIDAD
NACIONAL
DE INGENIERÍA

ESCUELA DE
POSGRADO

Teléfono central:
481-1070, Anexo 5223

Escuela de Posgrado UNI

979 038 521



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, Auditoría 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 School 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 Thornton. 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 trabajado en importantes empresas como COSAPI DATA, AirON Group, Adexus Perú, Axcoss Financiera 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.





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, Vlsanet 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 Pacífico, 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.





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 Auditoría 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 Aldoradín

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.

