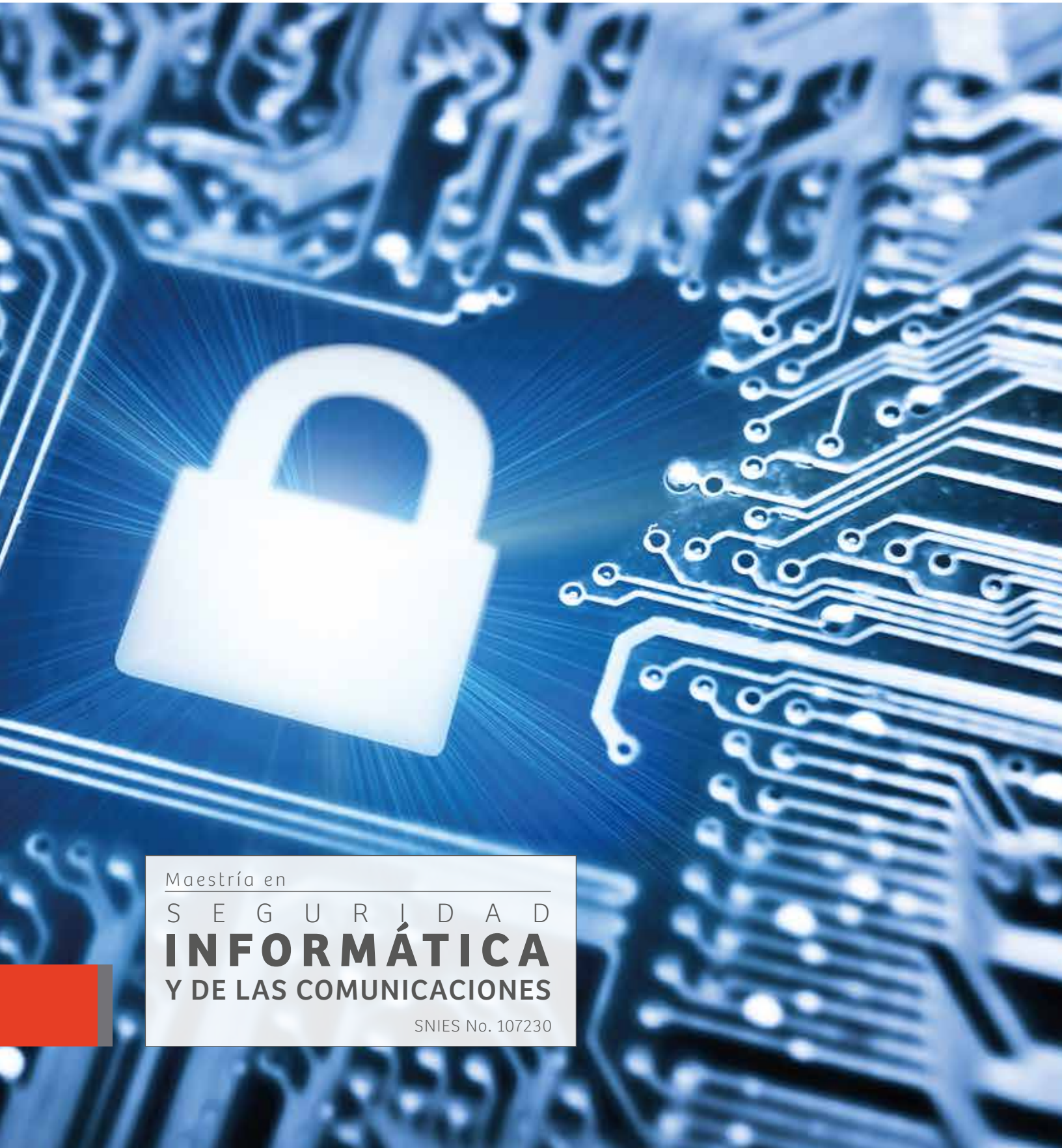
UNIVERSIDAD Piloto DE COLOMBIA



Maestría en

SEGURIDAD

# INFORMÁTICA

## Y DE LAS COMUNICACIONES

SNIES No. 107230

Maestría en

# SEGURIDAD INFORMÁTICA Y DE LAS COMUNICACIONES

Conozca, identifique e implemente con eficacia y eficiencia las principales técnicas de protección frente a ataques y amenazas en los sistemas operativos, las redes de comunicaciones, el software de aplicación, los entornos Web y las bases de datos. Adquiera las competencias para la gestión, análisis de riesgos y auditoría de la seguridad de las tecnologías de la información y de las comunicaciones en cualquier organización.

Resolución de Registro Calificado N°. 12576 del 03/08/2018; vigencia por 7 años. SNIES No. 107230 del 13/08/2018.
Título: Magíster en Seguridad informática y de las comunicaciones.
Nivel: Maestría. | Metodología: Presencial. | Sede Bogotá.

## Información general

Duración
**4 semestres, 2 años.**

Horario
**Viernes de 6:00 a 10:00 p.m. y sábados de 7:00 a.m. a 1:00 p.m.**

Metodología y sedes
**Presencial**
**Sede Bogotá**

Créditos
**43 créditos**

La Maestría tiene como objeto la formación integral y de profundización en la seguridad informática y de las comunicaciones cubriendo aspectos detallados de la preparación y análisis técnico de los sistemas basados en TIC (análisis de vulnerabilidades, análisis de malware, técnicas de ataque frecuentes, análisis forense, hacking ético en redes y sistemas), combinada con una preparación completa en aspectos legales (regulación de las telecomunicaciones, privacidad, propiedad intelectual y delitos informáticos), y el currículo orientado hacia la generación de competencias necesarias para la gestión de la seguridad y el riesgo (auditoría, estándares y procesos). Proporcionando además las bases para que los estudiantes puedan afrontar con éxito los procesos de certificación personales y empresariales relacionados con la seguridad informática y de las comunicaciones que el mercado exige y que son de carácter internacional.

El Magíster en Seguridad informática y de las comunicaciones, logrará conocer, identificar e implementar con eficacia y eficiencia las principales técnicas de protección frente a ataques y amenazas en los sistemas operativos, las redes de comunicaciones, el software de aplicación, los entornos Web y las bases de datos, así como proporcionar las competencias necesarias para la gestión, análisis de riesgos y auditoría de la seguridad de las tecnologías de la información y de las comunicaciones en cualquier organización pública o privada del ámbito local, regional o mundial.

Maestría en
# SEGURIDAD INFORMÁTICA Y DE LAS COMUNICACIONES
SNIES No. 107230

## Propósitos del programa

La Maestría en Seguridad informática y de las comunicaciones tiene como propósito la formación en innovación con amplio criterio en la toma de decisiones en los temas relacionados con la seguridad informática y de las comunicaciones; con competencias en el diseño, planeación, organización, ejecución, control y evaluación, de tal forma que se puedan garantizar la integridad, confidencialidad y disponibilidad de la información y las comunicaciones dentro de las organizaciones.

Y como propósitos específicos:

- Constituir un espacio abierto para la formación posgradual que propicie el aprendizaje permanente, brindando la posibilidad de abrir la puerta al conocimiento, fomentando la movilidad social con el fin de formar profesionales que participen activamente en los sectores productivos y abiertos a las incertidumbres del mundo de los negocios digitales y el desarrollo tecnológico de las empresas.
- Propiciar espacios de investigación que permitan el diseño de proyectos relacionados con la seguridad informática y de las comunicaciones, y que a través de la utilización de tecnologías de punta le permitan ampliar sus conocimientos científicos para que pueda integrarlos a la sociedad, por medio de la implementación en las empresas, fomentando y desarrollando la investigación aplicada, científica y tecnológica.
- Contribuir a comprender, interpretar, preservar, reforzar, fomentar y difundir las mejores prácticas éticas en relación con el desarrollo tecnológico al interior de las organizaciones.

## Perfiles del programa

**Perfil de ingreso**

Las características de ingreso de los aspirantes que desean cursar la Maestría y que son factores importantes dentro del proceso de selección son las siguientes:

Ingenieros de sistemas, Ingenieros informáticos, Ingenieros electrónicos con énfasis en telecomunicaciones, Ingenieros de telecomunicaciones, Ingenieros de software, ingenieros en telemática, Ingenieros en teleinformática, Especialistas en Seguridad informática, Especialistas en Seguridad de la información, Especialistas en Telecomunicaciones, o profesionales en otras áreas que cumplan alguno(s) de los siguientes perfiles:

- Aspirantes con experiencia laboral en cargos administrativos relacionados con procesos de gestión tecnológica.
- Aspirantes con experiencia laboral en el diseño e implementación de proyectos de seguridad informática.
- Aspirantes con experiencia laboral en el diseño e implementación de proyectos de redes de comunicaciones.
- Aspirantes con un pensamiento creativo, con disposición y apertura hacia el cambio, y con una sólida actitud hacia el uso de nuevas tecnologías.
- Aspirantes proactivos para dar solución a problemas relacionados con el aseguramiento de la información.
- Aspirantes con capacidad para trabajar bajo presión y para el trabajo en equipo.
- Aspirantes con una fuerte motivación para trabajar en análisis, diseño e implementación de tecnología, de sistemas, de procesos y de servicios relacionados con la seguridad informática y redes de comunicaciones.
- Consultores e investigadores interesados en las temáticas relacionadas con la seguridad informática y las redes de comunicaciones.
- Empresarios independientes que deseen desarrollar habilidades estratégicas en el campo de la seguridad informática y las redes de comunicaciones.
- Los aspirantes deben manifestar además su interés para trabajar en análisis, diseño e implementación de tecnologías, de sistemas, de procesos y de servicios relacionados con la seguridad informática y de las comunicaciones, y su interés por generar solución a problemas relacionados con el aseguramiento de la información en los entornos TIC.

**Perfil ocupacional**

El Magíster en Seguridad informática y de las comunicaciones egresado de la Universidad Piloto de Colombia, estará altamente capacitado para vincularse activamente a la sociedad en empresas públicas y privadas de cualquier sector, ocupando algunas de las posiciones relacionadas con:

- Administrador de seguridad de la información.
- Director de proyectos tecnológicos.
- Asesor empresarial para el análisis, diseño, implementación, evaluación y gestión de procesos y servicios con alto componente tecnológico, especialmente relacionados con la seguridad de la información utilizando tecnologías informáticas y de comunicaciones.
- Director del área de Tecnologías de la información y las comunicaciones.
- Estratega de seguridad de la información.
- Docente experto en seguridad informática.
- Investigador en temática relacionadas con la seguridad informática y de las comunicaciones.

Maestría en
# SEGURIDAD INFORMÁTICA Y DE LAS COMUNICACIONES
SNIES No. 107230

**Perfil del egresado**
Magísteres con capacidades investigativas para el diseño e interpretación de modelos, estrategias y programas; capaces de dar respuesta y soluciones humanas y tecnológicas para la salvaguarda de la información, y así, mitigar los riesgos y amenazas inherentes a la informática de las organizaciones, garantizando la integridad y confidencialidad de la información y de los sistemas informáticos. Hacer realidad la investigación en el campo específico, que permita el logro de posiciones éticas y de aporte social en el desarrollo de las regiones, proyectándose a resultados innovadores que apoyen a los procesos investigativos en el marco de las necesidades sociales y empresariales.

El Magíster en Seguridad informática y de las comunicaciones egresado de la Universidad Piloto de Colombia, es un profesional con habilidades para adelantar proyectos relacionados con la seguridad informática y de las comunicaciones utilizando recursos relacionados con las TIC; así como dirigir, y asesorar recursos humanos y tecnológicos en las áreas de seguridad informática, tanto en entidades receptoras de tecnología, como en entidades fabricantes de productos y proveedoras de servicios; de carácter público o privado.

## Plan de estudios

**PLAN DE ESTUDIOS**

| Núcleos temáticos | SEMESTRE 1 | SEMESTRE 2 | SEMESTRE 3 | SEMESTRE 4 |
|---|---|---|---|---|
| **GESTIÓN DE LA SEGURIDAD Y EL RIESGO -GSEGYRIES-** | Las asignaturas correspondientes a este núcleo temático, están orientadas a las labores propias de los procesos de gestión o administración de los sistemas de gestión de la seguridad y el riesgo informático, los cuales en general están basados en los ciclos PHVA (planear, hacer, verificar y actuar) y que buscan dar el soporte metodológico, táctico y estratégico a los posteriores procesos de tipo tecnológico y que incluyen las personas, los procesos y los procedimientos organizacionales. Esta área abarca tres asignaturas que abordan los principales estándares de la industria relacionados con la gestión de la seguridad: Gestión de riesgos y continuidad, Gobierno TIC y BCP planes de continuidad del negocio. | | | |
| | **Gobierno TIC**<br>- 3 créditos - | **BCP Planes de continuidad del negocio**<br>- 3 créditos - | **Gestión de riesgos y continuidad**<br>- 1 crédito - | |
| **MODELOS FORMALES Y CRIPTOGRAFÍA -MFYCRIPT-** | La rápida evolución de la tecnología, trae consigo nuevos conceptos, retos y experiencias inimaginadas hace algunos años; a su vez esta evolución ha masificado la incorporación de las Tecnologías de la Información y las Comunicaciones (TICs) a la vida cotidiana de las personas, gracias a la penetración de redes de banda ancha, Smartphones, dispositivos móviles, entre otros, así como también producto de la modernización de organizaciones públicas y privadas que han digitalizado los servicios que prestan a sus usuarios, agilizando con ello los trámites, la productividad y la eficacia en sus usos. Esta evolución exige un alto compromiso de protección de la información por parte de las compañías que procesan, almacenan y generan información, para proteger secretos corporativos, dar cumplimiento a legislaciones internaciones y locales, y como buena práctica en la gestión de seguridad de la información.<br><br>Así las cosas, resulta de vital importancia que el estudiante conozca y domine correctamente conceptos, técnicas, aplicaciones y algoritmos de cifrado, disponibles en la industria para implementar sistemas seguros, que permitan garantizar la confidencialidad, integridad y no repudio en la información en sus diferentes estados (reposo, uso y movimiento), los temas generales a tratar son: sistemas simétricos o criptografía moderna de clave secreta, sistemas asimétricos o criptografía moderna de clave pública, integridad y autenticación, infraestructura de clave pública PKI, intercambio de claves secretas, criptografía basada en identidad, protocolos criptográficos. | | | |
| | | | **Criptografía**<br>- 3 créditos - | |

UNIVERSIDAD Piloto DE COLOMBIA

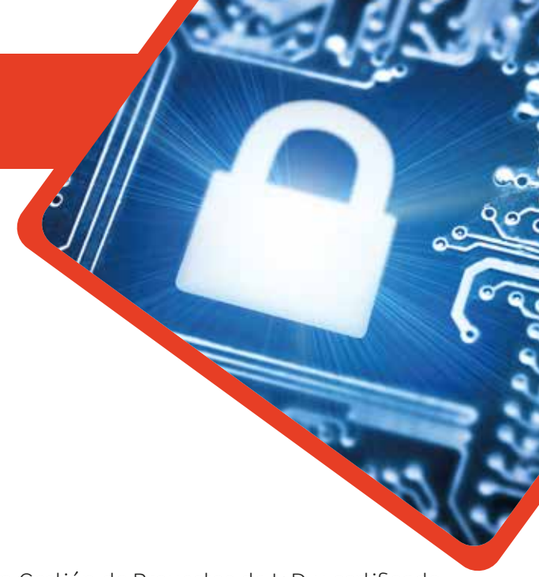
Maestría en
SEGURIDAD
# INFORMÁTICA
Y DE LAS COMUNICACIONES

SNIES No. 107230

## PLAN DE ESTUDIOS

| Núcleos temáticos | SEMESTRE 1 | SEMESTRE 2 | SEMESTRE 3 | SEMESTRE 4 |
|---|---|---|---|---|
| **SEGURIDAD DE LAS COMUNICACIONES - SEGCOM -** | Las cuatro asignaturas correspondientes a este núcleo temático, de tipo teórico-práctico, están enfocadas en el carácter técnico y operativo de la seguridad informática y de las comunicaciones, los cuales incluyen los dispositivos de comunicaciones y de seguridad, los protocolos y las redes de comunicaciones, y los sistemas operativos; elementos, todos ellos fundamentales de la continuidad operativa de las organizaciones modernas y encargados de los procesos de transmisión de la información.<br>Las asignaturas relacionadas son: Arquitecturas de seguridad, seguridad en redes de comunicaciones, pruebas de penetración a infraestructuras TIC, detección de intrusos y analítica de datos en seguridad. | | | |
| | **Seguridad en redes de comunicaciones**<br>- 3 créditos - | **Arquitecturas de seguridad**<br>- 3 créditos - | **Detección de intrusos y analítica de datos en seguridad**<br>- 3 créditos - | **Pruebas de penetración a infraestructuras TIC**<br>- 3 créditos - |
| **SOFTWARE SEGURO - SOFSEG -** | Las tres asignaturas de este núcleo temático se enfocan en el aseguramiento de todos aquellos elementos de software encargados de la generación, tratamiento y almacenamiento de la información, de forma confiable para las organizaciones. Las asignaturas relacionadas son: Seguridad en sistemas operativos y software de base, diseño de software seguro, seguridad en bases de datos. | | | |
| | **Seguridad en bases de datos**<br>- 2 créditos - | | | **Diseño de software seguro**<br>- 3 créditos - |
| | **Seguridad en sistemas operativos y software de base**<br>- 2 créditos - | | | |
| **COMPUTACIÓN FORENSE - COMFORE -** | Este núcleo temático aborda conceptos fundamentales relacionados con la recuperación de la información ante eventos fortuitos, el seguimiento a eventos fraudulentos tendientes a identificar perpetradores y las herramientas de tipo legal para el cumplimiento de las normas y para los procesos de judicialización en casos de robo o compromiso de la información.<br>Las asignaturas relacionadas con este módulo son: Manejo de incidentes, ataques e informática forense y derecho informático | | | |
| | | | **Manejo de incidentes, ataques e informática forense**<br>- 3 créditos - | |
| | | | **Derecho informático**<br>- 1 crédito - | |
| **ELECTIVAS** | Se han planteado una serie de electivas con enfoque de profundización para el tercer semestre y con enfoque de investigación para el cuarto semestre, que buscan profundizar en algunas de las temáticas tratadas en los semestres previos además de fortalecer las dinámicas propias de la investigación aplicada en el salón de clases. El objetivo de estas electivas es poder tener una oferta dinámica de temas de acuerdo con la evolución propia de la disciplina, las temáticas propuestas son: toma de decisiones en seguridad informática, evaluación, pruebas y auditorías en seguridad informática, gestión empresarial legal orientada a la seguridad informática, restos y oportunidades de innovación para las empresas, investigación del mercadeo en el entorno digital, gestión de identidades y accesos (enfoque investigación), seguridad en sistemas ciber-físicos (enfoque investigación). | | | |
| | | **Electiva profundización I**<br>- 2 créditos - | | **Electiva profundización II**<br>- 2 créditos - |
| **SEMINARIO Y PROYECTO DE GRADO** | **Seminario de tecnología ciencia y sociedad (sello unipiloto)**<br>- 1 crédito - | **Seminario de investigación I**<br>- 2 créditos - | | **Proyecto de grado profundización**<br>- 3 créditos - |
| | **11 créditos** | **10 créditos** | **11 créditos** | **11 créditos** |

Maestría en
SEGURIDAD
**INFORMÁTICA**
**Y DE LAS COMUNICACIONES**
SNIES No. 107230



## Equipo Docente

**ÁLVARO ESCOBAR ESCOBAR**
Director del programa

Magíster en Administración MBA – Universidad de la Salle. Ingeniero de Sistemas – Universidad Piloto de Colombia. Especialista en Telemática y negocios por Internet – Escuela Colombiana de Ingeniería. Especialista en Seguridad Informática – Universidad Piloto de Colombia. Formación como instructor CCNA, CCNP y CCNA Security – Universidad Nacional de Colombia sede Medellín. Consultor en temas relacionados con la seguridad informática y servicios telemáticos e Internet.

Ha sido director de Departamentos de Sistemas en empresas como Mapfre Seguros Generales de Colombia y Emermédica S.A., y como investigador en la División de investigación y desarrollo en Telecom. Catedrático y director de programas de pregrado y posgrado en las Universidades Santo Tomás, Militar Nueva Granada, Escuela de Comunicaciones del Ejército, Sergio Arboleda y Universidad Piloto de Colombia.

**CÉSAR IVÁN RODRÍGUEZ SÁNCHEZ**
Máster Universitario en Seguridad de las TIC, Universitat Autónoma de Barcelona-Universitat Rovira I Virgil-Universitat Oberta de Catalunya, con especialidad en investigación. Especialista en Construcción de Software para Redes, Universidad de los Andes. Ingeniero Electrónico, Universidad Distrital. Consultor en Seguridad de la Información y Continuidad del Negocio, Certified Information Systems Security Professional (CISSP), Certified Business Continuity Professional (CBCP), Certified Ethical Hacker (CEH), GIAC Certified Forensic Analyst (GCFA), Certified SCADA Security Architect (CSSA), certificado auditor líder ISO 27001. Experto en diseño, implementación y verificación de sistemas y controles de seguridad de la información y continuidad del negocio.

**HÉCTOR GIOVANNI CRUZ FORERO**
Master en Seguridad informática, Especialista en Gestión de Proyectos de I+D y certificado en GSEC, CEH, LA 27000, CWSP y CEI. CEO de CSIETE donde, con su experiencia de 10 años en consultoría técnica y de gestión en seguridad de la información genera, junto a su equipo de trabajo, propuestas de investigación, desarrollo e innovación en dicho tema.

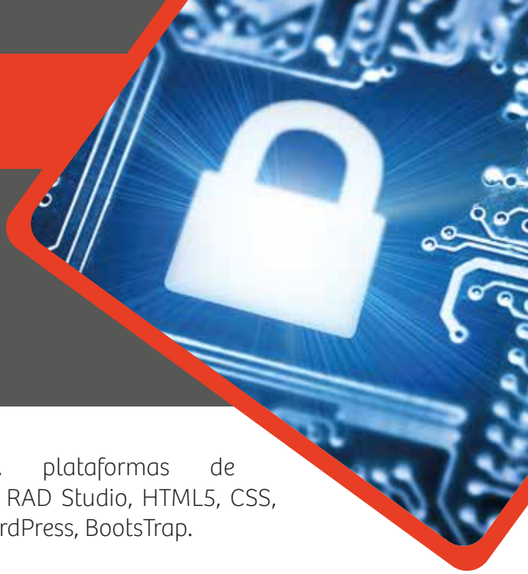
Docente en diferentes universidades, entrenador de certificaciones y cursos abiertos y en diferentes eventos. Es fundador y organizador de BSides Colombia, cofundador de Barcamp Security Edition y Busy Tone Group.

**JOHN JAIRO ECHEVERRY ARISTIZABAL**
Ingeniero de Sistemas, Especialista en Telecomunicaciones, Máster en Auditoría, Seguridad, Gobierno y Derecho de las TICS de la Universidad Autónoma de Madrid. Perito internacional en computo forense, ENCE (EncaSe Certified Examiner), ACE (Access Data Certified Examiner), consultor en seguridad de la información, certificado como auditor líder e interno en la norma 27001/2013. Consultor agencia ICITAP (International Criminal Training Assistace Program) de los Estados Unidos de Norteamérica. Instructor de las agencias OPDAT (Office of Overseas Prosecutorial Development Assitance and Training) y ATA (Antiterrorism Assistance Program).

Docente universitario en maestría y posgrados en la Universidad Piloto de Colombia, Universidad Sergio Arboleda, Universidad Libre, Universidad Cooperativa, entre otras.

**RICARDO ENRIQUE HERRERA HERNÁNDEZ**
Profesional con nueve años de experiencia en seguridad de la información y TICs, con grado de Maestría en Ingeniería de Sistemas y Computación. Experiencia en el desarrollo e implementación de Modelos de Seguridad de la Información (SGSI), gobierno de seguridad, estrategia de seguridad de la información, ciberseguridad, gestión de riesgos, cumplimiento (SOX, Circulares Superfinanciera, PCI) entre otras actividades. Habilidad para analizar, identificar y generar opciones de mejora a nivel de procesos de negocio. Cuenta con certificaciones del campo como Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Ethical Hacker (CEH) y Lead Auditor ISO/IEC 270001.

Maestría en
SEGURIDAD
INFORMÁTICA
Y DE LAS COMUNICACIONES
SNIES No. 107230



**ÁNGELA MARCELA MEJÍA FAJARDO**
Doctora en Ingeniería – Universidad de los Andes. Doctora en Telemática – Universidad Politécnica de Cataluña. Ingeniera Electrónica – Universidad Santo Tomás. Magíster en Teleinformática – Universidad Distrital Francisco José de Caldas. Conocimientos en gerencia de proyectos, diseño y configuración de redes de comunicaciones, seguridad en redes y programación en Java, entre otros. Posee valiosa experiencia en docencia e investigación, gerencia de proyectos y manejo de personal en las Universidades Santo Tomás y Militar Nueva Granada, además de desarrollo del ejercicio profesional en empresas como Concasa y Caracol Televisión.

**CARLOS ANDRÉS LOZANO GARZÓN**
Doctor en Ingeniería – Universidad de los Andes. Doctor en Tecnologías – Universidad de Girona. Ingeniero de sistemas – Universidad Nacional de Colombia. Posee valiosa experiencia en docencia e investigación, ha estado vinculado con diferentes centros educativos e investigativos, además de desarrollo del ejercicio profesional en empresas como Compensar y el Departamento Nacional de Planeación.

**ERICH SIEGERT CEREZO**
Oficial grado Coronel de la reserva activa del Ejército de Colombia, Magister EMBA Universidad Politécnica de Valencia, Universidad Sergio Arboleda, Especialista en Estado Mayor, Especialista en Seguridad y Defensa Nacional, Especialista en Telecomunicaciones e Informática, Especialista en aspectos puntuales de ciberseguridad y ciberdefensa, EMBA con homologación en negocios internacionales enfocados a ciencia y tecnología, Especialista en Educación para la informática.

**RAFAEL LEONARDO OCHOA URREGO**
Doctor en Ingeniería – Industria y Organizaciones y Magíster en Administración de la Universidad Nacional de Colombia, Máster en E-business: Telecomunicaciones y Nuevos Modelos de Negocio de la Universidad de Cantabria, España e Ingeniero de Sistemas de la Universidad Nacional de Colombia.

Su trabajo de investigación se ha concentrado en el análisis y estudio de la apropiación de innovaciones tecnológicas, complementado con el manejo de técnicas de creatividad e ideación orientadas a la solución de problemas organizacionales. Tiene experiencia en el diseño de iniciativas de comercio electrónico, así como en el planteamiento de modelos y planes de negocio para la implementación de dichas iniciativas. Ha participado y dirigido distintos proyectos de investigación relacionados con innovación y su implementación en modelos de negocio electrónicos.

**ANDRES MAURICIO MARÍN RESTREPO**
Ingeniero de Sistemas, magister en ingeniería de sistemas, Profesional con más de 10 años de experiencia en la gerencia de proyectos de desarrollo de software. Experto en PSP, TSP, CMMi, SCRUM, Scaled Agile, PMI, desarrollo de aplicaciones empresariales en JEE, arquitecturas Orientadas a Servicios, Cloud, Data Warehouse y Cobol para el ámbito financiero.

**FREDY YARNEY ROMERO MORENO**
Magister en Ciencias de la Información y las Comunicaciones, Especialista en Auditoría de Sistemas, Ingeniero de Sistemas con énfasis en Software, perfil orientado a la planificación, organización, dirección y control de procesos productivos y administrativos, habilidad para el análisis, diseño y desarrollo de soluciones tecnológicas específicas para la gestión, elaboración y control de la información. Conocimientos sólidos en: administración y procesamiento de la información, estructuración y seguimiento a través de tableros de control, seguimiento al manejo de la información en todas sus etapas (entrada, procesamiento, salida, archivo), generación de todo tipo de reportes e informes de gestión, manejo de bases de datos (SQL Server, Interbase, Sybase, MySQL, Access), plataformas de programación Visual Studio y RAD Studio, HTML5, CSS, JavaScript, SQL, PHP, MVC, WordPress, BootsTrap.

**DIANA LORENA TORO BETANCUR**
Ingeniería Electrónica, Especialista en Seguridad de la Información, Master en Auditoría, Seguridad, Gobierno y Derecho de las TIC en la Universidad Autónoma de Madrid. Certificado como primer respondiente de incidentes informáticos (CFRI) en manejo de evidencias digitales para laboratorio forense de E-Evidence, Auditora Líder ISO 27001:2013, ITIL; Auditora interna continuidad del negocio ISO 22301, Gestor de Ciberseguridad ISO 27032, Oficial de Datos personales ISO 27018, PMP (Project Management Professional), Análisis de indicadores ISO 27004:2016, Datos personales ISO 270017:2019, Mentalidad Ofensiva y Cursos de CEH (Certified Ethical Hacking), Gestión de Incidentes de seguridad y Buenas prácticas de desarrollo seguro. Experiencia laboral como directora, consultora y gerente de proyectos relacionados con seguridad y privacidad de la información, desarrollando e implementando estrategias y lineamientos para beneficio de las organizaciones, optimización de procesos e identificación de oportunidades de mejora continua.

En integración con los demás programas de la Escuela de Ingenierías TIC de la Universidad Piloto de Colombia, los siguientes docentes apoyarán actividades de investigación y generación de productos de la Maestría en Seguridad Informática y de las Comunicaciones:

**Ing. Luis Felipe Quintero, PhD.**
**Ing. Diego Fernando Bermúdez Garzón, PhD.**
**Ing. Gilberto Pedraza García, PhD.**
**Ing. Juan Carlos Navarro Beltrán, MsC.**
**Ing. Henry Arturo Bastidas Mora, MsC.**

## Requisitos para ingreso

- Formulario de inscripción diligenciado y con firma.
- 2 fotografías tipo documento 3×4 fondo blanco*.
- Fotocopia de la cédula de ciudadanía ampliada al 150% o equivalente según el país de origen del estudiante, pasaporte y visa.
- Fotocopia de carné o constancia de afiliación a EPS o SISBEN.
- Hoja de vida del solicitante.
- Fotocopia del diploma y acta de grado.
- Recibo de pago de la inscripción.
- Consignación del pago de matrícula.
  (No se aceptan fotocopias en las cuales no estén legibles firmas, folio, libro, fechas o no se entreguen en el tamaño especificado).

* Las fotografías deben ser en alta resolución, no tener más de 6 meses de antigüedad, centrada y enfocada, la cara debe aparecer mirando directamente a la cámara, no de perfil ni mirando por encima del hombro, y no debe haber sombras sobre la cara ni sobre el fondo. No se aceptarán fotos con gafas de fantasía ni con reflejos en los cristales, ni con sombrero, gorro, pañuelo o visera. En caso de traer la documentación por medio físico, se debe tener en cuenta que las fotografías deben ser impresas en papel de calidad fotográfica (no papel común).

## Descuentos y Entidades FINANCIERAS

Para mayor información sobre los **DESCUENTOS** que ofrece la Universidad a sus aspirantes y egresados:
http://www.unipiloto.edu.co/descargas/DESCUENTOS_EC.pdf

Aplican convenios con **ENTIDADES FINANCIERAS** vigentes. para mayor información:
http://www.unipiloto.edu.co/descargas/ENTIDADES-FINANCIERAS_2019.pdf

La información estará sujeta a cambios según disposiciones de cada entidad.

Acreditación institucional de alta calidad
Resolución 018115 del 27/09/2021 (4 años)

## Contáctenos


Posgrados y Educación Continuada - Universidad Piloto de Colombia
correo electrónico: asesor-20@unipiloto.edu.co
**www.unipiloto.edu.co**

**PBX: (60-1) 332 2900 Ext. 621**

Calle 45 A No. 9 - 17 | Bogotá - Colombia.


"En caso de no contar con el número mínimo de inscritos, la Universidad se reserva el derecho de apertura o aplazamiento de los cursos, seminarios, diplomados, especializaciones y maestrías. El grupo docente estará sujeto a cambios según disponibilidad de su agenda al igual que el cronograma de actividades académicas".

Para todos los efectos, la presentación al proceso de inscripción, admisión y matrícula a cada programa hace constar el conocimiento y aceptación de lo dispuesto en el Reglamento Estudiantil de Posgrados vigente, el cual puede consultar en www.unipiloto.edu.co. Se enfatiza de manera particular el Artículo 28 (Cancelación de matrícula), el Artículo 29 (Abonos y devoluciones) y el Artículo 33 (Asistencia y participación en las actividades curriculares).


VIGILADA MINEDUCACIÓN

Institución de educación superior sujeta a la inspección y vigilancia del Ministerio de Educación Nacional de Colombia. Reconocimiento de personería jurídica como institución de educación superior con Resolución No. 3681 del 27 de noviembre de 1962 del Ministerio de Educación Nacional de Colombia. Código institución: 1815.

Vigencia desde 2019