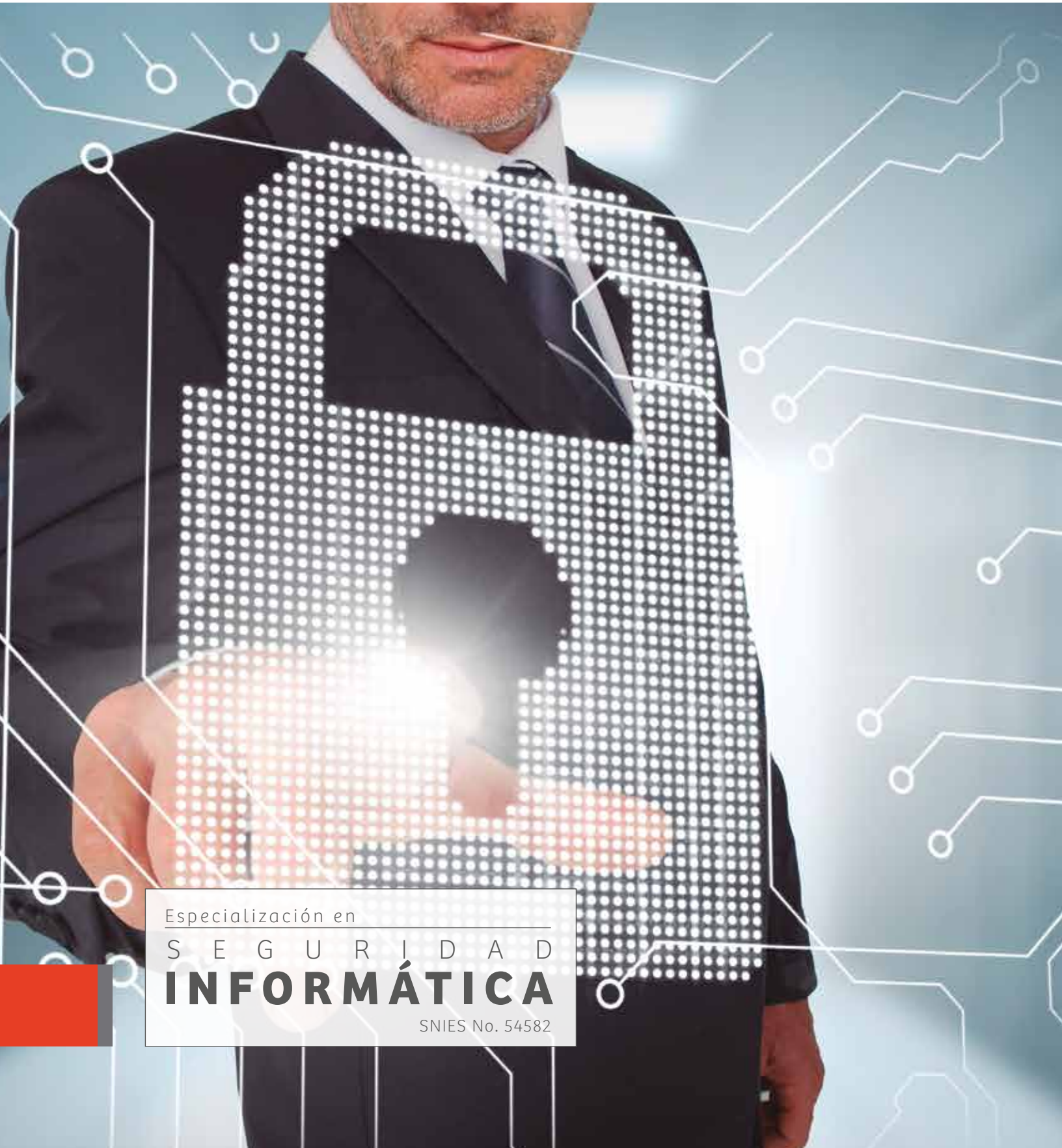
UNIVERSIDAD Piloto DE COLOMBIA



Especialización en

# SEGURIDAD INFORMÁTICA

SNIES No. 54582

Especialización en

# SEGURIDAD INFORMÁTICA

La Especialización tiene como objetivo formar profesionales especializados en la toma de decisiones en los temas de seguridad e integridad de la información, que planee, organice, ejecute, dirija, controle y evalué los riesgos y amenazas que se deben reducir y preservar la integridad de la información de las organizaciones.

Resolución de Registro Calificado N°. 16391 del 18/11/2013; vigencia por 8.5 años. SNIES No. 54582 del 05/05/2009. Título: Especialista en Seguridad Informática. | Nivel: Especialización. | Metodología: Presencial. | Sede Bogotá.

## Información general

Duración
**1 año académico (3 ciclos).**

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
**27 créditos**

En un período relativamente corto de tiempo, los datos del mundo de los negocios han pasado de simples archivos de papel, con copias en carbón y archivadores físicos, a los archivos electrónicos almacenados en muy poderosos sistemas de cómputo. Hemos pasado de tener la seguridad de los archivos de papel en una sala de archivos dentro de una oficina, a la seguridad de los datos en los computadores que acceden a las redes y a través de Internet.

La gestión de los registros en formato electrónico ha creado una industria totalmente nueva, que, a su vez, ha creado una generación de tecnología más pequeña, más rápida y más potente. El resultado ha sido la necesidad de contar con herramientas para administrar y asegurar esta información electrónica de manera eficiente y eficaz. Este nuevo paradigma de negocios del siglo XXI ha dado lugar a los riesgos de la información, los cuales se pueden considerar como la probabilidad de que la información almacenada electrónicamente privada o confidencial se pueda acceder y/o explotar por terceros no autorizados, lo cual es un problema cada vez mayor para las empresas de todos los sectores que utilizan tecnología.

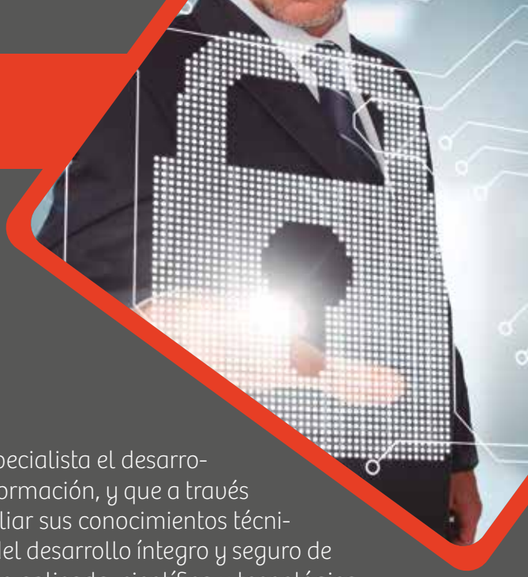
No hace mucho tiempo, una empresa podía implementar una solución de seguridad para toda la empresa que podía permanecer efectiva durante un par de años. Hoy en día, a medida que más y más empresas se vuelven dependientes de las redes de computadores, de información electrónica, de almacenamiento basado en la nube, del comercio electrónico, de las redes sociales, de la mensajería instantánea y el uso de Internet en general, ha llevado a un nuevo paradigma, en donde las soluciones establecidas para proteger los bienes electrónicos y la información tienen una vida media relativamente corta[1].

El presente capitulo plantea una panorámica del contexto nacional, latinoamericano y mundial de lo que ha sido la formación en la Especialización de seguridad informática en concordancia con los lineamientos, directrices, normatividad y estándares que rigen las actividades relacionadas con el adecuado tratamiento de la información por medios informáticos; argumentos que soportan la importancia y pertinencia de desarrollar un programa de formación avanzada en Seguridad Informática a la luz de las necesidades y exigencias de mayor formación de los profesionales, como también, las oportunidades de desempeño de acuerdo a las necesidades identificadas para el país y el entorno latinoamericano, dando realce particularmente a la propuesta que hace la Universidad Piloto de Colombia.

[1] Information Risks & Risk Management GIAC (GLEG) Gold Certification, John Wurgler, April 23 2013.

UNIVERSIDAD Piloto DE COLOMBIA

Especialización en
SEGURIDAD
# INFORMÁTICA
SNIES No. 54582



## Presentación del programa

Con los conocimientos y habilidades adquiridos durante el desarrollo de los diferentes módulos, el Especialista en Seguridad Informática fortalece y consolida la capacidad para la toma de decisiones frente a las problemáticas relacionadas con la seguridad de la información y con habilidades y competencias para:

- Aplicar conocimientos técnicos y procedimentales de forma integral, con visión de futuro, para aportar a la solución de problemas relacionados con la protección de la información, que garanticen elevar el nivel de seguridad y confiabilidad de las empresas, de acuerdo con las necesidades y exigencias del mercado.
- Analizar, diseñar, implementar, evaluar y gestionar proyectos relacionados con la seguridad de la información utilizando para ello tecnología de punta.
- Promover cambios culturales al interior de las organizaciones que propicien una concientización de la importancia de la seguridad de la información y de la ética en el manejo de la misma.
- Formular, implementar, evaluar y ajustar políticas, guías y procedimientos relacionados con la seguridad de la información.
- Propiciar espacios de investigación que permitan al especialista el desarrollo de proyectos relacionados con la seguridad de la información, y que a través de la utilización de nuevas tecnologías le permitan ampliar sus conocimientos técnicos para que pueda integrarlos a la sociedad, por medio del desarrollo íntegro y seguro de las empresas, fomentando y desarrollando la investigación aplicada, científica y tecnológica.
- Contribuir a comprender, interpretar, preservar, reforzar, fomentar y difundir las mejores prácticas en relación con el desarrollo tecnológico al interior de las organizaciones.

## Objetivo del programa

**Objetivo General**

La Especialización en Seguridad Informática tiene como propósito "Formar profesionales con amplio criterio en la toma de decisiones en los temas relacionados con la seguridad de la información; capaces de planear, organizar, ejecutar, evaluar, dirigir y controlar las actividades de salvaguarda y mitigación de los riesgos y las amenazas inherentes al manejo de la información, de tal forma que se puedan garantizar la integridad, confidencialidad y disponibilidad de la misma dentro de las organizaciones".

**Objetivos Específicos**

- Constituir un espacio abierto para la formación superior que propicie el aprendizaje permanente, brindando al profesional la posibilidad de realización individual y fomentando la movilidad social con el fin de formar ciudadanos que participen activamente en los sectores productivos y abiertos a las incertidumbres del mundo de los negocios electrónicos y el desarrollo tecnológico de las empresas.

## Perfiles del programa

**PERFIL DEL ASPIRANTE**

- 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 de la información.
- 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.
- Aspirante con una fuerte motivación para trabajar en análisis, diseño e implementación de tecnología, de sistemas, de procesos y de servicios relacionados con la seguridad de la información.
- Consultores e investigadores interesados en las temáticas relacionadas con la seguridad de la información.
- Empresarios independientes que deseen desarrollar habilidades estratégicas en el campo de la Seguridad Informática.
- Los aspirantes deben manifestar además su interés para trabajar en análisis, diseño e implementación de tecnología, de sistemas, de procesos y de servicios relacionados con la seguridad de la información. Y su interés por generar solución a problemas relacionados con el aseguramiento de la información.

Especialización en
SEGURIDAD
# INFORMÁTICA
SNIES No. 54582

## PERFIL PROFESIONAL DEL EGRESADO

El Especialista en Seguridad Informática egresado de la Universidad Piloto de Colombia es un profesional con habilidades para adelantar proyectos relacionados con la seguridad de la información; así como dirigir, gerenciar 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.

## PERFIL OCUPACIONAL

El Especialista egresado de la Especialización en Seguridad Informática 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.
- Director del área de Tecnologías de la Información y las Comunicaciones.
- Estratega de Seguridad de la Información.
- Docente Experto en Seguridad Informática.

## Metodología del programa

El Programa de Especialización en Seguridad Informática estructura su plan de estudios a partir de áreas (área de profundización, de investigación y complementaria) y núcleos temáticos específicos que se desarrollan en 3 ciclos de formación en correspondencia con los lineamientos de las políticas institucionales.

Cada uno de los núcleos temáticos son la base de las líneas de investigación y son los que definen de manera integral la estructura curricular y dan el sentido y la identidad al programa y se pueden resumir de la siguiente forma: En los dos primeros ciclos se hace especial énfasis en la fundamentación teórica y práctica que buscan darle al Especialista las herramientas necesarias para abordar problemáticas relacionadas con la seguridad de la información; en el tercer ciclo, se complementa el plan de estudios y proporciona al programa de especialización el componente flexible, a través de las electivas que se ofrecen para que el estudiante pueda profundizar en alguno de los temas de actualidad.

El proyecto de grado, busca que el Especialista tenga la posibilidad de aplicar los conocimientos adquiridos en un proyecto de investigación aplicada; se trabaja desde el primer ciclo, donde se le da al estudiante una fundamentación filosófica del conocimiento y el método científico, para que el futuro especialista apropie una idea de aplicabilidad a la ingeniería en el área de seguridad y pueda culminar con un documento que se convertirá en su anteproyecto, el cual terminará en el tercer ciclo en el que deberá presentar el resultado final de su investigación, para lo cual ha tenido el acompañamiento de un docente que hace las veces de tutor.

UNIVERSIDAD Piloto DE COLOMBIA

Especialización en
SEGURIDAD
# INFORMÁTICA
SNIES No. 54582

Plan
de estudios

Período 01
10 créditos

## PROFUNDIZACIÓN 8 Cred

### MODELOS FORMALES Y CRIPTOGRAFÍA

**1. Introducción a la seguridad**
2 créditos

Objetivos:
- Conocer el ámbito, la justificación y el panorama general de las técnicas más utilizadas en la seguridad informática.
- Tener clara la importancia del análisis de riesgos para tomar decisiones adecuadas en cuanto a seguridad informática.
- Desarrollar habilidades para seleccionar o establecer

**2. Criptografía**
3 créditos

Objetivos:
- Permitir que el estudiante participe activamente en el proceso de aprendizaje, adquiriendo una visión analítica para llegar a la comprensión de la importancia de la seguridad de la información mediante el uso de algoritmos y estándares de cifrado de información.
- Identificar los principales modos y tipos de cifrado, algoritmos y modelos comerciales que se pueden implementar en la actualidad.
- Comprender técnicas de criptoanálisis y esteganografía aplicados a modelos de cifrado contemporáneos.
- Diferenciar los diferentes tipos de cifradores y sus aplicaciones en implementaciones de arquitecturas de seguridad de la información basado en los principios de integridad, confidencialidad y no repudio.
- Identificar técnicas de cifrado actuales y buscar aplicaciones de acuerdo al modelo a implementar.

### GESTIÓN DE LA SEGURIDAD Y EL RIESGO

**1. Gestión de la seguridad informática**
3 créditos

Objetivos:
- Conocer y aplicar los elementos necesarios para planificar, implementar, mantener y mejorar la gestión de la seguridad de la información dentro de la organización.
- Comprender la interrelación entre los objetivos de la estrategia organizacional y los requerimientos de la seguridad de la seguridad de la información.
- Entender la importancia de la gestión de riesgos de la seguridad de la información como una herramienta para el logro de los objetivos del negocio y para el desarrollo de un programa apropiado de gobierno de la seguridad.
- Entender la dinámica de implementación de un programa de seguridad de la información bajo la óptica de la norma ISO27001:2005
- Identificar los conceptos fundamentales asociados al diseño de un plan de continuidad de negocio.

## INVESTIGACIÓN 2 Cred

**1. Investigación I**
2 créditos

Objetivos:
- Aplicar de cada módulo visto los conocimientos adquiridos de forma tal que se inicie la implementación de un modelo basado en investigación aplicada, para ir desarrollando el
- proyecto final.

UNIVERSIDAD Piloto DE COLOMBIA

Especialización en
SEGURIDAD
# INFORMÁTICA
SNIES No. 54582

## Período 02
9 créditos

## PROFUNDIZACIÓN
9 Cred

### TÉCNICAS DE DETECCIÓN

**1. Seguridad operativa**
3 créditos

Objetivos:
- Entendimiento y capacidad de aplicación de descripciones generales de los diferentes planteamientos de Seguridad Informática, alrededor de las redes de datos y los sistemas operativos.
- Identificación de mecanismos de protección y defensa en redes de datos y sistemas operativos.
- Capacidad de diseño/rediseño de una Arquitectura de Red Segura.
- Reconocimiento de las vulnerabilidades y los patrones normales de ataques en redes de datos y en sistemas operativos.
- Adquirir destrezas en los mecanismos que permiten implementar un ambiente de seguridad operativa en la red de las organizaciones para tomar decisiones adecuadas sobre las variables como son el modelo de comunicaciones TCP/IP, su funcionalidad y deficiencias. Además adquirir capacidad para detectar y corregir las fallas en la seguridad de los sistemas operacionales.
- Familiarizar a los estudiantes con los conceptos básicos de arquitectura de redes seguras, tipos de ataques y de vulnerabilidades, manejo seguro de sistemas operativos y su aseguramiento.

**2. Detección de intrusos**
3 créditos

Objetivos:
- El objetivo principal de este curso es proveer al estudiante las técnicas de análisis para la detección de intrusos en sistemas de información.
- Análisis de tráfico en Internet: TCP/IP, el principal protocolo utilizado en internet, así como ICMP y UDP serán temas de estudio.
- Uso de herramientas de análisis de tráfico en internet como TCPDump/WinDump.
- Uso de Snort, sistema real de detección de intrusos.

### INFORMÁTICA FORENSE

**1. Informática forense**
3 créditos

Objetivos:
- Generar competencias que permitan administrar adecuadamente la evidencia digital bajo un concepto de seguridad, teniendo en cuenta los principios de la informática forense.
- Aseguramiento del lugar en donde ocurre la incidencia informática o cibernética.
- Recolección de la evidencia digital teniendo en cuenta estándares internacionales frente a la administración de evidencia computacional.
- Extracción de imágenes forenses bajo el concepto de preservación de la evidencia.
- Aseguramientos de la evidencia teniendo en cuenta el concepto de seguridad de la información (integridad, confidencialidad, disponibilidad, seguridad y no repudio), frente a la cadena de custodia (mismidad, autenticidad y seguridad) y frente a la norma (legalidad, autenticidad y validación).

Especialización en
SEGURIDAD
# INFORMÁTICA
SNIES No. 54582

Período 03
8 créditos

## PROFUNDIZACIÓN 3 Cred

### GESTIÓN DE LA SEGURIDAD Y EL RIESGO

**1. Seguridad en aplicaciones**
3 créditos

Objetivos:
- Presentar de manera teórica y práctica las fallas en la seguridad de los sistemas operacionales y en las aplicaciones web y cliente servidor mediante la realización de talleres prácticos.

## INVESTIGACIÓN 3 Cred

### INVESTIGACIÓN

**1. Investigación II**
3 créditos

Objetivos:
- El estudiante debe realizar un proyecto final en donde debe aplicar los conocimientos adquiridos, el cual debe ser la continuación de un modelo basado en investigación aplicada, adelantado en Investigación I.

## ELECTIVA 2 Cred

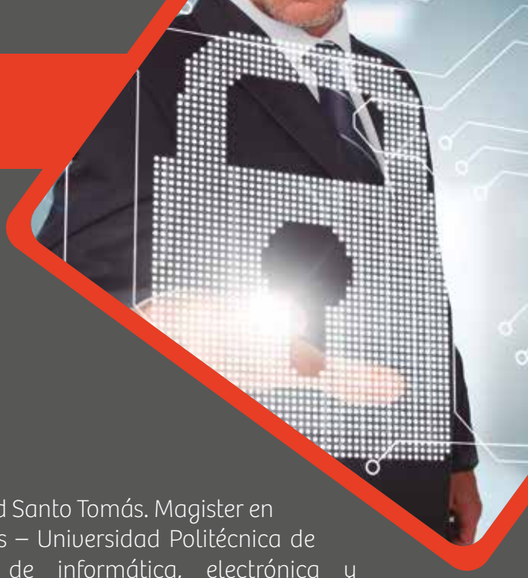
### ELECTIVA

**1. Electiva: Legislación informática**
2 créditos

Objetivos:
- Enunciar y explicar los diferentes tipos de pruebas técnicas, con un vocabulario apropiado, distinguiendo los criterios básicos de presentación de cada prueba digital.
- Recolectar, dirigir, montar y explicar, una prueba digital dentro de cualquier clase de proceso, de igual forma presentará cualquier tipo de actuación procesal en medios digitales.
- Enunciar y describir la inspección judicial en las distintas clases de procesos judiciales.
- Solicitar y practicar, una inspección judicial de acuerdo a los parámetros de técnica probatoria apropiados para la formalidad de cada proceso.

**TOTAL CRÉDITOS ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA - 27 CRÉDITOS**

Especialización en
SEGURIDAD
INFORMÁTICA
SNIES No. 54582



# Equipo Docente

**ÁLVARO ESCOBAR ESCOBAR**
Magister 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 de Ejército, Sergio Arboleda y Universidad Piloto de Colombia.

**ALEXANDER RODRÍGUEZ**

Ingeniero en Control Electrónico e Instrumentación. Especialista en Seguridad de la Información. Candidato a Magister en Comunicaciones y Ciencias de la Información. Amplios conocimientos en informática forense y seguridad en infraestructuras de red y host, conocimiento y manejo de diferentes plataformas de seguridad como IPS, IDS, Firewall, UTM, NAC, Hips, Desktop Firewall, Analizadores de Vulnerabilidades, Protección de Fuga de Información, Routing, entre otras. Experiencia en docencia Universitaria por más de 4 años. Funcionario del área de tecnología de McAfee, Inc. Colombia.

**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 Tomas y Militar Nueva Granada, además de desarrollo del ejercicio profesional en empresas como Concasa y Caracol Televisión.

**JENNY ALEJANDRA VARELA SEGURA**

Ingeniera de Telecomunicaciones – Universidad Santo Tomás. Magister en Redes Corporativas e Integración de Sistemas – Universidad Politécnica de Valencia, España. Formación en áreas de informática, electrónica y telecomunicaciones con profundización en redes. Experiencia en el área de Seguridad informática en la empresa Arolen S.A. Experiencia como docente en la Escuela de Comunicaciones del Ejército en la Especialización en Seguridad Informática y en el programa de pregrado en Ingeniería en Telecomunicaciones de la Universidad Militar.

**JOHN JAIRO ECHEVERRY ARISTIZABAL**

Máster en Auditoria Seguridad, Gobierno y Derechos de las TICs – Universidad Autónoma de Madrid España. V – Universidad Piloto de Colombia. Ingeniero de Sistemas – Universidad Católica de Colombia. Certificación Internacional EnCE "ENCASE Certified Examiner" 2011. Certificación Internacional ACE "AcessData Certified Examiner". Experiencia profesional y especializada por más de quince (15) años en temas de delitos informáticos, fraudes electrónicos, ciberdelito, ciberdelincuencia, entre otros, orientadas a la investigación de incidencias informáticas que afectan a la administración pública y de justicia (Contrataciones Públicas), el patrimonio económico (Hurtos mayor Cuantías), los derechos de autor y propiedad intelectual, la integridad moral de las personas, accesos ilegales a sistemas, entre otros. Así mismo, posee habilidades en la informática forense, la administración de evidencia digital y/o electrónica, recuperación de información, desencripción de claves, intervención de correos electrónicos, manejo de Internet en escenarios virtuales mediante el empleo de herramientas forenses de las cuales se encuentra certificado internacionalmente.

**EDGAR MAURICIO LOPEZ ROJAS**

Profesional en Ingeniería de Sistemas, Especialista en Seguridad en Redes Informáticas, Especialista en Docencia Universitaria, Máster Seguridad Informática,

con experiencia como docente de 10 años en instituciones de Educación superior dictando en ambientes presenciales y virtuales. Experiencia en el sector productivo de más de 20 años en administración de infraestructura física y virtual, redes LAN, dispositivos networking, sistemas operativos, gestión de accesos, análisis de riesgos, implementación de controles y procedimientos.

**LEONARDO ERNESTO VENEGAS OSUNA**

Ingeniero de Sistemas con especialización en Seguridad Informática y de la información, Técnico en Sistemas y Tecnólogo de sistemas, Certificado como Ethical Hacker (CEH), Certificado OSWP, Certificado en Auditor Interno y Auditor Líder ISO27001:2013, con formación integral en sistemas informáticos y las comunicaciones. Ejecución de pruebas de Ethical Hacking y Pentesting a entornos Web, entornos Cloud entornos Mobile e Infraestructura Empresariales. Análisis, resolución de problemas. Verificación y auditoría de sistemas ISO 27001:2013 y PCI. Especial énfasis en seguridad y vulnerabilidad de la información, procesos, terminales, bases de datos. Control de amenazas, protección, respaldo y autenticación de usuarios, procesos y datos.

**SANDRA LORENA OCAMPO CORREA**

Ingeniero de Sistemas y Computación – Universidad del Quindío, Especialista en Seguridad Informática – Universidad Piloto de Colombia, Técnico Profesional en Ingeniería de Sistemas – Corporación Unificada Nacional. Certificada en la creación de páginas web en HTML y Javascript, desempeño en bases de datos en ACCESS y SQL, Calidad en el desarrollo de software, Técnica de comunicación en el nivel operativo, Fundamentación para la Implementación de los SGC, Capacitación en el desarrollo de relaciones interpersonales, laborales y talento humano con experiencia en Docencia Universitaria, Desempeño en comercio electrónico y Auditoría Interna de Calidad y de SGC, asesora y consultora en la elaboración, formulación, ejecución y evaluación de procesos sistemáticos a través de UML.

Experiencia como Ingeniero de Calidad Líder de Proyecto en GGT para ICETEX, implantadora de Queryx 7 para SQL Software, implementación del directorio activo en la Universidad del Quindío, responsable del departamento de nómina de SEMCOL CTA.

**HÉCTOR GIOVANNI CRUZ FORERO**

Master en Seguridad de la Información, 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.

**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.

**LEONARDO CRISTANCHO HOYOS**

Abogado egresado de la facultad de Derecho de la Universidad de la Sabana. Posteriormente, se recibió como especialista en Derecho Comercial y en su segunda especialización, se facultó como Especialista en Derecho de La Empresa, ambos posgrados los realizó en la Facultad de Jurisprudencia de la Universidad del Rosario. En ejercicio de su carrera, se ha desempeñado realizando funciones como: consultor en asuntos legales, abogado litigante, estructurador empresarial, director jurídico, profesor universitario tanto en pregrado como en posgrados y conferensista internacional; actualmente se encuentra en ejercicio de su profesión como CEO de la firma Cristancho Hoyos & Abogados Asociados y como docente de la Universidad Piloto de Colombia. Dentro de las áreas de su ejercicio profesional encontramos las siguientes: Derecho Comercial, Derecho de la Empresa y de Los Negocios, Derecho de las Telecomunicaciones, Derecho de las Tecnologías de la Información, Potección de Datos y de la Seguridad Informática, Propiedad Intelectual, Derecho de la Responsabilidad y Arbitraje.

**RICARDO E. 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.

Especialización en
SEGURIDAD
INFORMÁTICA
SNIES No. 54582

**CARLOS VILLAMIZAR R.**

Ingeniero de Sistemas de la Universidad Nacional de Colombia y Especialista en Auditoría de Sistemas de Información de la Universidad Católica de Colombia. Cuenta con amplia experiencia en los campos de gobierno de TI, riesgos, auditoría, control y seguridad de la información. Ha trabajado como Auditor de sistemas en Price Waterhouse y Grupo Empresarial Protela realizando labores en Colombia, México, Venezuela y Ecuador, y como Gerente de consultoría en Digiware en proyectos de seguridad de la información. Actualmente se desempeña como Director de desarrollo de negocios para Latinoamérica de Globalsuite y consultor en seguridad de la información, contribuyendo a la certificación ISO 27001 de varios clientes. Fue presidente de ISACA capítulo Bogotá en el período 2007-2009 y en 2010 fue distinguido por ISACA con el premio John Kuyers como mejor contribuyente de la Asociación en LATAM. Profesor universitario y conferencista en eventos y foros nacionales e internacionales. Cuenta con las certificaciones CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CGEIT (Certified in the Governance of Enterprise IT), CRISC (Certified in Risk and Information Systems Control), Cobit Foundations Certificate, Auditor Lider ISO 27001 e Implementador Líder ISO22301.

## 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).

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

## Contáctenos


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

**PBX: 232 4122 - 580 0968**
Whatsapp: 318 280 0923

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


# 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.

"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 2021