UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

FACULTAD TECNOLÓGICA

ESTUDIO DE PERTINENCIA DE UN PROGRAMA

Proyecto Curricular: __ Maestría en Gestión y Seguridad de la Informacion _____

Este formato está diseñado para proporcionar un análisis exhaustivo de la pertinencia de un programa de posgrado, ayudándote a tomar decisiones informadas y estratégicas basadas en la demanda del mercado, las necesidades de los estudiantes y la capacidad institucional.

PRESENTACIÓN DEL PROGRAMA

Nombre del Programa: Maestría en Gestión y Seguridad de la Informacion.

Código SNIES: 110811.

Resolución del MEN: 018323 del 28 de septiembre de 2021.

Modalidad: Virtual.

Número de créditos: 40.

Justificación del programa: La Maestría en Gestión y Seguridad de la Información (MGSI) de la Universidad Distrital Francisco José de Caldas – Facultad Tecnológica es un programa de posgrado creada mediante el acuerdo No. 007 del 2020, que ofrece una opción virtual, la cual tiene como objetivo una formación académica integral que permita a los estudiantes comprender, analizar y gestionar los riesgos asociados con el uso de las Tecnologías de la Información, además, liderar y gestionar proyectos de seguridad de la información en las organizaciones. El programa se enfoca en el desarrollo de habilidades técnicas y gerenciales para la identificación, evaluación y mitigación de riesgos de seguridad de la información, así, como en la implementación de políticas y procedimientos para la protección de los activos de información.

Desde sus inicios, la Maestría ha evolucionado para adaptarse a los avances tecnológicos y las nuevas amenazas a la seguridad cibernética. Los procesos académicos se han ido ampliando y

mejorando en aspectos tanto teóricos como prácticos, brindando a los estudiantes las herramientas necesarias para gestionar de manera efectiva la seguridad de la información.

La Maestría en Gestión y Seguridad de la Información tiene una duración de cuatro semestres académicos. El programa cuenta con un plan de estudios que permite una formación en los campos clave de la ciberseguridad y la gestión de la información, con una sólida base teórica complementada con prácticas y proyectos que reflejan situaciones reales del entorno profesional.

La Maestría en Gestión y Seguridad de la Información desempeña un papel crucial dentro de la Facultad Tecnológica de la Universidad Distrital F.J.C.. Este programa contribuye a la misión de la Facultad, la cual es formar profesionales altamente capacitados en el ámbito de las Tecnologías de la Información, con un enfoque en la innovación y la calidad educativa. Además, la Maestría refuerza el compromiso de la Universidad con el desarrollo tecnológico y científico de la región y el país, al generar conocimiento y soluciones que impactan positivamente en el sector productivo y en la seguridad digital de las organizaciones.

Objetivos del programa: La Maestría en Gestión y Seguridad de la Información de la Universidad Distrital Francisco José de Caldas - Facultad Tecnológica tiene como propósito principal formar profesionales altamente capacitados para liderar y gestionar proyectos de seguridad de la información en diversas organizaciones.
Las metas del programa se enfocan en alcanzar los siguientes logros:

1. **Formación de expertos en la seguridad de la información**: el programa busca capacitar a los estudiantes en el manejo de las principales herramientas, técnicas y metodologías relacionadas con la gestión de la seguridad de la información.
2. **Implementación de políticas de seguridad efectivas**: los egresados serán capaces de diseñar y aplicar políticas de seguridad robustas que aseguren la protección de los activos informáticos en diferentes tipos de organizaciones, considerando las amenazas emergentes y las necesidades específicas del entorno.
3. **Capacitación en la gestión de riesgos tecnológicos**: la Maestría tiene como objetivo enseñar a los estudiantes a identificar, evaluar y mitigar los riesgos tecnológicos y cibernéticos, proporcionando las bases para crear planes de contingencia y recuperación ante desastres.
4. **Desarrollo de un pensamiento estratégico y ético**: el programa busca que los estudiantes desarrollen habilidades críticas para tomar decisiones estratégicas, siempre bajo un marco ético que promueva la transparencia, la privacidad y el respeto por los derechos de los usuarios y las organizaciones.
5. **Interacción con el entorno profesional y empresarial**: fomentar la vinculación entre el mundo académico y el profesional, creando redes de colaboración con empresas y organismos relacionados con la gestión de la seguridad de la información, permitiendo a los estudiantes aplicar sus conocimientos en escenarios reales y actuales.

Análisis del Entorno.

La Maestría en Gestión y Seguridad de la Información de la Universidad Distrital Francisco José de Caldas – Facultad Tecnológica, responde a una serie de tendencias globales y locales en el ámbito tecnológico, que incluyen el aumento de la ciberseguridad, la digitalización de los procesos y la implementación de normativas nacionales e internacionales. Las políticas educativas y las regulaciones sobre protección de datos personales y ciberseguridad han generado un entorno favorable para la creación y expansión del programa. Además, el contexto

socioeconómico actual, caracterizado por el crecimiento de la economía digital y la necesidad de profesionales altamente calificados, ha elevado la demanda de este tipo de formación especializada, convirtiendo a la Maestría en una opción estratégica para aquellos interesados en el campo de la gestión y seguridad de la información.

1. Tendencias del sector:

La industria de la tecnología, particularmente la relacionada con la gestión y seguridad de la información, está en constante evolución debido a la creciente dependencia de las tecnologías digitales y el aumento de las amenazas cibernéticas lo que impacta directamente en la Maestría ofrecida por la Universidad Distrital Francisco José de Caldas – Facultad Tecnológica. Algunas de las principales tendencias incluyen:

- **Crecimiento de la ciberseguridad**: la ciberseguridad se ha convertido en una prioridad estratégica para las organizaciones a nivel mundial debido al aumento de los ciberataques, las amenazas de retención de datos y/o dispositivos (*Ransomware*) y los riesgos asociados con la protección de datos sensibles. Este aumento en los riesgos digitales ha impulsado la demanda de expertos en seguridad de la información, generando una necesidad creciente de programas académicos especializados en este campo. Fuentes: *MinTic*, *Deloitte*, plataformas de empleo(*LinkedIn, Computrabajo e Indeed*), observatorio laboral del SENA.
- **Transformación digital**: la adopción de tecnologías emergentes como la Inteligencia Artificial (*IA*), el Internet de las Cosas (*IoT*), la computación en la nube y el Big Data ha transformado las organizaciones, lo que a su vez incrementa la vulnerabilidad de los sistemas de información. Por esta razón, las empresas requieren profesionales capacitados para gestionar estos entornos tecnológicos y garantizar la seguridad de la información.
- **Cumplimiento de normativas nacionales e internacionales**: la implementación de normativas y estándares internacionales como el *Reglamento General de Protección de Datos* (GDPR) en Europa, y la *Ley de Protección de Datos Personales* en Colombia, está generando una creciente demanda de especialistas que entiendan y puedan aplicar estas regulaciones en el contexto corporativo.
- **Automatización de la ciberseguridad**: la automatización y el uso de herramientas avanzadas para detectar amenazas y gestionar la seguridad de la información están en auge. Esto hace que los programas académicos deban incorporar enfoques que enseñen a los estudiantes a utilizar tecnologías como la Inteligencia Artificial y el aprendizaje de las máquinas (*Machine Learning*) para identificar y mitigar dichos riesgos de manera eficaz y eficiente.

2. Políticas y normativas:

La creación y el desarrollo de la Maestría en Gestión y Seguridad de la Información se ve influenciada por diversas políticas y normativas, tanto a nivel educativo como en el ámbito de la seguridad de la información:

- **Normativas educativas**: la legislación educativa en Colombia, como la Ley 30 de 1992, establece los lineamientos para la educación superior en el país, exigiendo que las Universidades ofrezcan programas académicos que respondan a las necesidades del entorno social y económico, promoviendo la calidad educativa. La Maestría en Gestión

y Seguridad de la Información está alineada con estos principios, ofreciendo un programa que responde a las demandas de la industria tecnológica.

- **Regulación de la protección de datos personales**: La ley 1581 de 2012 en Colombia y el decreto 1377 de 2013, regulan la protección de datos personales, lo que genera la necesidad de la formación en gestión de la información para asegurar el cumplimiento de las normativas de protección de datos. La Maestría ayuda a los profesionales a comprender y aplicar estas leyes, asegurando que los egresados sean capaces de implementar políticas y soluciones que protejan los datos personales dentro de las organizaciones.
- **Normas nacionales e internacionales de ciberseguridad**: la implementación de políticas y estrategias para fortalecer la ciberseguridad en el país (CONPES 3995 de 2020), la implementación de estándares internacionales, como ISO/IEC 27001 y 27002 (relacionados con la gestión de la seguridad de la información), el NIST Cybersecurity Framework para la gestión de riesgos y la normativa GDPR en Europa, impulsan la formación de profesionales en esta área que adquieran el conocimiento necesario para cumplir con los estándares nacionales e internacionales y las mejores prácticas de seguridad.

3. Contexto socioeconómico:

Los factores socioeconómicos juegan un papel importante en la demanda de programas como la Maestría en Gestión y Seguridad de la Información. Algunos de los factores más relevantes son:

- **Crecimiento de la economía digital**: la economía digital está en expansión tanto en Colombia como a nivel global. Las empresas de diferentes sectores están adoptando soluciones tecnológicas avanzadas, lo que genera una mayor demanda de profesionales capacitados en la gestión y seguridad de la información.
- **Aumento de los ciberataques y la conciencia social**: los ciberataques y las fugas de información son un problema creciente, lo que ha generado una mayor conciencia en la sociedad sobre la importancia de la seguridad de la información. Este fenómeno ha llevado a las organizaciones a invertir más en la protección de sus activos digitales, lo que aumenta la demanda de especialistas en el área. Esta tendencia se refleja en la necesidad de programas académicos especializados en seguridad de la información. Entre los ataque más relevantes se pueden mencionar: *IFX Networks (2023), Empresas Públicas de Medellín (EPM), EPS Sanitas, Universidad Javeriana, Claro Colombia, Invima, etc*.

- **Desempleo tecnológico y necesidad de capacitación avanzada**: en un contexto en el que el mercado laboral en Colombia enfrenta una alta tasa de desempleo, especialmente en sectores tradicionales, la formación avanzada en áreas tecnológicas como la ciberseguridad se ha convertido en una vía estratégica para mejorar las perspectivas de empleo. La Maestría ofrece a los profesionales la posibilidad de acceder a un mercado de trabajo altamente demandante en el campo de la tecnología y la seguridad de la información. *Fuente: plataformas de empleo.*
- **Desarrollo de políticas públicas y proyectos en Tecnología**: en el marco de las políticas públicas, el gobierno colombiano ha venido promoviendo la digitalización de las instituciones públicas y el fortalecimiento de la infraestructura tecnológica en el país. Iniciativas como el "Plan Nacional de Ciberseguridad" también refuerzan la

necesidad de formación especializada en la protección de datos y sistemas, favoreciendo la expansión y consolidación de programas académicos como la Maestría.

Análisis de la Oferta de Programas a nivel local, regional y nacional

Programas Similares: en la siguiente tabla se realiza una comparación con programas similares ofrecidos por otras instituciones.

Tabla 1. Estado del programa a nivel nacional

Nombre de la IES	Números de periodos académicos	Modalidad	Número de créditos académicos	Denominación del programa
Universidad de los Andes	4	presencial	40	Magíster en Seguridad de la Información.
UNAD	3	virtual	36	Magister en Ciberseguridad
Universidad Piloto de Colombia	4	presencial	43	Magíster en Seguridad informática y de las comunicaciones
Pontificia Universidad Javeriana	3	presencial	40	Magíster en Seguridad Digital
Universidad de Manizales	4	presencial	52	Magister en Seguridad de la Información
Instituto Tecnológico Metropolitano	4	Presencial y mediado por TIC	60	Magíster en Seguridad Informática

Fuente: SNIES

Conclusiones comparativas:

Universidad	Denominación del Programa	Conclusión Comparativa
Universidad Distrital Francisco José de Caldas	Maestría en Gestión y Seguridad de la Información (MGSI)	Se ubica en un punto intermedio en cuanto a créditos académicos y duración. Su enfoque en "Gestión y Seguridad de la Información" la diferencia de otras Maestrías con orientaciones más específicas en ciberseguridad o seguridad digital.
Universidad de los Andes	Magíster en Seguridad de la Información	Tiene una duración y modalidad similar a la MGSI, pero con menos créditos. Su enfoque es más directo en seguridad de la información.
UNAD	Magíster en Ciberseguridad	Se distingue por su modalidad virtual y menor duración. Su énfasis en ciberseguridad puede ser más técnico en comparación con la MGSI
Universidad Piloto de Colombia	Magíster en Seguridad Informática y de las Comunicaciones	Similar en duración y modalidad a la MGSI, pero con un enfoque más orientado a la seguridad informática y las comunicaciones.
Pontificia Universidad Javeriana	Magíster en Seguridad Digital	Presenta una menor duración con los mismos créditos que otras instituciones. Su enfoque en seguridad digital puede ser más amplio en el ámbito tecnológico.
Universidad de Manizales	Magíster en Seguridad de la Información	Es la segunda Maestría con más créditos académicos. Comparte la misma orientación en seguridad de la información con la MGSI.
Instituto Tecnológico Metropolitano	Magíster en Seguridad Informática	Es la Maestría con más créditos académicos, lo que sugiere una mayor carga de contenido. Comparte la misma orientación en seguridad de la información con la MGSI.

Comparación de Programas: análisis comparativo de contenido, estructura y resultados de programas similares.

Universidad	Contenido	Estructura	Resultados
Universidad Distrital Francisco José de Caldas	Enfoque en gestión y seguridad de la información, abarcando normativas, análisis de riesgos y tecnologías emergentes.	4 semestres, presencial y 40 créditos académicos.	Formación integral en gestión y seguridad de la información y desarrollo de habilidades para liderar proyectos de seguridad
Universidad de los Andes	Énfasis en seguridad de la información con orientación técnica y estratégica.	4 semestres, presencial y 40 créditos académicos.	Formación de expertos en seguridad de la información y desarrollo de habilidades de investigación, con énfasis en la aplicación de conocimientos.
UNAD	Focalizado en ciberseguridad, con un enfoque en herramientas digitales y protección de infraestructuras críticas.	3 semestres, virtual y 36 créditos académicos.	Formación en ciberseguridad para entornos virtuales y desarrollo de habilidades para la detección y prevención de amenazas
Universidad Piloto de Colombia	Seguridad informática y comunicaciones, con énfasis en redes y transmisión de datos segura.	4 semestres, presencial y 43 créditos académicos.	Formación en seguridad informática y de comunicaciones y desarrollo de habilidades técnicas y de gestión.
Pontificia Universidad Javeriana	Seguridad digital con un enfoque integral en tecnología, normatividad y privacidad de datos.	3 semestres, presencial y 40 créditos académicos.	Formación en seguridad digital integral y desarrollo de habilidades para la gestión de riesgos digitales.
Universidad de Manizales	Seguridad de la información con un enfoque holístico en riesgos, auditoría y cumplimiento normativo.	4 semestres, presencial y 52 créditos académicos.	Formación en gestión de la seguridad de la información y desarrollo de habilidades para la implementación de sistemas de gestión.
Instituto Tecnológico Metropolitano	Se enfoca en identificar, analizar y mitigar riesgos de seguridad y ciberseguridad que puedan afectar a una organización.	4 semestres, presencial/mediados por TIC y 60 créditos académicos.	Formación en la identificación, el análisis y la reducción de los diferentes riesgos de seguridad y ciberseguridad que puedan impactar negativamente a una organización.

Tabla 2. Resumen del estado del programa a nivel nacional

Sector	A distancia	Presencial	Virtual	Total
Oficial		2		2
Privada		3	1	4
Total				6

Fuente: SNIES

Conclusiones.

De las universidades que ofrecen programas de Maestría similares a la MGSI, cuatro de ellas son privadas y dos son públicas, donde una de las privadas ofrece su Maestría en modalidad virtual y una de las públicas en modalidad presencial/mediadas por TIC y las demás en modalidad presencial.

Programas existentes en otras instituciones. Teniendo en cuenta los programas descritos en la tabla 1, haga una descripción de los elementos que diferencian el programa de la competencia.

La Maestría en Gestión y Seguridad de la Información de la Universidad Distrital Francisco José de Caldas – Facultad Tecnológica, se ubica en un punto intermedio en cuanto a créditos académicos y duración. Su enfoque en "*Gestión y Seguridad de la Información*" la diferencia de las otras Maestrías con orientaciones más específicas en ciberseguridad o seguridad digital, además, orienta su formación a la gestión y seguridad de la información con lo cual se obtiene habilidades para liderar proyectos de seguridad.

La siguiente tabla se muestra la información que se encuentra en la página web de cada IES.

Tabla 3 Perfiles y rasgos distintivos

Nombre de la IES	Denominación del programa	Perfil profesional	Rasgos distintivos	Página web
Universidad Distrital Francisco José de Caldas	Maestría en Gestión y Seguridad de la Información (MGSI)	Profesional con los conocimientos necesarios para desarrollar e innovar los procesos y sistemas relacionados con la gestión y seguridad de la información integrando políticas y tecnologías con los objetivos del negocio, planteando soluciones a corto, mediano y largo plazo en las áreas estratégicas, tácticas y operacionales de la organización.	Formar magísteres con los conocimientos teórico-prácticos suficientes para el desarrollo y adaptación de modelos necesarios en la gestión y seguridad de la información.	MGSI
Universidad de los Andes	Magíster en Seguridad de la Información	Profesional preparado para tomar decisiones estratégicas, tácticas y operacionales en materia de seguridad de la información, con la idoneidad necesaria para causar impacto en el estamento directivo y actuar en forma pertinente hasta los niveles tanto tácticos como operacionales en TIC.	Formar profesionales expertos con cierto nivel de madurez, con un perfil estratégico, pero con conocimiento táctico y técnico, para que sean las personas que lideren procesos de Seguridad de la Información en diferentes sectores del país.	MSI
UNAD	Magíster en Ciberseguridad	Profesional con criterios éticos y con habilidades de liderazgo, capaz de transformar su contexto a través del desarrollo de procesos de I+D+i, soportado por tecnologías emergentes que a partir del despliegue de habilidades técnicas y estratégicas contribuya en la mejora de capacidades de ciberseguridad generando valor agregado en lo local, regional y global. .	Se destaca por su modalidad virtual, lo que permite una cobertura amplia y accesible en todo el país, superando las limitaciones de la oferta presencial concentrada en pocas regiones	MC
Universidad Piloto de Colombia	Magíster en Seguridad Informática y de	Profesional con habilidades para adelantar proyectos relacionados con la seguridad informática y de las	Profundización en la seguridad informática y de las comunicaciones cubriendo aspectos	MSIC

	las Comunicaciones	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.	detallados de la preparación y análisis técnico de los sistemas basados en TIC, combinada con una preparación completa en aspectos legales.	
Pontificia Universidad Javeriana	Magíster en Seguridad Digital	Profesional en el diseño de estrategias de prevención, detección, contención y reacción ante vulnerabilidades y amenazas digitales, que pongan en riesgo la seguridad de la información en las organizaciones privadas o públicas.	Posibilidad de profundizar de acuerdo con el perfil e intereses de los estudiantes en marco legal y nuevas tecnologías, seguridad organizacional y seguridad de sistemas.	MSD
Universidad de Manizales	Magíster en Seguridad de la Información	Profesional que estará en capacidad de tomar decisiones empleando metodologías, estándares y herramientas pertinentes al área de la seguridad de la información, evaluando y utilizando soluciones tecnológicas de acuerdo con las necesidades de operación, comunicación y protección de los datos de las empresas.	Énfasis en el fortalecimiento y consolidación de competencias y habilidades en la seguridad en la infraestructura tecnológica (hardware y software) y la seguridad de la información en la organización.	MSI
Instituto Tecnológico Metropolitano	Magíster en Seguridad Informática	Profesional con habilidades para gestionar los incidentes de seguridad de la información aplicando el dominio técnico, ético y administrativo con estándares internacionales.	Énfasis en identificar, analizar y reducir los diferentes riesgos de seguridad y ciberseguridad que puedan impactar negativamente a una organización.	MSINF

Fuente: Páginas oficiales de las universidades.

Conclusiones generales

- **Diversidad de enfoques**: las Maestrías analizadas ofrecen una amplia gama de enfoques, desde la gestión integral de la seguridad hasta la ciberseguridad especializada, pasando por la seguridad en redes y comunicaciones, la seguridad digital en un sentido amplio y la gestión de la seguridad vinculada a la continuidad de negocio.
- **Modalidades presenciales y virtuales**: la mayoría de las Maestrías son presenciales, lo que facilita la interacción y el aprendizaje colaborativo. Sin embargo, la UDISTRITAL y la UNAD ofrecen una opción virtual para aquellos que buscan flexibilidad en sus estudios.
- **Duración y créditos académicos**: la duración de las Maestrías varía entre 3 y 4 períodos académicos, y el número de créditos académicos oscila entre 36 y 52.

Conclusiones específicas

- **Universidad Distrital Francisco José de Caldas**: la Maestría se distingue por su modalidad virtual, su enfoque integral en gestión y aspectos técnicos, su orientación hacia la práctica y su énfasis en la seguridad de la información.
- **Universidad de los Andes**: esta Maestría se caracteriza por su profundización en temas técnicos y de gestión, su desarrollo de habilidades de investigación y su énfasis en la aplicación de conocimientos.
- **UNAD**: su programa de ciberseguridad se destaca por su modalidad virtual flexible, su enfoque en ciberseguridad y respuesta a incidentes, y su desarrollo de habilidades para entornos virtuales.
- **Universidad Piloto de Colombia**: esta Maestría se distingue por su énfasis en la seguridad en redes y comunicaciones, su formación técnica y de gestión, y su preparación para el sector de las telecomunicaciones.
- **Pontificia Universidad Javeriana**: su programa de seguridad digital se caracteriza por su visión amplia de la seguridad, que incluye aspectos legales y de protección de datos, su formación integral y su preparación para el cumplimiento normativo.
- **Universidad de Manizales**: esta Maestría se distingue por su énfasis en la gestión de la seguridad y su relación con la continuidad de negocio, su formación en gestión de la seguridad de la información y su énfasis en la protección de activos de información.
- **Instituto Tecnológico Metropolitano**: esta Maestría se enfatiza en identificar, analizar y reducir los diferentes riesgos de seguridad y ciberseguridad que puedan impactar negativamente a una organización.

Posicionamiento en el Mercado:

Universidad	**Maestría**	**Estrategias de Posicionamiento y Diferenciación**	**Estrategias de Marketing y Posicionamiento**
Universidad Distrital Francisco José de Caldas	Gestión y Seguridad de la Información	- **Enfoque integral**: combina gestión y aspectos técnicos, diferenciándose de programas más especializados. - **Precio competitivo**: ofrece una formación de calidad a un costo accesible. - **Énfasis en la normativa**: prepara para el cumplimiento legal en seguridad de la información.	- **Presencia en línea**: promoción a través de la página web de la universidad y redes sociales. - **Eventos y charlas**: participación en eventos del sector y organización de charlas informativas.
Universidad de los Andes	Seguridad de la Información	- **Prestigio académico**: respaldo de una universidad reconocida por su excelencia. - **Enfoque en investigación**: desarrollo de habilidades para la investigación y la innovación en seguridad. - **Red de contactos**: amplia red de egresados y profesores con experiencia en el sector.	- **Marketing digital**: campañas en línea dirigidas a profesionales y estudiantes interesados en seguridad. - **Eventos académicos**: organización de congresos, seminarios y talleres sobre seguridad de la información. - **Publicaciones**: difusión de investigaciones y artículos científicos en el área de seguridad.
UNAD	Ciberseguridad	- **Modalidad virtual**: flexibilidad y accesibilidad para	- **Marketing digital**: promoción a través de redes sociales, correo

		estudiantes con restricciones de tiempo o ubicación. - **Enfoque en ciberseguridad**: especialización en un área de alta demanda laboral. - **Cobertura nacional**: presencia en todo el país gracias a su modelo de educación a distancia.	electrónico y publicidad en línea. - **Eventos virtuales**: organización de webinars y conferencias en línea sobre ciberseguridad. - **Alianzas**: Convenios con empresas y organizaciones para ofrecer descuentos y oportunidades a estudiantes.
Universidad Piloto de Colombia	Seguridad Informática y de las Comunicaciones	- **Énfasis en redes y comunicaciones**: formación especializada para el sector de las telecomunicaciones. - **Trayectoria y experiencia**: programa con años de experiencia en la formación de profesionales en seguridad.	- **Marketing tradicional**: publicidad en medios impresos, radio y televisión. - **Eventos presenciales**: participación en ferias y eventos del sector tecnológico. - **Convenios**: alianzas con empresas de telecomunicaciones para ofrecer prácticas y oportunidades laborales.
Pontificia Universidad Javeriana	Seguridad Digital	- **Visión integral**: enfoque amplio que incluye aspectos legales y de protección de datos. - **Reputación y tradición**: universidad con reconocimiento y trayectoria en la formación de profesionales. - **Énfasis en valores**: formación ética y humanística en seguridad digital.	- **Marketing digital**: campañas en redes sociales, correo electrónico y publicidad en línea. - **Eventos académicos**: organización de seminarios y conferencias sobre seguridad digital. - **Publicaciones**: difusión de investigaciones y artículos en el área de seguridad digital.
Universidad de Manizales	Seguridad de la Información	- **Gestión de la seguridad**: enfoque en la implementación de sistemas de gestión de seguridad. - **Continuidad de negocio**: vinculación de la seguridad con la protección de activos y la operación de la empresa. - **Enfoque práctico**: desarrollo de habilidades para la aplicación de conocimientos en el mundo laboral.	- **Marketing digital**: promoción a través de redes sociales, correo electrónico y publicidad en línea. - **Eventos presenciales**: participación en ferias y eventos del sector empresarial. - **Alianzas**: Convenios con empresas de la región para ofrecer prácticas y oportunidades laborales.
Instituto Tecnológico Metropolitano	Magíster en Seguridad Informática	- **Enfoque en la práctica:** la formación orientada a la resolución de problemas reales y al desarrollo de habilidades prácticas en seguridad informática. - **Infraestructura y recursos:** laboratorios especializados, software y herramientas de vanguardia disponibles para los estudiantes. - **Convenios con empresas:** acuerdos con empresas del sector que permiten a los estudiantes realizar prácticas profesionales o proyectos de investigación. - **Énfasis en áreas específicas:** se enfoca en áreas como	- **Marketing digital** promoción a través de: Página web del programa, Redes sociales, publicidad online **Eventos y ferias:** participar en eventos y ferias relacionadas con seguridad informática para dar a conocer la maestría y contactar con potenciales estudiantes.

		ciberseguridad, análisis forense o seguridad en redes industriales.	

Contexto internacional de la educación y de la ocupación en el programa

Tabla 4 Estado del programa a nivel internacional.

País	Nombre de la universidad	Nombre del programa	Hipervínculo del enlace de la página web	Números de periodos académicos	Modalidad	Números de créditos académicos
España	Universidad Internacional de la Rioja UNIR	Master Universitario en Ciberseguridad	MUC	2	virtual	60
España	Universidad Nacional de Educación a Distancia -UNED	Master Universitario en Ciberseguridad	MUNUNED	2	Distancia	60
España	Universitat Obert de Catalunya	Master de Ciberseguridad y privacidad	MCP	4	Online	60
España	Universidad Autónoma de Barcelona (UAB)	máster de Seguridad de las Tecnologías de la Información y las Telecomunicaciones	MISTIC	4	Presencial	60
USA	Carnegie Mellon University	Maestría en Ciencias en Seguridad de la Información	MCSI	4	Presencial	48-60
Reino Unido	Imperial College London	Maestría en Ciencias en Seguridad de la Información	MSI	4	presencial	60
El salvador	Universidad de El Salvador	Maestría en Seguridad y Gestión de Riesgos Informáticos	MSGRI	4	presencial	60
El salvador	Universidad Francisco Gavidia	Maestría en Gestión de la Ciberseguridad	MGC	4	Virtual	64
Francia	Universidad de Tecnología de Troyes	Máster en Seguridad de los Sistemas de Información	MSSI	2	Presencial	52

Fuente: Páginas web universidades.

Conclusiones Generales:

- **Modalidad predominante:**
  - Existe una distribución equitativa entre programas presenciales y a distancia/en línea. Esto refleja la creciente demanda de flexibilidad en la educación superior, especialmente en campos tecnológicos como la ciberseguridad.
  - España muestra una gran oferta de programas en línea, y a distancia, lo cual demuestra que está a la vanguardia de las nuevas tecnologías de educación.
- **Créditos ECTS:**
  - La mayoría de los programas ofrecen 60 créditos ECTS, lo cual es un estándar común en las Maestrías europeas. Esto facilita la movilidad y el reconocimiento de títulos a nivel internacional.
  - Los programas de Estados Unidos presentan una variación en el número de créditos, lo cual puede significar una mayor flexibilidad.

- **Duración y modalidad:**
    - Los programas presenciales tienden a tener una duración de 4 periodos académicos, mientras que los programas a distancia/en línea varían entre 2 y 4 periodos. Esto sugiere que la modalidad a distancia puede ofrecer opciones más intensivas o flexibles en cuanto a la duración.
    - Se puede observar que en países de habla hispana, la duración de los programas es de 4 periodos, lo que equivale a 2 años.
- **Variedad internacional:**
    - La tabla muestra una diversidad de programas en diferentes países, lo que permite a los estudiantes elegir opciones que se adapten a sus preferencias geográficas y culturales.
    - La tabla demuestra que la Maestría en ciberseguridad, es una Maestría que se encuentra en un proceso de expansión mundial.
- **Créditos y duración:**
    - La Universidad de Tecnología de Troyes (Francia) ofrece un programa con 52 créditos, lo que indica que puede tener un enfoque más especializado o una duración más corta.

Perfil profesional del estudiante

- **Características demográficas:**
    - **Edad:** El rango de edad predominante se sitúa entre los 29 y 45 años.
    - **Género:** de los 67 estudiantes admitidos, el 80% son hombres y el 20% mujeres.
    - **Ubicación:** La mayoría de los estudiantes residen en Bogotá, aunque también hay un porcentaje bajo de estudiantes de otras regiones, y uno que reside fuera del país.
    - **Nivel socioeconómico:** Los estudiantes actualmente activos (55) pertenecen a los estratos 1 (2), 2 (20), 3(23) y 4(10).
- **Motivaciones y expectativas:**
    - **Factores que influyen en la elección del programa:**
        - La creciente demanda de profesionales en seguridad de la información en el mercado laboral.
        - El interés por adquirir conocimientos especializados en un área de alta relevancia tecnológica.
        - La búsqueda de mejores oportunidades laborales y salariales.
    - **Expectativas sobre el programa:**
        - Obtener una formación integral y actualizada en gestión y seguridad de la información.
        - Desarrollar habilidades teórico/prácticas para enfrentar los desafíos en la seguridad de la información. .
        - Obtener un título que les permita ascender profesionalmente.
- **Preferencias académicas:**
    - **Áreas de interés:**
        - Seguridad de la información.
        - Ciberseguridad.
        - Gestión de riesgos y cumplimiento normativo.
        - Análisis forense.
        - Seguridad en la nube y protección de datos.
        - Auditoria en seguridad de la información.
        -

    - **Preferencias educativas:**
        - Metodologías de aprendizaje teórica/prácticas.
        - Estudios de casos y simulaciones de escenarios reales.
        - Formación en el manejo de herramientas de software especializadas.

Satisfacción de los estudiantes

- **Encuestas de opinión:**
    - Los resultados de las encuestas realizadas a estudiantes en el año 2024 reflejaron un alto nivel de satisfacción general con el programa.
    - Entre los aspectos mejor valorados se refleja que el programa académico responde a las necesidades de la sociedad en relación con las políticas de desarrollo nacional, regional y local, la calidad del cuerpo docente y la pertinencia del plan de estudios.
- **Retroalimentación cualitativa:**
    - **Fortalezas:**
        - Los estudiantes destacan la actualización constante del plan de estudios, adaptado a las últimas tendencias en seguridad de la información.
        - Se valora la experiencia y el conocimiento de los docentes.
        - Los syllabus del programa cumplen con los propósitos de formación.
        - El material didáctico producido por los docentes tiene una buena aceptación por parte de los estudiantes.
    - **Áreas de mejora:**
        - Mantener una actualización permanente del material didáctico y de los syllabus..
        - Fortalecer la investigación y la publicación de artículos científicos.
        - Actualización de los recursos informáticos y de comunicación.
- **Expectativas y resultados:**
    - En general, el programa cumple con las expectativas iniciales de los estudiantes, especialmente en lo que respecta a la adquisición de conocimientos en gestión y seguridad de la información.
    - La Maestría genera un valor agregado al perfil profesional de los estudiantes.

Capacidad Institucional

- **Recursos académicos:**
    - La Maestría cuenta con docentes con experiencia académica y profesional en el campo de la seguridad de la información.
    - Los recursos educativos son pertinentes y apoyan los objetivos de la Maestría.
    - Se realiza una actualización permanente del material didáctico.
- **Infraestructura y tecnología:**
    - La disponibilidad y calidad de la infraestructura y los recursos educativos son generalmente buenos, aunque existen oportunidades de mejora en la actualización constante de los equipos.
    - La infraestructura y recursos tecnológicos utilizados en el programa incluyen:
        - Plataformas de aprendizaje virtual.
        - Material didáctico.
- **Capacidad administrativa:**
    - La Universidad cuenta con una estructura administrativa para gestionar y apoyar la Maestría.

- Los procesos de admisión, matrícula y seguimiento académico son en general aceptables, aunque se pueden optimizar los tiempos de respuesta a las solicitudes de los estudiantes.
- La Universidad cuenta con plataformas de gestión académica que facilitan los procesos administrativos.

- **Colaboraciones y alianzas:**
  - La Universidad específicamente la Maestría busca activamente nuevas alianzas para fortalecer el programa y ampliar las oportunidades para los estudiantes.

Estructura y Contenido del Programa

- **Descripción del programa:**
  - La estructura y el contenido de la malla curricular está diseñada para proporcionar una formación integral en Gestión y Seguridad de la Información, abarcando desde aspectos técnicos hasta aspectos de gestión y normativos. Por otro lado, se tiene en cuenta que este tipo de formación preste especial atención a la transmisión de conocimientos, habilidades y capacidades que, no sólo permitan a los egresados dominar una serie de tecnologías actuales que faciliten su rápida y correcta inserción en el mercado laboral, sino que también le permitan comprender y participar en la evolución de estas tecnologías. Así mismo, y de cara a liderar el desarrollo de la gestión y seguridad de la información, es muy importante que, en su proceso de formación, pueda conocer cómo las TIC han contribuido, contribuyen y pueden contribuir al desarrollo de determinados dominios socio-económicos. El proyecto curricular Maestría en Gestión y Seguridad de la Información está conformado por 40 créditos académicos, los cuales deben ser desarrollados en un periodo de tiempo de dos años (cuatro semestres académicos). Sin embargo, como se mencionó el trabajo que exige un proyecto curricular con metodología virtual requiere de una comprensión distinta de las actividades académicas.

Tabla 5.Plan de Estudios del Proyecto Curricular Maestría en Gestión y Seguridad de la Información.

Fuente: Proyecto Curricular Maestría en Gestión y Seguridad de la Información.

El plan de Estudios de la Maestría en Gestión y Seguridad de la Información está conformado por cuatro núcleos, como se observa en la tabla 6, un núcleo fundamental, un núcleo de énfasis, un núcleo electivo y un núcleo de investigación y desarrollo.

NOTA: la disponibilidad de las asignaturas electivas está sujeta a la oferta que realice el programa cada semestre.

Tabla 6. Núcleos que componen el plan de estudios Maestría en Gestión y Seguridad de la Información

NUCLEO FUNDAMENTAL	NUCLEO DE ENFASIS	NUCLEO ELECTIVO	NUCLEO DE INVESTIGACION
12 CREDITOS	12 CREDITOS	10 CREDITOS	6 CREDITOS

- ✓ El *núcleo de fundamentación* provee al estudiante herramientas conceptuales requeridas para abordar la solución a problemas de forma metódica. Este núcleo está compuesto por cuatro espacios académicos obligatorios, cada uno de tres créditos.
- ✓ El *núcleo de énfasis* consta de cuatro espacios académicos obligatorios, de tres y cuatro créditos, los cuales proporcionan temáticas con un mayor grado de profundidad.
- ✓ El *núcleo electivo* permite al estudiante profundizar en temáticas asociadas a su trabajo de investigación, aportando conocimientos específicos respecto al área de su interés. Este núcleo se compone de tres espacios académicos electivos, cada uno de tres créditos.
- ✓ Sumado a lo anterior, el *núcleo de investigación* y desarrollo orienta al estudiante en la formulación de proyectos que aporten soluciones a problemáticas reales. El núcleo de investigación está compuesto por dos espacios académicos que suman 6 créditos.

- En el tiempo de formación en la Maestría el contenido de las asignaturas se ha ido actualizando constantemente para reflejar las últimas tendencias y desafíos en el campo de la gestión y la seguridad de la información.
- Las áreas de especialización incluyen la ciberseguridad, gestión de riesgos, el análisis forense digital y seguridad en la nube, entre otros.
- El programa tiene una periodicidad de admisión semestral, los encuentros sincrónicos se programan entre lunes a jueves de 6 pm a 10 pm. Los espacios académicos del programa equivalen a cuarenta (40) créditos académicos.

- **Innovaciones pedagógicas:**
  - Se utilizan métodos de enseñanza innovadores, como casos de estudio y proyectos prácticos.
  - Se fomenta el aprendizaje colaborativo y el uso de herramientas tecnológicas.
  - Se promueve la participación en eventos académicos y la interacción con profesionales del sector.
- **Resultados del aprendizaje:**
  - Los estudiantes adquieren las competencias en la identificación y gestión de riesgos de seguridad de la información.
  - Desarrollan habilidades para diseñar e implementar estrategias de ciberseguridad efectivas.
  - Aprenden a gestionar incidentes de seguridad.
  - El egresado estará en la capacidad de tomar decisiones empleando metodologías, estándares y herramientas pertinentes al área de la seguridad de la información, evaluando y utilizando soluciones tecnológicas de acuerdo con las necesidades de operación, comunicación y protección de los datos de las organizaciones.
- **Cambios en el currículo:**
  - El programa se actualiza periódicamente para incorporar nuevas tecnologías y tendencias en el campo de la seguridad de la información.
  - Se realizan ajustes en el contenido de las asignaturas para garantizar su relevancia y pertinencia.
  - La actualización curricular que ha hecho el programa, es el de mantener actualizado el programa de acuerdo a las tendencias mundiales y las necesidades del mercado, preparando a los profesionales para enfrentar los desafíos de la seguridad de la información en un entorno cada vez más digitalizado.
  -

- **Adaptabilidad:**
  - El programa tiene la capacidad de adaptarse a los cambios en la demanda del mercado laboral y a las nuevas tendencias educativas.
  - Con un enfoque en la ciberseguridad y la gestión de riesgos, este programa capacita para diseñar e implementar estrategias de seguridad robustas, asegurando la integridad y confidencialidad de la información.

- **Estructura curricular:**
  - El programa consta de un conjunto de materias obligatorias y electivas que cubren los diferentes aspectos de la gestión y seguridad de la información.
  - Los requisitos de graduación incluyen la aprobación de todas las materias y la elaboración de un trabajo de grado (monografía o artículo de revisión).
  - La Maestría en Gestión y Seguridad de la Información está dirigida a profesionales relacionados con las áreas de Telemática, Sistemas, Telecomunicaciones, Electrónica, Industrial, y afines que deseen profundizar en la gestión y la seguridad de la información.

Evaluación Financiera

- **Análisis de costos:**
  - **Costos de desarrollo:**
    - *Plan de estudios*: lo genera un profesor de planta de UD, el cual le puede dedicarle 40 horas, por lo que es el costo podría ser aproximadamente de $10.000.000
    - *Contenidos de autor*: se pueden estimar los siguientes costos por asignatura:
      - Contratación de profesor especializado: $4.500.000
      - Revisor y editor: $4.500.000.
  - **Costos de implementación:**
    - Las necesidades de infraestructura tecnológica, para el desarrollo de la Maestría, se asocia a la aula virtual (Moodle) y conexión a Internet.
  - **Costos de operación:** para una cohorte de 16 estudiantes con costos del 2024, y teniendo en cuenta las siguientes consideraciones:
    (1) Los ingresos presupuestados no consideran tasa de deserción
    (2) Los descuentos por diferentes ítems se consideran de un 35% por semestre.
    (3) Se considerando una dedicación de 10 horas semanales a la Coordinación del programa de postgrado por parte de un docente de planta.
    (4) El apoyo profesional es proporcional al número de programas (2) que atiende.
    (5) El valor hora docente $290.000 aproximadamente, incluido factor prestacional.
    (6) La cantidad de docentes por cada periodo académico son: 4, 4, 4, 2.
    (7) Para el tercer y cuarto semestre se considera un incremento del 5% tanto para ingresos como para egresos.

A continuación, se muestra los costos de operación.

Tabla 7.Presupuesto por Cohorte Maestría en Gestión y Seguridad de la Información

Maestría en Gestión y Seguridad de la Información Presupuesto por cohorte			
Número de estudiantes inscritos	16	**Valor Crédito**	$ 650,000.00

CONCEPTO	Q	Tiempo horas semanales	Valor Unitario	Valor anual			
				Semestre I	Semestre II	Semestre III	Semestre IV
Número de créditos				**12**	**12**	**10**	**6**
INGRESOS							
Inscripciones	16		174,300	2,788,800	0	0	0
Matrícula (1)	16		7,800,000	124,800,000	124,800,000	109,200,000	65,520,000
Total ingresos				**127,588,800**	**124,800,000**	**109,200,000**	**65,520,000**
EGRESOS							
Descuentos							
Descuentos por certificado electoral, Descuento egresados, hijos de funcionarios, becas (2)				43,680,000	43,680,000	38,220,000	22,932,000
Costos y gastos de funcionamiento							
Gastos administrativos							
Coordinador de Maestría (3)	1	10.00	53,542	8,566,667	8,566,667	8,995,000	8,995,000
Apoyo asistencial	1	40.00	12,410	7,942,253	7,942,253	8,339,366	8,339,366
Apoyo profesional (4)	1	20.00	22,834	7,306,877	7,306,877	7,672,221	7,672,221
Costos de docencia							
Créditos (5)(6)			290,000	37,120,000	37,120,000	38,976,000	19,488,000
Gastos generales							
Otros			200,000	1,000,000	1,000,000	1,050,000	1,050,000
Subtotal costos y gastos				**105,615,797**	**105,615,797**	**103,252,587**	**68,476,587**
Diferencia (7)				**21,973,003**	**19,184,203**	**5,947,413**	**-2,956,587**

Total ingresos: $427.108.800
Total Egresos : $382.960.769
Utilidad : $ 44.148.031
% de utilidad : 10.34

OBSERVACIÓN: En el presupuesto del primer semestre no se tiene cubierto los costos en que incurre la Maestría, como apoyo a los estudiantes de Graduación Oportuna y Modalidad de Grado, los cuales se les asigna cupos (7 y 8 respectivamente) en las asignaturas de Seguridad de la Informacion, Ciberseguridad y Arquitectura Empresarial.

Desempeño del Programa

- **Tendencias de matrícula:**
  - El interés en la seguridad de la información ha aumentado significativamente en los últimos años, lo que se refleja en un incremento estable en las inscripciones y matrículas de la Maestría.

- Este crecimiento puede atribuirse a la creciente conciencia sobre los riesgos cibernéticos y la demanda de profesionales capacitados en este campo.

- **Retención y graduación:**
  - Desde el inicio de actividades académicas de la Maestría (2022-II) a la fecha se han admitidos 67 estudiantes, de los cuales 40 estudiantes están cursando asignaturas, 14 están en el proceso de la realización del proyecto de grado, 4 se han graduado (2024-3) y el resto han aplazado semestre o simplemente no continuaron con sus estudios.
  - Esta tasa de retención sugiere que los estudiantes están satisfechos con el programa y encuentran que cumple con sus expectativas.
  - A pesar de llevar activa académicamente únicamente dos años y medio ya existen 4 graduandos.
- **Rendimiento académico:** a continuación se detalla el rendimiento académico de los estudiantes de la Maestría.

Tabla 8. Rendimiento académico estudiantes MGSI.

Periodo académico	2022-3	2023-1	2023-3	2024-1	2024-3
Total asignaturas	4	8	12	14	12
Número de Estudiantes	19	22	34	38	33
Promedio semestre	44	44	45	42	43
Numero estudiantes y asignaturas perdidas por semestres	1(1)	0	3(6)	3 (3)	1(3)
Tasa de aprobación	99%	100%	99%	97.5%	99%

Inscritos, admitidos, matriculados y graduados

Tabla 9 Estado inscritos, admitidos y matriculados

Nombre de la IES	Denominación	Modalidad	Inscritos	Admitidos	Matriculados en 1er curso	Periodo	Año
Universidad Distrital F.J.C. – Facultad Tecnológica.	Maestría en Gestión y Seguridad de la Informacion.	Virtual	19	19	19	II	2022
			3	3	0	I	2023
			12	12	12	II	2023
			9	9	9	I	2024
			12	12	12	II	2024
			14	12	12	I	2025

Fuente: Coordinación MGSI

Conclusiones Generales:

- **Tasa de admisión y matrículas:**
  - La Maestría en Gestión y Seguridad de la Información en la Universidad Distrital F.J.C. – Facultad Tecnológica presenta una tasa de admisión y matrícula del 100% en la mayoría de los periodos.
  - La Universidad tiene una capacidad para admitir a todos los solicitantes cualificados.
- **Modalidad virtual establecida:**
  - El programa se ofrece en modalidad virtual, lo que puede explicar la consistencia en el número de inscritos, admitidos y matriculados. La modalidad virtual permite mayor flexibilidad y accesibilidad.
- **Crecimiento consistente:**
  - Con la excepción del primer periodo del 2023, se observa una estabilidad relativa en el número de estudiantes matriculados en cada periodo, lo que sugiere una tendencia positiva y un interés creciente en el programa.
- **Estabilidad en la demanda:**
  - Los números de inscritos se mantienen relativamente estables a lo largo de los periodos, lo que indica una demanda constante del programa.

Tabla 10. Estado de graduados

Nombre de la IES	Denominación	Modalidad	Graduados	Periodo	Año
Universidad Distrital F.J.C.	Maestría en Gestión y Seguridad de la Información.	Virtual	4	3	2024

Fuente: Coordinación MGSI.

A pesar de llevar activa académicamente únicamente dos años y medio ya existen 4 graduandos.

Demanda de Mercado laboral del programa

A continuación, se presenta un análisis detallado de la demanda del mercado laboral para este programa:

1. Necesidades del mercado laboral:

- **Identificación de necesidades:**
  - El aumento de los ciberataques, la protección de datos personales y la necesidad de garantizar la seguridad de la infraestructura crítica son algunos de los factores que impulsan la demanda de expertos en seguridad de la información. *Fortinet* han ubicado a Colombia como uno de los países con mayores registros de ataques en América Latina, con miles de millones de intentos de ciberataques, por otro lado, la Policía Nacional estimó que los ciberataques en el primer semestre de 2023 se redujeron en un 2% en comparación al mismo periodo del año inmediatamente anterior, pasando de 24.111 casos, a 23.640. Lo anterior se traduce en un promedio de 168 delitos cibernéticos al día. Fuente: https://linktic.com/blog/panorama-completo-de-la-ciberseguridad-en-colombia/

    - Existe una creciente necesidad de profesionales capaces de gestionar riesgos, analizar vulneralidades, implementar políticas de seguridad y responder a incidentes de seguridad.
- **Relevancia del programa:**
    - El programa de la Universidad Distrital aborda estas necesidades al proporcionar una formación integral en gestión y seguridad de la información, que incluye aspectos técnicos, legales y de gestión.
    - La actualización constante del plan de estudios garantiza que los graduados estén preparados para enfrentar los desafíos del mercado laboral.
- **Transformación digital:**
    - La adopción de tecnologías como la nube, el Internet de las Cosas (IoT) y la Inteligencia Artificial (IA) amplía la superficie de ataque cibernético.
    - La gestión de la seguridad en estos entornos complejos requiere profesionales con conocimientos avanzados y habilidades de liderazgo.
    - La Maestría aborda estas necesidades emergentes, preparando a los egresados para enfrentar los desafíos de la seguridad en la era digital.

2. Oportunidades de empleo:

- **Análisis de oportunidades:**
    - Los graduados de este programa pueden encontrar empleo en una amplia gama de sectores, incluyendo el gobierno, la banca, las telecomunicaciones, la industria y el sector de la tecnología.
    - Las oportunidades de empleo incluyen puestos como:
        - Gerente de seguridad de la información.
        - Analista de seguridad.
        - Auditor de seguridad.
        - Consultor de ciberseguridad.
        - Analista forense digital.

3. Proyecciones de crecimiento:

- **Mercado en expansión:**
    - Se espera que el mercado laboral de la seguridad de la información continúe creciendo en los próximos años, impulsado por la digitalización de la economía y la creciente sofisticación de los ciberataques.
    - La inversión en seguridad de la información se considera cada vez más una prioridad estratégica para las organizaciones.
- **Nuevas tecnologías:**
    - La adopción de tecnologías emergentes, como la Inteligencia Artificial y el aprendizaje automático, está transformando el panorama de la seguridad cibernética. Si bien estas tecnologías pueden ser utilizadas para realizar ataques más sofisticados, también ofrecen herramientas avanzadas para la defensa y protección de la información.

4. Competencias adquiridas:

- **Habilidades técnicas:**
    - Análisis de riesgos y vulnerabilidades.
    - Diseño e implementación de estrategias de ciberseguridad.
    - Análisis forense digital.
    - Auditoría en seguridad de la información.

- **Habilidades de gestión:**
  - Liderazgo y gestión de equipos de seguridad.
  - Conocimiento de normativas y regulaciones de seguridad de la información.
  - Gestión de proyectos de seguridad.
  - Toma de decisiones estratégicas.

5. Inserción Laboral:

- **Tasa empleabilidad:**
  - Aunque no se disponen de datos específicos de inserción laboral para este programa en Colombia, la alta demanda de profesionales en seguridad de la información sugiere una tasa de empleabilidad favorable. Fuente: Mintic
- **Roles relevantes:**
  - Los egresados suelen ocupar roles de liderazgo y gestión en áreas de seguridad de la información.

6. Opinión de empleadores:

- **Retroalimentación de empleadores:**
  - Por ser un programa aun joven no existe un estudio sobre el desempeño de los graduados.
  - Es importante que la Universidad implemente un plan de comunicación constante con los empleadores para conocer sus necesidades y adaptar el programa en consecuencia.

Referencias Gremiales y Académico-Profesionales:

- **Asociaciones:**
  - ISACA (Information Systems Audit and Control Association).
  - (ISC)² (International Information System Security Certification Consortium).
  - IEEE (Institute of Electrical and Electronics Engineers).
- **Federaciones:**
  - Federación Colombiana de Ingenieros (FCI).

Análisis descriptivo:

- La Maestría en Gestión y Seguridad de la Información responde a una necesidad crítica del mercado laboral actual.
- La demanda de profesionales en este campo seguirá creciendo debido a la digitalización y el aumento de las amenazas cibernéticas.
- Los egresados tienen amplias oportunidades de empleo en diversos sectores y pueden ocupar roles de liderazgo y gestión.
- La combinación de habilidades técnicas y de gestión adquiridas en el programa los prepara para enfrentar los desafíos de la seguridad en la era digital.

Análisis de la deserción de programas iguales o con denominaciones similares

El análisis de la deserción en programas de Maestría relacionados con la seguridad de la información en Colombia revela tendencias significativas que afectan la continuidad académica de los estudiantes. A continuación, se detallan los hallazgos más relevantes:

1. Tasas generales de deserción en Posgrados:

- **Maestrías:** según datos del Ministerio de Educación Nacional, la deserción en programas de Maestría alcanza el 47% después de cuatro semestres de observación. Este incremento notable en el cuarto semestre podría estar asociado a desafíos relacionados con el trabajo de grado.
- **Especializaciones:** presentan una deserción del 53% en el mismo período, con un aumento significativo entre el primer y segundo semestre.
- **Doctorados:** registran una deserción menor, del 27%, en comparación con Maestrías y Especializaciones.

  Fuente: Ministerio de Educación

2. Factores contribuyentes a la deserción:

- **Metodología de estudio:** los posgrados virtuales, en general, tienden a tener tasas de deserción más altas que los presenciales debido a la necesidad de mayor autodisciplina y gestión del tiempo.
- **Servicios académicos y currículo:** factores como la atención al estudiante, dificultades tecnológicas y problemas con la plataforma educativa, así como deficiencias en el currículo, influyen significativamente en la deserción en programas virtuales de posgrado.
- **Factores influyentes:** factores socioeconómicos, dificultades tecnológicas, falta de apoyo académico y problemas personales impactan la deserción en todos los niveles de posgrado.

Se puede concluir que:

- Las Especializaciones suelen tener tasas de deserción más bajas en comparación con las Maestrías y los Doctorados. Esto podría deberse a su duración más corta y a su enfoque más práctico y orientado al mercado laboral.
- Las Maestrías, especialmente las de investigación, pueden presentar tasas de deserción más elevadas debido a la exigencia académica y la necesidad de desarrollar proyectos de investigación. Las Maestrías virtuales pueden aumentar esta tendencia debido a la falta de interacción presencial y la necesidad de autogestión.
- Los Doctorados suelen tener las tasas de deserción más altas debido a su larga duración, la alta exigencia investigativa y la necesidad de dedicación exclusiva. Los Doctorados virtuales presentan desafíos adicionales, como la necesidad de realizar investigación independiente y la falta de interacción presencial con otros investigadores.

Fuente:

- **SPADIES:**
  - El Sistema de Prevención y Análisis de la Deserción en las Instituciones de Educación Superior (SPADIES) del Ministerio de Educación Nacional recopila

datos sobre deserción, pero no siempre desglosa la información por tipo de posgrado virtual.

3. Desafíos específicos en Programas de Seguridad de la Información:

Aunque no se dispone de datos específicos de deserción para programas de Maestría en Seguridad de la Información en Colombia, es razonable inferir que enfrentan desafíos similares a otros programas de posgrado. La complejidad técnica de estos programas, sumada a las posibles dificultades en la conciliación entre estudios, trabajo y vida personal, podría contribuir a tasas de deserción comparables o incluso superiores al promedio.

Análisis de oportunidades de desarrollo socioeconómico, tecnológico o cultural que se pueden materializar con el proyecto curricular

La Maestría en Gestión y Seguridad de la Información de la Universidad Distrital - Facultad Tecnológica ofrece diversas oportunidades de desarrollo socioeconómico, tecnológico y cultural, tanto para los estudiantes como para la sociedad en general. A continuación, se detallan algunas de estas oportunidades:

Desarrollo socioeconómico:

- **Generación de empleo:**
  - El programa contribuye a la formación de profesionales altamente capacitados en un área de alta demanda, lo que aumenta sus oportunidades de empleo y mejora sus ingresos.
  - Se puede dar un impulso a la economía digital, lo que puede garantizar la seguridad de las transacciones y la información en línea, fomentando el crecimiento del comercio electrónico y los servicios digitales.
- **Fortalecimiento del sector empresarial:**
  - Los graduados de la Maestría pueden ayudar a las empresas a proteger sus activos de información, reducir riesgos y mejorar su competitividad. Esto es especialmente importante en la era digital, donde la seguridad de la información es crucial para el éxito de las empresas.
- **Desarrollo de políticas públicas:**
  - El programa puede contribuir a la formación de profesionales capaces de diseñar e implementar políticas públicas en materia de seguridad de la información. Esto es fundamental para proteger a los ciudadanos y a las instituciones públicas de los ciberataques.

Desarrollo tecnológico:

- **Impulso a la innovación:**
  - El programa formará líderes capaces de diseñar e implementar políticas de seguridad alineadas con la estrategia organizacional, mejorando la resiliencia cibernética y la competitividad empresarial en el ámbito nacional e internacional. Esto puede conducir a la creación de nuevas empresas y productos que mejoren la seguridad digital.
- **Fortalecimiento de la infraestructura digital:**
  - Los graduados de la Maestría pueden contribuir a la protección de la infraestructura digital del país, lo que es esencial para el desarrollo de la economía digital.

- **Adaptación a nuevas tendencias:**
    - La Maestría puede impulsar la investigación y el desarrollo de nuevas tecnologías y soluciones para proteger la información.
    - Los egresados pueden aplicar sus conocimientos en empresas y organizaciones, mejorando sus capacidades en ciberseguridad.

Desarrollo cultural:

- **Concientización sobre la seguridad de la información:**
    - La Maestría puede contribuir a crear conciencia sobre la importancia de la seguridad de la información en la sociedad.
- **Promoción de la ética profesional:**
    - La Maestría puede fomentar la reflexión sobre los dilemas éticos relacionados con la ciberseguridad y el uso de la tecnología.
- **Fortalecimiento de la identidad digital:**
    - La formación en ciberseguridad promueve el respeto por la privacidad de los datos personales y la protección de los derechos digitales.

Fuentes:

- I**ntegración de Inteligencia Artificial (IA) en la Seguridad de la Información (**5 tendencias en ciberseguridad que marcarán el futuro a partir de 2025).
- **Formación en Ciberseguridad Orientada a la Gestión Estratégica (**5 tendencias en formación TIC para 2025).
- **Enfoque en la Seguridad de Infraestructuras Críticas y Sectores Estratégicos (**Cadena SER).
- **Gestión de Riesgos y Cumplimiento Normativo (**IEEE).

Análisis de las estrategias

Se realiza un análisis de características más sobresalientes de los cinco (5) programas que tienen mayor participación de mercado en la actualidad.

Análisis de programas de Maestría con mayor participación en el mercado:

1. Magíster en Seguridad de la Información - Universidad de los Andes.

- **Enfoque formativo:** este programa está diseñado para formar directores de seguridad de la información (CISO) y responsables de la toma de decisiones en seguridad de la información y comunicaciones dentro de las organizaciones.
- **Fortalezas**: prestigio de la universidad, conexiones con la industria, cuerpo docente altamente calificado.
- **Características sobresalientes**: énfasis en la investigación y la innovación.

2. Magíster en Ciberseguridad - Universidad Nacional Abierta y a Distancia (UNAD).

- **Enfoque formativo:** este programa se centra en la formación de especialistas capaces de gestionar análisis de riesgos, auditorías y protección contra amenazas al software en entornos tanto públicos como privados.
- **Fortalezas**: cobertura nacional, flexibilidad, enfoque en la aplicación práctica.
- **Características sobresalientes**: flexibilidad de estudio, gran alcance nacional.

3. Magíster en Seguridad Informática y de las Comunicaciones - Universidad Piloto de Colombia.

- **Enfoque formativo:** este programa busca formar profesionales con habilidades para diseñar, implementar y gestionar sistemas de seguridad informática y de comunicaciones, protegiendo la información y los recursos tecnológicos de las organizaciones.
- **Fortalezas**: Enfoque interdisciplinario, formación en áreas convergentes.
- **Características sobresalientes**: Integración de redes y seguridad.

4. Magíster en Seguridad Digital - Pontificia Universidad Javeriana.

- **Enfoque formativo:** este programa está orientado a la formación de expertos en seguridad digital, capaces de abordar desafíos relacionados con la protección de datos y la privacidad en entornos digitales.
- **Fortalezas**: formación humanística, énfasis en la responsabilidad social.
- **Características sobresalientes**: énfasis en la ética y la legislación.

5. Magíster en Seguridad de la Información - Universidad de Manizales.

- **Enfoque formativo:** este programa se enfoca en la formación de profesionales capaces de gestionar la seguridad de la información, implementando políticas y estrategias que protejan los activos informáticos de las organizaciones.
- **Fortalezas**: enfoque práctico, alineación con estándares internacionales.
- **Características sobresalientes**: gestión de riesgos y cumplimiento normativo.

Desafíos para la Maestría en Gestión y Seguridad de la Información de la Universidad Distrital:

- **Desafíos académicos:**
  - *Mantener un currículo actualizado*: la ciberseguridad evoluciona rápidamente, por lo que el programa debe adaptarse constantemente a las nuevas amenazas y tecnologías.
  - *Integrar investigación y práctica*: equilibrar la formación teórica con la aplicación práctica de los conocimientos mediante laboratorios virtuales, simulaciones y casos de estudio reales.
  - *Fomentar la investigación*: estimular a los estudiantes a participar en proyectos de investigación que generen conocimiento innovador.
- **Desafíos formativos:**
  - *Desarrollar habilidades blandas*: además de las habilidades técnicas, los egresados necesitan habilidades de liderazgo, comunicación y gestión de equipos.
  - *Adaptar la formación a la modalidad virtual*: asegurar la calidad de la enseñanza y el aprendizaje en un entorno virtual.
  - *Fomentar la ética profesional*: promover una cultura de responsabilidad y ética en el uso de la tecnología.
- **Desafíos de extensión:**
  - *Establecer alianzas con la industria*: establecer alianzas con empresas y organizaciones gubernamentales para facilitar prácticas profesionales, asegurando que la formación responda a las necesidades del mercado laboral.
  - *Difundir el conocimiento*: organizar eventos y actividades de divulgación para crear conciencia sobre la importancia de la ciberseguridad.

    - *Generar proyectos de impacto social*: desarrollar proyectos que aborden problemáticas locales y regionales en seguridad de la información, contribuyendo al desarrollo científico y tecnológico del país.
- **Desafíos científicos:**
    - *Promover la investigación interdisciplinaria*: fomentar la colaboración entre diferentes áreas del conocimiento para abordar los desafíos de la ciberseguridad.
    - *Participar en redes de investigación*: establecer alianzas con otras universidades y centros de investigación a nivel nacional e internacional.
    - *Contribuir a la generación de políticas públicas*: alinear el programa con las políticas y regulaciones nacionales en materia de seguridad digital, garantizando que los egresados estén capacitados para cumplir y asesorar en el cumplimiento de dichas normativas.

ESTUDIO DEL ENTORNO NACIONAL E INTERNACIONAL

Estudio del entorno nacional e internacional

1. Tendencias mundiales:

- **Economía digital y ciberseguridad:**
    - El crecimiento exponencial de la economía digital ha incrementado la exposición a ciberataques, generando una demanda global de expertos en seguridad de la información.
    - Tendencias como el Internet de las Cosas (IoT), la inteligencia artificial y la computación en la nube plantean nuevos desafíos en materia de seguridad.
- **Regulaciones y normativas:**
    - Países y organizaciones internacionales están implementando regulaciones más estrictas sobre protección de datos y ciberseguridad (GDPR, ISO 27001, etc.). Esto genera una demanda creciente de profesionales que puedan garantizar el cumplimiento normativo.
- **Transformación digital:**
    - La creciente adopción de tecnologías emergentes como la Inteligencia Artificial, Blockchain y el Internet de las cosas (IoT), crea nuevas oportunidades para expertos en seguridad de la información en diversos sectores (salud, finanzas, educación, etc.).
- **Amenazas cibernéticas:**
    - La sofisticación de los ciberataques, incluyendo el ransomware y los ataques dirigidos, exige profesionales con habilidades avanzadas en detección y respuesta a incidentes.

2. Entorno nacional y regional:

- **Políticas públicas y programas:**
    - En Colombia, el Gobierno ha implementado políticas y estrategias para fortalecer la ciberseguridad, como el CONPES 3995 de 2020, que busca mejorar la seguridad digital del país.
    - Los planes de desarrollo y los Objetivos de Desarrollo Sostenible (ODS) también incluyen metas relacionadas con la seguridad digital y la protección de datos.
- **Variables sociales:**
    - El aumento del uso de internet y dispositivos móviles en Colombia incrementa la exposición a riesgos cibernéticos.

    - El Índice de Gin, aunque ha mejorado en los últimos años, la desigualdad sigue siendo un reto, lo que implica oportunidades para la inclusión digital y la seguridad de la información en sectores menos favorecidos.
    - La demanda de expertos en ciberseguridad y gestión de la información ha aumentado, pero existe un déficit de talento calificado.
- **Variables económicas:**
    - El crecimiento de sectores como el de las tecnologías de la información y las comunicaciones (TIC) y el comercio electrónico genera una demanda creciente de expertos en ciberseguridad.
    - La competitividad y el emprendimiento en el sector digital dependen en gran medida de la capacidad de las empresas para proteger sus activos de información.

3. Oportunidades de desempeño laboral:

- **Necesidades del País:**
    - Colombia enfrenta desafíos importantes en materia de ciberseguridad, incluyendo la protección de infraestructuras críticas y la prevención de fraudes cibernéticos.
    - Existe una alta demanda de profesionales en ciberseguridad en Colombia, tanto en el sector público como en el privado.
    - Las regiones con mayor concentración de empresas tecnológicas y financieras (Bogotá, Medellín, Cali) ofrecen más oportunidades laborales.
- **Campos de desempeño:**
    - Los egresados de la Maestría pueden desempeñarse en roles como:
        - Gerentes de seguridad de la información.
        - Analistas de ciberseguridad.
        - Consultores de seguridad.
        - Auditores en seguridad de la información.
        - Investigadores en ciberseguridad.
- **Articulación con el Programa:**
    - Es necesario que el programa de Maestría se articule con las necesidades del país, ofreciendo una formación actualizada y relevante para el mercado laboral. Esto incluye la inclusión de temas como:
        - Ciberseguridad en infraestructuras críticas.
        - Protección de datos personales.
        - Gestión de riesgos cibernéticos.
        - Ciberseguridad en la nube.
        - Análisis forense digital.

Informe de percepción y validación del programa con posible público objetivo

Se aplica una encuesta en línea al sector empleador-estudiantes potenciales, la ficha técnica de la encuesta como el informe de la encuesta va como un anexo, en este numeral se incorpora el análisis de cada una de las estadísticas.

1. Metodología de recolección de datos:

- **Encuesta:** se diseñó una encuesta para determinar la percepción del programa (anexo A).

2. Análisis de la percepción del programa:

- **Relevancia del plan de estudios:**
  - El contenido curricular de la MGSI responde a las necesidad del sector académico y profesional.
- **Calidad del cuerpo docente:**
  - La experiencia y el conocimiento de los docentes apoya en gran medida los objetivos de la MGSI..
  - La MGSI cuenta con una plataforma virtual para los encuentros sincrónicos, como apoyo a la labor académica.
- **Infraestructura y recursos:**
  - La MGSI cuenta con una plataforma virtual para los encuentros sincrónicos, como apoyo a la labor académica.
- **Reputación de la Universidad Distrital:**
  - La Universidad cuenta con una aceptable percepción sobre la calidad académica.

3. Validación del Programa con el público objetivo:

- **Necesidades del mercado laboral:**
  - Debido a la transformación digital, Colombia enfrenta desafíos en la ciberseguridad, lo que requiere una gran demanda de profesionales en esta área tanto a nivel público como privado.
- **Oportunidades de empleo:**
  - Actualmente en el entorno de la seguridad de la información, los estudiantes de la MGSI tienen una buena perspectiva de empleo. Los egresados se pueden desempeñar como: gerentes en gestión y seguridad de la información, analistas, consultores y auditores en seguridad de la información, entre otros.
- **Expectativas de los posibles estudiantes:**
  - La MGSI a través del tiempo se ha dado a conocer dentro del ámbito académico, lo que generado expectativas en los posibles nuevos estudiantes, que consideran la Maestría un programa de calidad, relevancia y oportunidades de desarrollo profesional.

4. Recomendaciones y mejoras:

- **Adaptación del plan de Estudios:**
  - Continuar con los ajustes en el plan de estudios para mejorar su relevancia y pertinencia.
- **Fortalecimiento del cuerpo docente:**
  - Promover la actualización y capacitación de los profesores.
- **Mejora de la Infraestructura y Recursos:**
  - Invertir en la adquisición y actualización de laboratorios y software.
- **Estrategias de promoción:**
  - Desarrollar estrategias de marketing y comunicación para dar a conocer el programa.
  - Establecer alianzas con empresas y organizaciones del sector.

Matriz FODA: Maestría en Gestión y Seguridad de la Información - Universidad Distrital

Fortalezas **(Ventajas Internas)**	**Oportunidades** **(Factores Externos Favorables)**
• **Cuerpo docente calificado:** docentes con experiencia académica y profesional en el sector.	• **Creciente demanda laboral:** aumento de la necesidad de expertos en ciberseguridad a nivel global y nacional.
• **Plan de estudios actualizado:** el contenido del plan de estudios es relevante y está adaptado a las tendencias del mercado.	• **Avances tecnológicos:** desarrollo de nuevas tecnologías y herramientas de ciberseguridad.
• **Reputación de la Universidad Distrital:** reconocimiento de la institución en el ámbito académico y profesional.	• **Políticas gubernamentales:** impulso a la ciberseguridad y la protección de datos por parte del gobierno.
	• **Colaboraciones y alianzas:** posibilidad de establecer convenios con empresas y organizaciones del sector.
	• **Concientización sobre la ciberseguridad:** mayor preocupación por la protección de datos y la seguridad digital en la sociedad.
Debilidades **(Áreas Internas que Requieren Mejoras)**	**Amenazas** **(Riesgos Externos que Podrían Impactar Negativamente)**
• **Recursos tecnológicos limitados:** necesidad de actualizar y ampliar la infraestructura tecnológica (laboratorios virtuales, herramientas de software especializadas).	• **Competencia de otros programas:** Existencia de otras Maestrías en ciberseguridad en universidades nacionales e internacionales.
• **Procesos administrativos:** oportunidad de optimizar los procesos de admisión, matrícula y seguimiento académico.	• **Cambios en el mercado laboral:** evolución rápida de las tecnologías y las necesidades del sector.
• **Visibilidad del programa:** necesidad de fortalecer la promoción y difusión de la Maestría.	• **Recesión económica:** posible disminución de la inversión en educación y capacitación.
• **Apoyo a la investigación:** oportunidad de fortalecer el apoyo a la investigación y la publicación de artículos científicos.	• **Ciberataques y incidentes de seguridad:** riesgo de ataques a la infraestructura tecnológica de la universidad.
• **Retroalimentación de los egresados:** oportunidad de fortalecer el seguimiento a los egresados y la obtención de retroalimentación sobre su desempeño laboral.	• **Regulaciones y normativas:** cambios constantes en las regulaciones y normativas de ciberseguridad.

Análisis de la Matriz:

- **Fortalezas y oportunidades:** la Maestría cuenta con fortalezas importantes que le permiten aprovechar las oportunidades del mercado. La calidad del cuerpo docente y el plan de estudios actualizado son ventajas competitivas.
- **Debilidades y Amenazas:** es importante abordar las debilidades internas y mitigar las amenazas externas para garantizar el éxito del programa. La inversión en recursos tecnológicos y la optimización de procesos administrativos son áreas clave de mejora.

CONCLUSIONES

Viabilidad y pertinencia:

- **Denominación:**
  - La denominación es adecuada y refleja las competencias clave del programa.
  - Existe una alta demanda de profesionales en gestión y seguridad de la información.
- **Pertinencia:**
  - El programa responde a las necesidades del mercado laboral, tanto a nivel nacional como internacional.
  - El plan de estudios está alineado con las tendencias y desafíos actuales en ciberseguridad.
  - El programa tiene una alta pertinencia debido al auge de la información y la importancia de su protección.

Características del Programa:

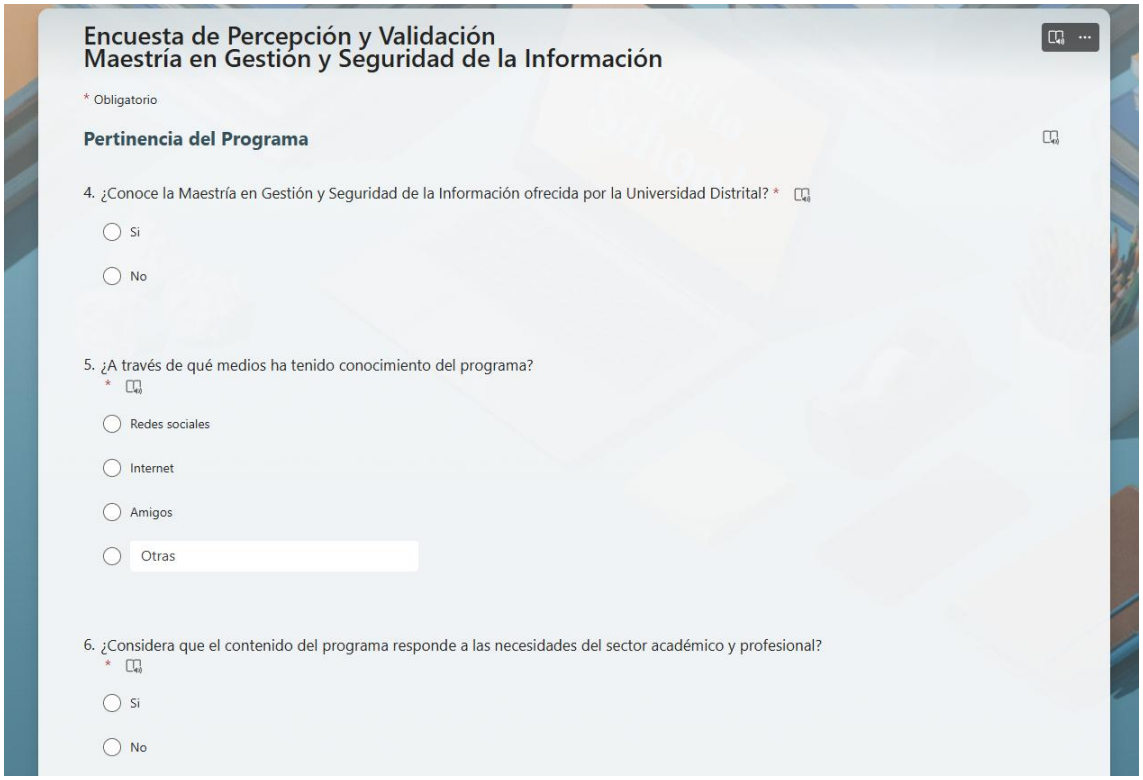
- **Modalidad:**
  - Se recomienda mantener la flexibilidad de la modalidad virtual, para ampliar el acceso a profesionales de diferentes regiones.
- **Rango de créditos académicos:**
  - Los 40 créditos académicos, se consideran adecuados para la formación integral en el área.
- **Períodos académicos:**
  - Se mantiene la periodicidad de admisión semestral, los encuentros sincrónicos se programan entre lunes a jueves de 6 pm a 10 pm.
- **Nicho de mercado:**
  - El programa se dirige a profesionales en áreas de TI, seguridad informática, gestión de riesgos y afines, con un enfoque en aquellos que buscan especialización y ascenso profesional (áreas de Telemática, Sistemas, Telecomunicaciones, Electrónica, Industrial, y afines).
- **Análisis integral:**
  - El análisis FODA revela fortalezas importantes, como un cuerpo docente calificado y un plan de estudios actualizado.
  - Las oportunidades externas, como la creciente demanda laboral y las políticas gubernamentales, respaldan la viabilidad del programa.
  - Es importante trabajar en las debilidades internas, como la actualización de recursos tecnológicos y la optimización de procesos administrativos.
  - Los egresados de la Maestría en Gestión y Seguridad de la Información tienen una alta posibilidad de empleabilidad.

En conclusión, la Maestría en Gestión y Seguridad de la Información de la Universidad Distrital es viable y pertinente, con un nicho de mercado bien definido y un alto potencial de impacto en el desarrollo socioeconómico y tecnológico del país.

ANEXO A


Encuesta de Percepción y Validación
Maestría en Gestión y Seguridad de la Información
6 mar 2025
El propósito de este formulario es evaluar la pertinencia, calidad, y alineación con las necesidades del sector académico y profesional y validación del programa Maestría en Gestión y Seguridad de la Información con posible público objetivo.
Empezar ahora


Encuesta de Percepción y Validación
Maestría en Gestión y Seguridad de la Información
* Obligatorio
Datos Generales
1. Digite su código de estudiante UD y/o número de cedula
Escriba su respuesta
2. Dirección de correo electrónico *
Escriba su respuesta
3. ¿Cuál es su perfil?
Docente Universitario
Estudiante universitario
Estudiante de posgrado
Investigador en el área
Profesional del sector TI / Seguridad de la Información
Profesional otras areas del conocimiento



Encuesta de Percepción y Validación
Maestría en Gestión y Seguridad de la Información

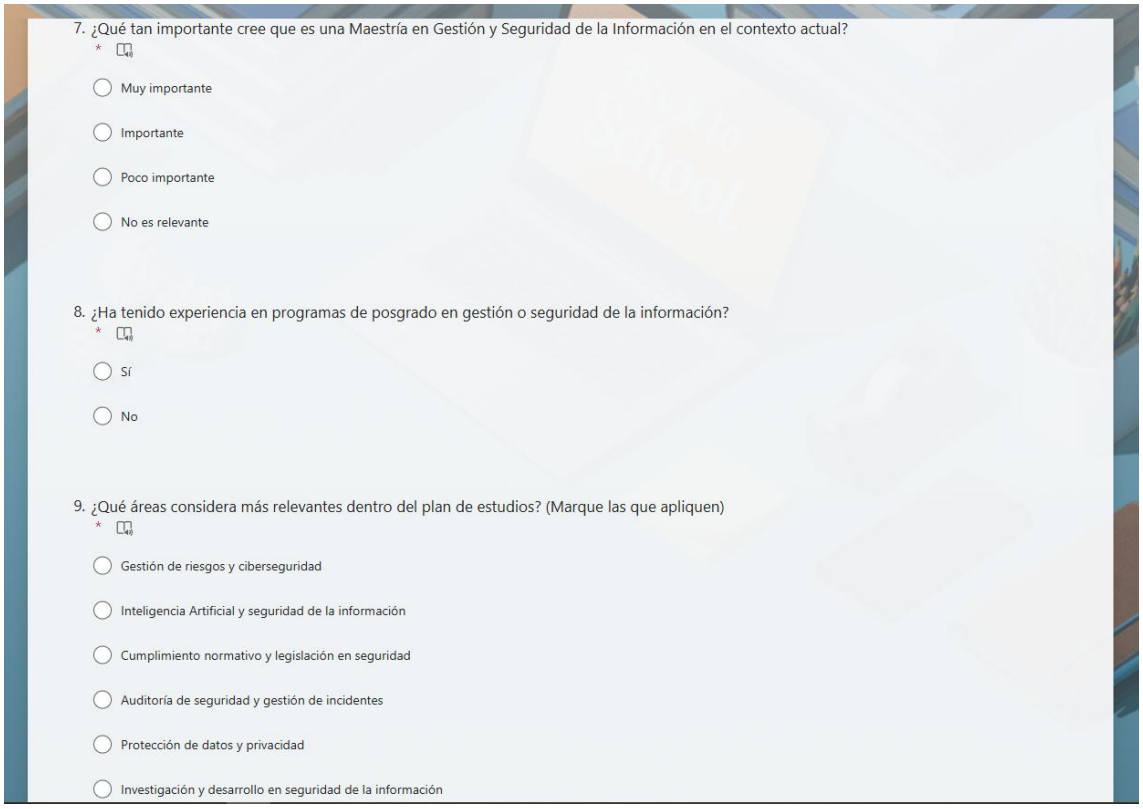
* Obligatorio

Pertinencia del Programa

4. ¿Conoce la Maestría en Gestión y Seguridad de la Información ofrecida por la Universidad Distrital? *
   - Si
   - No

5. ¿A través de qué medios ha tenido conocimiento del programa? *
   - Redes sociales
   - Internet
   - Amigos
   - Otras

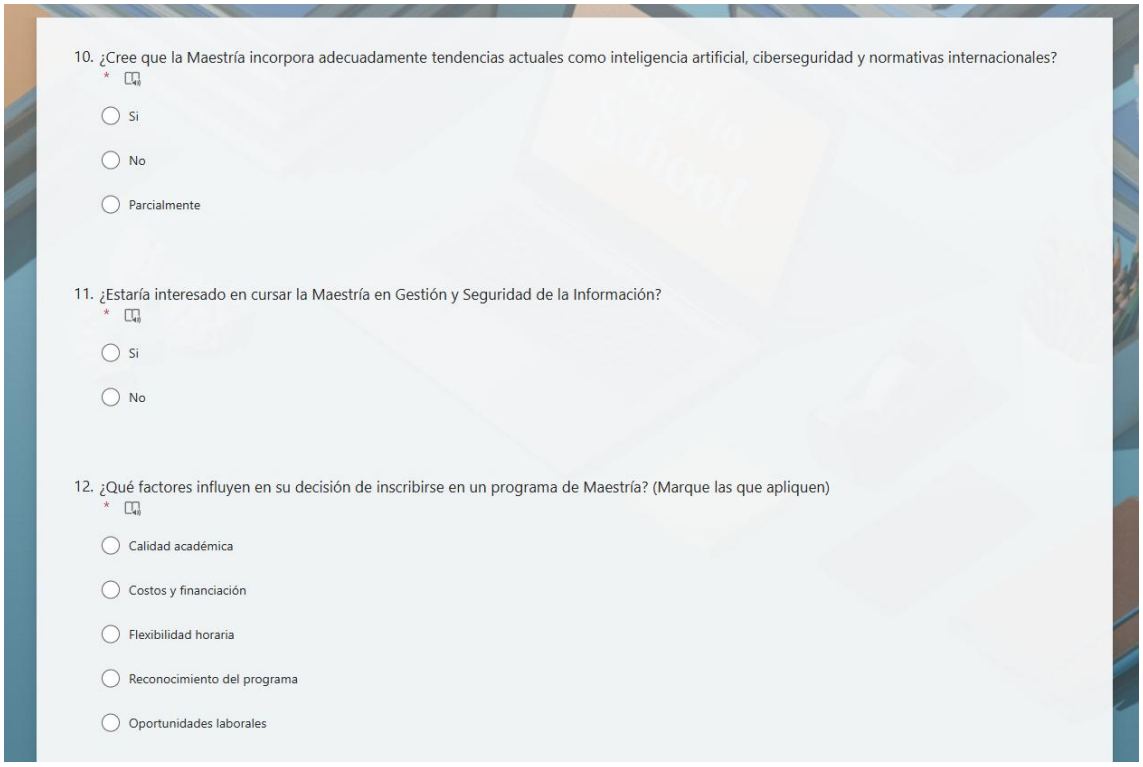
6. ¿Considera que el contenido del programa responde a las necesidades del sector académico y profesional? *
   - Si
   - No

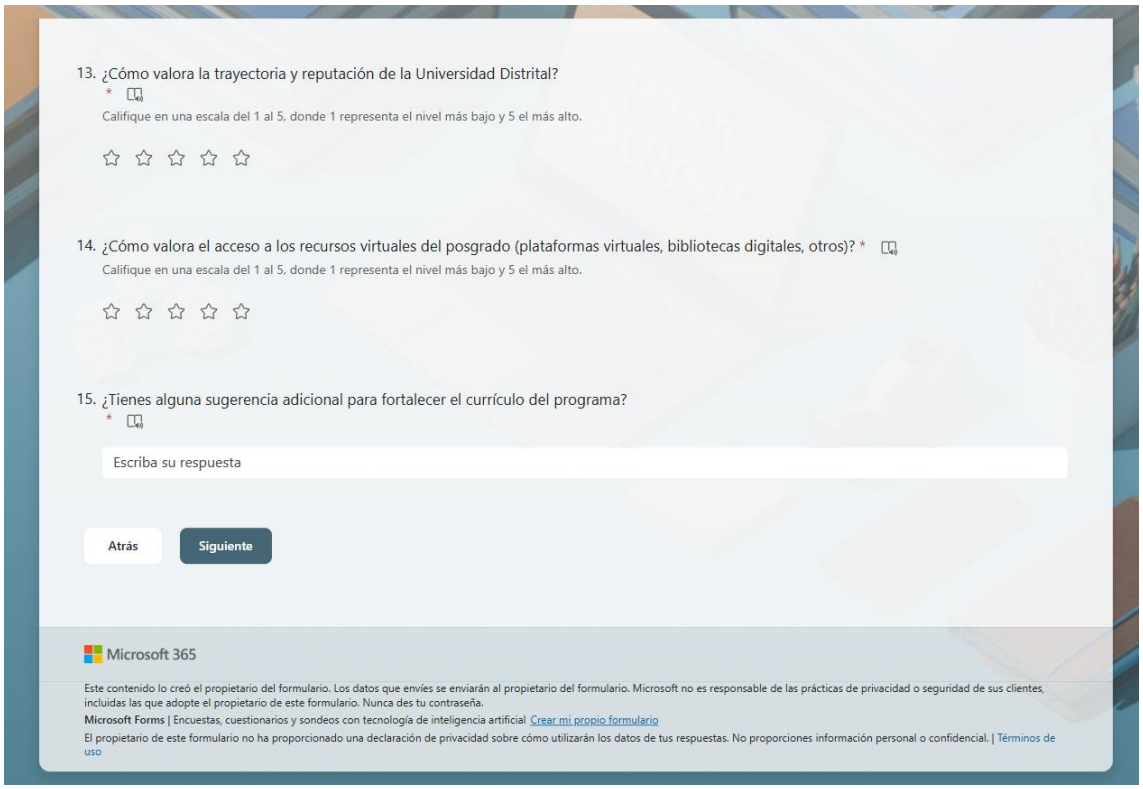


7. ¿Qué tan importante cree que es una Maestría en Gestión y Seguridad de la Información en el contexto actual? *
   - Muy importante
   - Importante
   - Poco importante
   - No es relevante

8. ¿Ha tenido experiencia en programas de posgrado en gestión o seguridad de la información? *
   - Sí
   - No

9. ¿Qué áreas considera más relevantes dentro del plan de estudios? (Marque las que apliquen) *
   - Gestión de riesgos y ciberseguridad
   - Inteligencia Artificial y seguridad de la información
   - Cumplimiento normativo y legislación en seguridad
   - Auditoría de seguridad y gestión de incidentes
   - Protección de datos y privacidad
   - Investigación y desarrollo en seguridad de la información


10. ¿Cree que la Maestría incorpora adecuadamente tendencias actuales como inteligencia artificial, ciberseguridad y normativas internacionales? *
Si
No
Parcialmente
11. ¿Estaría interesado en cursar la Maestría en Gestión y Seguridad de la Información? *
Si
No
12. ¿Qué factores influyen en su decisión de inscribirse en un programa de Maestría? (Marque las que apliquen) *
Calidad académica
Costos y financiación
Flexibilidad horaria
Reconocimiento del programa
Oportunidades laborales


13. ¿Cómo valora la trayectoria y reputación de la Universidad Distrital? *
Califique en una escala del 1 al 5, donde 1 representa el nivel más bajo y 5 el más alto.
14. ¿Cómo valora el acceso a los recursos virtuales del posgrado (plataformas virtuales, bibliotecas digitales, otros)? *
Califique en una escala del 1 al 5, donde 1 representa el nivel más bajo y 5 el más alto.
15. ¿Tienes alguna sugerencia adicional para fortalecer el currículo del programa? *
Escriba su respuesta
Atrás
Siguiente
Microsoft 365
Este contenido lo creó el propietario del formulario. Los datos que envíes se enviarán al propietario del formulario. Microsoft no es responsable de las prácticas de privacidad o seguridad de sus clientes, incluidas las que adopte el propietario de este formulario. Nunca des tu contraseña.
Microsoft Forms | Encuestas, cuestionarios y sondeos con tecnología de inteligencia artificial Crear mi propio formulario
El propietario de este formulario no ha proporcionado una declaración de privacidad sobre cómo utilizarán los datos de tus respuestas. No proporciones información personal o confidencial. | Términos de uso