# Estudio de Pertinencia para la Apertura del Programa de Posgrado en Seguridad Informática en el Instituto Tecnológico del Putumayo

Luis Alejandro Mora Jojoa & Diego Fernando Ortega Guevara
Junio 2024.

Instituto Tecnológico del Putumayo.
Facultad de Ingeniería y Ciencias Básicas
Especialización en Seguridad Informativa

**Agradecimientos**

Con mucha satisfacción, llegamos al final de esta etapa significativa de nuestra formación académica en el Instituto Tecnológico de Putumayo (ITP). Este momento representa la culminación de un esfuerzo conjunto y una oportunidad para expresar nuestra profunda gratitud a quienes hicieron posible este logro.

Agradecemos al ITP por brindarnos un entorno académico de excelencia y a nuestros profesores por su dedicación y paciencia. Especialmente, queremos agradecer a nuestro asesor de tesis, Jhon Henry Cuellar, por su guía y apoyo invaluable.

A nuestras familias, gracias por su amor, comprensión y apoyo inquebrantable. Su paciencia y motivación fueron fundamentales para alcanzar esta meta.

A nuestros compañeros y amigos, les agradecemos por su camaradería y apoyo constante.

Finalmente, agradecemos a todos los que contribuyeron a la realización de este logro. Su apoyo fue esencial para lograr este objetivo.

Con gratitud y aprecio,

Luis Alejandro Mora Jojoa
Diego Fernando Ortega Guevara

## Resumen

De acuerdo con MinTIC (2023), a junio de 2023 el país cerró con más de 41 millones de accesos móviles a internet, en donde cerca del 88% se realizaron a través de tecnología 4G. Seguramente, las estadísticas de acceso al uso de tecnologías que intervienen con conectividad, van a seguir creciendo y la atención a estos requerimientos de diseño y administración de infraestructura en conectividad se deberán prever; sin embargo, el uso de las tecnologías ha hecho que una problemática como la de los ataques informáticos y demás, aparezca y ponga en riesgo la privacidad y la protección de datos, donde el acceso de no autorizados, ponen en peligro a las empresas y personas en general, haciendo que cada vez más, sea necesario proteger la integridad y la privacidad de la información almacenada en los sistemas informáticos de cibercriminales. Consientes de este panorama, el Instituto Tecnológico del Putumayo y la Facultad de Ingeniería y Ciencias Básicas, propenden por ofertar programas de pregrado y posgrado pertinentes, programas que las empresas y el mercado laboral en sí requieren ante situaciones como las que se han descrito en esta sección, programas que respondan a las necesidades y problemáticas de todos los sectores de la sociedad, como es el caso de la seguridad informática. El objetivo de este estudio fue determinar la pertinencia del programa de posgrado en Seguridad Informática para su apertura en el Instituto Tecnológico del Putumayo. Para ello, se recurrió al enfoque cuantitativo de investigación, con un tipo investigación descriptiva, correlacional y explicativa, las cuales ayudaron al desarrollo de cada uno de los objetivos específicos, el diseño fue no experimental con un tipo de muestreo no probabilístico y se recurrió a la encuesta. Con el desarrollo de este estudio se obtuvo que el programa de posgrado en Seguridad Informática es pertinente porque se evidenció la necesidad de un programa de posgrado en seguridad informática, alineado con las demandas del mercado y las necesidades específicas de protección de datos y sistemas en un entorno digital en constante evolución. El plan de estudios presentado es el resultado de los análisis realizados y es una guía indispensable para la institución.

**Abstract**

According to MinTIC (2023), by June 2023, Colombia recorded over 41 million mobile internet accesses, with approximately 88% using 4G technology. These figures are expected to continue rising, necessitating special attention to the design and management of connectivity infrastructures. However, technological growth has also heightened cybersecurity risks, threatening data privacy and integrity. In response, the Institute Technologic del Putumayo and the Faculty of Engineering and Basic Sciences aim to provide relevant academic programs, particularly in cybersecurity, to meet the demands of the labor market and businesses. This study focused on determining the relevance of a postgraduate program in Cybersecurity at the Institute Technologic del Putumayo. Using a quantitative approach and a descriptive, correlational, and explanatory methodology, it was concluded that the program is pertinent for the region and the country.

## Tabla de Contenidos

Resumen ..... 3

Abstract ..... 4

Introducción ..... 10

Generalidades del Estudio de Pertinencia ..... 12

Planteamiento del Problema ..... 12

Pregunta de Investigación ..... 16

Justificación ..... 16

Objetivos ..... 19

Objetivo General. ..... 19

Objetivos General. ..... 19

Marco de Referencia ..... 20

Marco Teórico ..... 20

Pertinencia de la Educación Superior ..... 20

Seguridad Informática ..... 25

Ciberseguridad ..... 29

Políticas de Seguridad ..... 30

Marco Conceptual ..... 32

Marco Contextual ..... 34

Departamento del Putumayo ..... 34

Municipio de Mocoa ..... 35

Instituto Tecnológico del Putumayo ..... 36

Programa de Ingeniería de Sistemas ..... 36

Marco Legal ..... 37

Metodología ..... 40

Enfoque de Investigación ..... 40

Fase de Planificación del Trabajo ..... 41

Fase de Recolección y Análisis de Documentos ..... 42

Fase de Elaboración del Documento Final ..... 43

Tipo de Investigación ..... 44

Diseño de Investigación ..... 46

Población y Muestra ..... 47

Técnica e Instrumento ..... 48

Resultados ..... 49

Estado de la Oferta de Educación del Programa en los Ámbitos Nacional e Internacional ..... 49

Análisis Comparativo de Mallas Curriculares en el Contexto Internacional, Nacional, Regional ..... 49

Análisis de los Perfiles profesionales, Ocupacionales y Modalidades en el Contexto Internacional y Nacional ..... 62

Necesidades del país y la Región ..... 73

Análisis en el Contexto Internacional de Planes y Programas de Organizaciones Internacionales ..... 73

Análisis en el Contexto Nacional de Planes y Políticas Nacionales ..... 78

Análisis en el Contexto Regional de Planes de Desarrollo ..... 82

Oferta Laboral a Nivel Regional: ..... 85

Análisis de los Planes Regionales y Locales Respecto a las Necesidades Laborales 85

Diseño, Aplicación y Análisis Encuesta Sector Productivo ..... 86

Análisis Nivel de Empleabilidad de los Egresados ..... 95

Diseño, Aplicación y Análisis Encuesta Egresados ..... 99

Conclusiones ..... 109

Recomendaciones ..... 111

Limitaciones ..... 112

Referencias ..... 113

Anexos ..... 120

## Lista de Tablas

Tabla 1. Lista de IES a Nivel Nacional e Internacional..... 50

Tabla 2. Créditos Académicos por Semestre. ..... 51

Tabla 3. Unidades de Formación por Institución..... 54

Tabla 4. Análisis de Perfiles. ..... 63

Tabla 5. Rasgos Representativos del Análisis de Perfiles. ..... 69

Tabla 6. Matriz de Retos, Oportunidades y Necesidades del Programa a Nivel Internacional. ..... 73

Tabla 7. Matriz de Retos, Oportunidades y Necesidades del Programa a Nivel Nacional. ..... 78

Tabla 8. Matriz de Retos, Oportunidades y Necesidades del Programa a Nivel Regional. ..... 83

Tabla 9. ¿Cuáles de las siguientes competencias o habilidades considera importantes en la formación a nivel posgrado del profesional en seguridad informática? ..... 90

Tabla 10. Tasa de Cotizantes. ..... 96

Tabla 11. ¿Cuáles de las siguientes competencias o habilidades considera importantes en la formación a nivel posgrado del profesional en seguridad informática? ..... 101

Tabla 12. Propuesta de unidades de formación y su descripción para el programa especialización profesional en seguridad informática. ..... 107

## Lista de Figuras

Figura 1. Proceso Cuantitativo..... 40

Figura 2. Alineación Fases Metodológicas..... 41

Figura 3. ¿Qué tan importante considera que el ITP forme (capacite) personal a nivel de posgrado en seguridad informática para el Putumayo? ..... 89

Figura 4. Ingreso base años 2019-2021. ..... 97

Figura 5. Graduados Según Tipo de Cotizante y Nivel de Formación. ..... 98

Figura 6. ¿Cómo Ingeniero de Sistemas graduado del Instituto Tecnológico del Putumayo ¿en qué nivel considera importante estudiar el posgrado en seguridad informática? ..... 100

## Introducción

La seguridad informática se ha convertido en un aspecto crucial para la protección de información sensible y la continuidad operativa de organizaciones tanto públicas como privadas. Según el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, 2023), Colombia cerró el año 2023 con más de 41 millones de accesos móviles a internet, destacando que el 88% de estos accesos se realizaron mediante tecnología 4G. Este crecimiento exponencial en la conectividad también ha intensificado los desafíos en ciberseguridad, con un aumento significativo en los ciberataques dirigidos a infraestructuras críticas y datos sensibles en todo el mundo.

El panorama global refleja una preocupante escalada en los incidentes cibernéticos, como lo reporta Microsoft (2022), donde los ataques a infraestructuras críticas han aumentado drásticamente. Además, el Banco Mundial (2023) subraya la importancia de fortalecer la ciberseguridad y la protección de datos personales para participar plenamente en la economía digital global. En el contexto colombiano, la Cámara Colombiana de Informática y Telecomunicaciones (2022) reporta un incremento considerable en los intentos de ataques cibernéticos, evidenciando la vulnerabilidad creciente de empresas y entidades gubernamentales frente a amenazas digitales.

Conscientes de estos desafíos y del impacto crítico que tienen en la seguridad y la privacidad de la información, el Instituto Tecnológico del Putumayo y la Facultad de Ingeniería y Ciencias Básicas se proponen ofrecer programas académicos pertinentes que aborden estas problemáticas emergentes. En este contexto, surge la necesidad de evaluar la pertinencia del programa de posgrado en Seguridad Informática para su potencial

apertura como una alternativa académica para los egresados del programa ingeniería de sistemas y todas las personas interesadas.

El presente estudio se enfoca en determinar la viabilidad y relevancia del programa de posgrado en Seguridad Informática en el Instituto Tecnológico del Putumayo. A través de un enfoque cuantitativo de investigación, utilizando métodos descriptivos, correlacionales y explicativos, se explorará el estado actual de la oferta educativa a nivel nacional e internacional, se identificarán las necesidades específicas del país y la región en términos de ciberseguridad, y se analizará la demanda laboral para profesionales especializados en este campo.

Además, se propondrá un plan de estudios detallado que responda a los desafíos y requerimientos actuales en ciberseguridad, asegurando que los graduados del programa estén debidamente preparados para enfrentar las amenazas digitales emergentes y contribuir de manera efectiva al desarrollo tecnológico y económico de la región.

## Generalidades del Estudio de Pertinencia

### Planteamiento del Problema

Según el informe anual de Defensa Digital (Microsoft, 2022) que proporciona nueva información sobre ciberataques y la creciente agresión cibernética originada por los lideres autoritarios en todas partes del mundo, durante el 2021, los ciberataques dirigidos a infraestructuras críticas aumentaron del 20% de todos los ataques de Estado nación detectados por Microsoft. a un impresionante 40%. Esta alza se debió en gran parte al objetivo de Rusia de dañar la infraestructura ucraniana y al espionaje agresivo dirigido a los aliados de este país, incluyendo los Estados Unidos. Rusia también aceleró sus intentos de comprometer a las compañías de TI para interrumpir u obtener inteligencia de los clientes gubernamentales de esas compañías en los países miembros de la OTAN. El 90% de los ataques rusos detectados por Microsoft el año pasado se dirigieron a los estados miembros de la OTAN, y el 48% se dirigieron a compañías de TI establecidas en los países miembros de la misma.

El mismo informe determina que, los ciberdelincuentes iraníes escalaron sus ataques después de la transición del poder presidencial. Mientras tanto, Corea del Norte lanzó una serie de ataques para robar tecnología a investigadores y compañías aeroespaciales del mundo. China por su lado, incrementó sus ciberataques de espionaje y robo de información en un intento por ejercer más influencia regional en el Sudeste Asiático y contrarrestar el creciente interés de los Estados Unidos. En cifras estadísticas, tan solo en el último año, el número estimado de ataques de contraseña por segundo aumentó en un 74%. Muchos de estos ataques fueron de ransomware (secuestro de

datos), lo que duplicó las demandas de rescate. Sin embargo, estos ataques no se propagaron de manera uniforme por todas las regiones. (Microsoft, 2022)

Actualmente, la Práctica Global de Desarrollo Digital trabaja con los Gobiernos de los países en desarrollo para sentar las bases de la transformación digital, que incluye su transición hacia economías, Gobiernos y sociedades digitales. Su labor se centra en pilares clave, como el acceso inclusivo a servicios de internet rápidos, confiables, seguros y asequibles. En todo el Banco Mundial, se procura estimular la demanda de aplicaciones, habilidades y plataformas digitales para ayudar a los Gobiernos, las empresas y las personas a participar más plenamente en la economía digital. Pero, ¿qué se necesitará para que los países cosechen los beneficios de la digitalización y participen de lleno en la economía digital mundial?, entre otros aspectos, crear sistemas digitales seguros y fiables, en un mundo que se está digitalizando, el fortalecimiento de la capacidad en áreas como la ciberseguridad y la protección de datos personales ha pasado a ser más importante que nunca. (Banco Mundial, 2023)

Según la BBC (2023), una prolífica banda de delincuentes cibernéticos, probablemente con sede en Rusia, ha dado un ultimátum a las víctimas de un ciberataque que ha afectado a organizaciones de todo el mundo. El grupo de piratas informáticos Clop advirtió en la dark web (web oscura) a las empresas afectadas por el ataque al software comercial MOVEit que, si no les envían un correo electrónico antes del 14 de junio para empezar negociaciones, se publicarán los datos robados. Más de 100.000 empleados de la BBC, British Airways y Boots han sido informados de que es posible que se hayan filtrado datos de sus nóminas. En el 2017, según este medio, un ciberataque

"de dimensión nunca antes vista" logró bloquear el acceso a los sistemas informáticos de instituciones estatales y empresas de varios países. La policía europea, Europol, indicó que el ciberataque era de una escala "sin precedentes" y advirtió que una "compleja investigación internacional" era necesaria para "identificar a los culpables". El ataque afectó a unas 200.000 víctimas en 150 países.

En Colombia, de acuerdo a la Cámara Colombiana de Informática y Telecomunicaciones (2022), en el año 2021 se presentaron 41 billones de intentos de ataques cibernéticos en el mundo y siete billones en Colombia. Los cibercrímenes generan cada vez más rentabilidad para los atacantes y en este sentido, sino existen herramientas para contrarrestarlos y estar protegidos, seguirá creciendo la curva de ciberataques para empresas y entidades de gobierno. De acuerdo con el último informe presentado por la Fiscalía General de la Nación, en Colombia en el año 2021 el número de ataques cibernéticos aumentó en un 30%, comparado con el año anterior. Si bien, las compañías y entidades oficiales han venido trabajando fuertemente en estrategias tendientes a robustecer las medidas de ciberseguridad, estas no han sido suficientes, ya que casos como el secuestro de información o la afectación de datos a entidades mediante Ransomware o ataques de día cero sin filtración de datos, aún continúan presentándose y han ocasionado grandes pérdidas económicas para las organizaciones ya que éstas han tenido que efectuar cuantiosos pagos frente a este tipo extorsiones a los cibercriminales.

El Presidente de la República, Gustavo Petro, en declaraciones a la prensa desde Nueva York, afirma que Colombia es víctima de ataque cibernético por guerras entre empresas privadas a escala mundial, añadió que este ataque afecta a más de 50 entidades

del Estado y empresas privadas y que la ciudadanía debe tener seguridad alrededor del uso cada vez más extendido de este tipo de aparatos que usan algoritmos y plataformas de software.

Aunado a este panorama crítico respecto a la vulnerabilidad de la información, la Pontificia Universidad Católica de Chile (2023), en el marco del mes internacional de la ciberseguridad, el reporte de Cybersecuriry Workforce Study, elaborado por ISC², menciona que existe un déficit aproximado de 3,4 millones de profesionales expertos en ciberseguridad a nivel mundial y sobre 500 mil en América Latina. De acuerdo a la Revista Semana (2021), en los últimos años, se ha experimentado un continuo crecimiento del interés por la ciberseguridad por estudiantes y profesionales y el número de expertos en esta área de la informática ha aumentado. Sin embargo, un reciente estudio publicado por la Agencia de Ciberseguridad de la Unión Europea (ENISA) advierte que persiste la brecha de habilidades en el sector. Esa es la conclusión del informe, que indica que a pesar de que cada vez son más los especialistas en seguridad, ni el número de expertos ni su cualificación profesional puede abarcar la demanda que existe. "En el mercado laboral falta personal capacitado y cualificado para trabajar en funciones de ciberseguridad y que pueda enfrentarse de forma eficiente a la gama de ciberamenazas que se plantean".

Como es evidente, las cifras hablan por sí solas; actualmente, de acuerdo con MinTIC (2023), a junio de 2023 el país cerró con más de 41 millones de accesos móviles a internet, en donde cerca del 88% se realizaron a través de tecnología 4G. Seguramente, las estadísticas de acceso al uso de tecnologías que intervienen con conectividad, van a

seguir creciendo y la atención a estos requerimientos de diseño y administración de infraestructura en conectividad se deberán prever; sin embargo, el uso de las tecnologías ha hecho que una problemática, como la mencionada hasta el momento, aparezca y ponga en riesgo la privacidad y la protección de datos, donde el acceso de no autorizados, ponen en peligro a las empresas y personas en general, haciendo que cada vez más, sea necesario proteger la integridad y la privacidad de la información almacenada en los sistemas informáticos de cibercriminales.

Dada la situación, el Instituto Tecnológico del Putumayo y la Facultad de Ingeniería y Ciencias Básicas, son conscientes de la importancia de ofertar programas de pregrado y posgrado pertinentes, programas que las empresas y el mercado laboral en sí requieren ante situaciones como las que se han descrito en esta sección, programas que respondan a las necesidades y problemáticas de todos los sectores de la sociedad. Por ello, es importante este estudio de pertinencia para la posible y necesaria oferta del programa de posgrado en seguridad informática en el Instituto Tecnológico del Putumayo.

**Pregunta de Investigación**

¿Cuál es la pertinencia del programa de posgrado en Seguridad Informática como propuesta de oferta académica en nivel posgrado en el Instituto Tecnológico del Putumayo?

**Justificación**

En una era digital como lo actual, en la que empresas, personas e incluso gobiernos poseen información importante y/o clasificada en dispositivos digitales (fijos o

móviles), se hace de vital importancia conocer los riesgos existentes ya sea de ataques, espionajes o actos delictivos de los cuales se puede ser víctima, así como de las herramientas existentes para detectarlos, prevenirlos y contrarrestarlos. Si bien es cierto que con el paso del tiempo los ciberataques y delincuencia cibernética han evolucionado, no en menor medida los programas y herramientas para evitar ser víctima de dichos ataques también han evolucionado. (Gamboa, s.f.)

Para Gamboa (s.f.), la seguridad informática se trata sobre la protección de información de índole personal, empresarial o gubernamental contenida no solo en la red, sino también en los dispositivos de uso diario como teléfonos celulares, tabletas, computadoras de escritorio, laptop o cualquier dispositivo digital, de amenazas que puedan poner en riesgo la información almacenada o transportada en alguno de los dispositivos antes mencionados.

Como se ha venido mencionando, en la era digital en la que se está inmerso, la interconexión y el contacto con la tecnología se han convertido en dos factores omnipresentes…nadie puede negar que el vertiginoso avance tecnológico ha traído consigo innumerables beneficios, pero también ha dado lugar a un aumento exponencial de las amenazas cibernéticas. La conectividad global, el almacenamiento masivo de datos y la proliferación de dispositivos conectados han creado un terreno propicio para los ciberdelincuentes, quienes, con ingenio y sofisticación, han encontrado nuevas formas de comprometer la seguridad de la información. En este contexto, la protección de datos personales y la implementación efectiva de medidas de ciberseguridad no solo se han

vuelto imperativas, sino que son esenciales para salvaguardar la integridad de los usuarios y garantizar la confianza en el espacio digital. (Gonzales, 2024)

El conocimiento respecto a la seguridad informática es cada vez más importante para el mundo, el país y la región; es necesario contar con profesionales expertos en el tema debido a que cada vez más esta problemática se expande más y más; por ello, es necesario que desde la academia se fortalezcan estos conocimientos a través de la oferta de programas pertinentes; es así que, se hace imperioso la realización de un estudio de pertinencia para determinar qué tan necesario es aperturar un programa de posgrado en seguridad informática en el ITP; aunque, las cifras, datos, estadísticas y estudios, con antelación dan una respuesta positiva a este planteamiento, la posible apertura de este programa debe estar respaldado por un estudio de pertinencia.

Los resultados de este estudio de pertinencia, son un insumo necesario y requisitorio para iniciar el proceso de solicitud de registro calificado del programa de posgrado ante el Ministerio de Educación Nacional. La Institución necesita soportar en este estudio, la pertinencia del programa de posgrado en seguridad informática, donde se pueda evidenciar que la nueva propuesta académica no solo formará especialistas en determinada área del conocimiento, sino que también va a aportar al desarrollo del país y la región, como evidentemente ocurrirá por la necesidad de estos profesionales ante la problemática y déficit dado.

## Objetivos

### *Objetivo General.*

Determinar la pertinencia del programa de posgrado en Seguridad Informática para su apertura en el Instituto Tecnológico del Putumayo.

### *Objetivos General.*

- Determinar el estado de la oferta de educación del programa en los ámbitos nacional e internacional.
- Identificar las necesidades del país y la región.
- Establecer la oferta laboral a nivel regional.
- Proponer un plan de estudios del programa de posgrado.

## Marco de Referencia

Con el fin de determinar la pertinencia para la apertura del programa de posgrado en Seguridad Informática en el Instituto Tecnológico del Putumayo, se menciona a continuación algunas referencias teóricas que dan soporte al objeto de estudio.

### Marco Teórico

#### *Pertinencia de la Educación Superior*

El Documento de Política para el Cambio y el Desarrollo en la Educación Superior de la UNESCO (1995), constituye la carta de navegación sobre educación superior para el próximo milenio. En él se plasma con claridad que al hablar de pertinencia se debe hacer desde el punto de vista del papel desempeñado por la enseñanza superior como sistema y por cada una de sus instituciones con respecto a la sociedad, y también desde el punto de vista de lo que la sociedad espera de la educación superior. La pertinencia debe pues abarcar cuestiones como la democratización del acceso y mayores oportunidades de participación en la educación superior durante las distintas fases de la vida, los vínculos con el mundo del trabajo y las responsabilidades de la educación superior con respecto al sistema educativo en su conjunto. No menos importante es la participación de la comunidad de la educación superior en la búsqueda de soluciones a problemas humanos apremiantes como la demografía, el medio ambiente, la paz y el entendimiento internacional, la democracia y los derechos humanos. La mejor manifestación de la pertinencia de la educación superior tal vez sea la variedad de "servicios docentes" que presta a la sociedad. En los años venideros será menester volver a definir y debatir los tipos y modalidades de prestación de dichos servicios.

De la misma manera, la UNESCO (s.f.), coincide en que la pertinencia debe ser la cualidad principal de la relación o vínculo Universidad-Sociedad, vista como el papel que desempeña y el puesto que ocupa la educación superior en el seno de la sociedad, pero también considera su misión y funciones, los programas, los modos de impartir la enseñanza y su contenido, como los temas de equidad, responsabilidad y financiamiento, al tiempo que destaca la libertad de cátedra y la autonomía institucional como principios sobre los que deben basarse todos los esfuerzos por garantizar y elevar la pertinencia.

La pertinencia involucra la educación para el desarrollo sostenible, cuyo objetivo es hacer posible que la comunidad educativa adquiera los valores, capacidades, habilidades y los conocimientos necesarios para contribuir a la construcción de una sociedad más sostenible. Este objetivo para la UNESCO implica la revisión del contenido de los programas educativos respondiendo a retos locales y globales, invita a promover modelos de enseñanza que permitan a los estudiantes adquirir capacidades, tales como el pensamiento interdisciplinario, la planificación integrada, la comprensión de la complejidad, la cooperación para la toma de decisiones y la participación en procesos locales, nacionales y globales para el desarrollo sostenible. (UNESCO, s.f.)

La Conferencia Mundial sobre la Educación Superior (CMES), definió la pertinencia en la educación superior como "la adecuación entre lo que la sociedad espera de las instituciones y lo que estas hacen". Este concepto, así formulado, vincula estrechamente a las universidades con las demandas de las sociedades en las que están insertas. Ello rige para el corto plazo, pero, por la naturaleza de los procesos de

enseñanza y de creación del conocimiento, debe proyectarse necesariamente al largo plazo. (Guarga, 2007)

El Ministerio de Educación Nacional (MEN, 2016), hace referencia a que la educación requiere ser pertinente, también, a los entornos inmediatos en donde las personas viven su cotidianidad. Esta pertinencia se refiere a la adecuación de los procesos, contenidos y fines educativos a las condiciones concretas de las comunidades que son sujeto de las acciones educativas, de modo que no se les apliquen raseros universales con pretensiones de homogeneizar, sino que los proyectos formativos sean correspondientes a las características culturales, sociales y geográficas propias de su contexto. Se habla aquí de la necesidad de que los agentes educativos reconozcan, valoren y sean respetuosos de los intereses, tradiciones y cosmovisiones de las comunidades que posean especificidades de orden social, cultural y/o étnico, formas propias de organización social, métodos ancestrales de producción, lenguajes, maneras particulares de relacionarse con los ecosistemas, etc., de modo que los proyectos educativos que construyan y ejecuten contemplen siempre una metodología participativa y sean congruentes y apropiados a estas comunidades.

Las estructuras que se dedican a impartir enseñanza superior se están diversificando con rapidez para adaptarse al mercado mundial que se está formando para este tipo de educación, fomentado por el adelanto de las telecomunicaciones, la mayor movilidad de los estudiantes y las culturas de gestión institucional que insisten en la recuperación de los costos y la generación de ingresos (Gibbons, 1998). Las necesidades y demandas de la sociedad actual exigen a las universidades asumir un rol protagónico en

las transformaciones económicas, políticas y sociales para el logro de un futuro sustentable (Álvarez et al., 2018). Por ello, la oferta educativa en las Instituciones de Educación Superior, debe estar definida por su pertinencia social que es el "grado de correspondencia que debe existir entre necesidades sociales e individuales a satisfacer con la educación universitaria y lo que realmente se llega a alcanzar; igual que otros aspectos como la socialización, legitimación, de formación cultural, de extensión y servicios" (ANUIES, s.f.)

El Consejo Nacional de Acreditación (CESU, 2020), define la pertinencia como la actuación congruente, conveniente, coherente y adecuada a las condiciones y demandas sociales, culturales y ambientales del contexto en el que las instituciones y los programas académicos desarrollan sus labores formativas, académicas, docentes, científicas, culturales y de extensión.

Para Ramírez (s.f.), el concepto de pertinencia social de la educación cobra importancia como parte de la nueva sociedad basada en el conocimiento y en la redistribución de la riqueza, debido a que la propia redistribución del conocimiento significa un acto de equidad social que posibilita nuevas oportunidades y desarrollo. Él define la pertinencia social como la relación de la educación superior con la sociedad y obliga a las universidades a responder sobre lo que estas generen como "productos" y servicios en relación a las expectativas sociales. Permite la interlocución efectiva de las instituciones educativas con los actores de su medio, ofreciendo respuestas concretas, apropiadas y oportunas a sus necesidades. La pertinencia social significa la capacidad

creativa que tiene la educación para responder en forma proactiva a las necesidades de su entorno.

De manera análoga con la pertinencia de las IES, la de los programas se encuentra definida por su capacidad de dar soluciones a los problemas de la sociedad; a diferencia de la pertinencia institucional, el ámbito para definir la de un programa es más específico, pues se encuentra circunscrito, en gran medida, a su área disciplinar o profesional y al desarrollo del conocimiento logrado por la misma. Esta delimitación indica que la pertinencia de un programa comienza en su estructura y contenidos curriculares; es decir, en las características del currículo se encuentran, en primera instancia, los fundamentos de su pertinencia. En un segundo momento, al recibir a los titulados, la sociedad confrontará esa pertinencia y, por tanto, la reconocerá o negará. Uno de los elementos determinantes de la calidad de un programa de educación superior es el reconocimiento social a los graduados: los egresados del programa son reconocidos por la calidad de la formación que reciben y se destacan por su desempeño en la disciplina, profesión, ocupación u oficio correspondiente. También se incluye la capacidad del programa de influir en el medio, según las actividades que desarrollan sus docentes y estudiantes. (Jaramillo et al., 2009)

Los autores mencionados coinciden que la pertinencia de un programa académico se enfoca en factores académicos y sociales. Académico porque su estructura y contenido curricular debe estar diseñado de tal manera que el estudiante pueda adquirir los conocimientos y habilidades suficientes que le sirvan de base para desempeñarse en el mundo laboral que está cambiando desmesuradamente, para dar soluciones a

problemáticas cotidianas, que sepan ser proactivos y creativos en la búsqueda a la hora de intervenir en situaciones importantes. En lo social, debe ser pertinente porque debe hacerse un acercamiento con las necesidades del sector productivo y las empresas en general, y los gustos y preferencias de los estudiantes de los colegios y juventud en general, esto, aunado a un análisis reflexivo de la actualidad que enfrenta ese programa a nivel internacional, nacional y local; solo así, se sabrá con exactitud si el programa es pertinente o no.

***Seguridad Informática***

Para Gamboa (s.f.), la seguridad informática se trata sobre la protección de información de índole personal, empresarial o gubernamental contenida no solo en la red, sino también en los dispositivos de uso diario como teléfonos celulares, tabletas, computadoras de escritorio, laptop o cualquier dispositivo digital, de amenazas que puedan poner en riesgo la información almacenada o transportada en alguno de los dispositivos antes mencionados. Una buena Ciberseguridad no solo se debe basar en la prevención de ataques, sino también detección y corrección de los mismos, reduciendo los riesgos de exposición de la información, brindando confianza a los usuarios. Las categorías de seguridad informática son seguridad de red, seguridad de las aplicaciones, seguridad de la información, seguridad operativa, recuperación ante desastres y la continuidad del negocio, capacidad de usuario final.

Por otro lado, Arango (s.f.), define la seguridad informática como el conjunto de prácticas, herramientas y técnicas diseñadas para proteger la confidencialidad, integridad y disponibilidad de los datos e información almacenados y procesados por los sistemas

informáticos. Los ataques cibernéticos y las amenazas informáticas, como los virus, el malware y los hackers, pueden comprometer la seguridad de los sistemas informáticos y causar pérdidas financieras, daños a la reputación y riesgos para la privacidad de los usuarios. Para él, existen muchas amenazas y vulnerabilidades a los sistemas informáticos que incluye virus informáticos, troyanos, gusanos, phishing, hacking, spyware, denegación de servicio. El autor concluye con que es importante entender los conceptos básicos de la seguridad informática y las amenazas y vulnerabilidades a los sistemas informáticos para poder proteger adecuadamente la información confidencial y los sistemas informáticos. La implementación de prácticas de seguridad informática y la utilización de herramientas y técnicas de protección adecuadas pueden ayudar a mitigar el riesgo de pérdida de datos y daños a los sistemas informáticos.

Otra definición, la da López (s.f.) en su libro "fundamentos de seguridad informática" de la Fundación Universitaria del Área Andina miembro de la Red Ilumno. (López, s.f.), define la seguridad informática como la disciplina que se encarga de proteger la integridad, disponibilidad y confidencialidad de la información y los sistemas informáticos que la contienen, expresa la condición de aplicar la protección hacia la rama computacional y la teleinformática, la cual busca, ante todo, prevalecer el cuidado y la prevención de la información que se maneja y circula en estos medios informáticos. De igual forma emplea diferentes procesos (métodos o técnicas), políticas, normas, procedimientos y estrategias para salvaguardar, mitigar y minimizar potenciales riesgos, amenazas o vulnerabilidades en que la información está expuesta (físico y lógico) y pueda así asegurar sus principios básicos asociados como confidencialidad, integridad y

disponibilidad, lo que contribuye a mantener un sistema de información (SI) de forma segura y confiable.

Por su parte, Baca (2016), determina que la seguridad informática es la disciplina que, con base a políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta…el autor hace mención que según marco de gestión y de negocio global para el gobierno y la gestión de las TI de la empresa, las características que debe poseer la información son: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, apego a los estándares y confidencialidad.

Adicionalmente, Romero et al., (s.f.), resaltan que seguridad informática y seguridad de la información, aunque suenen parecidos, tienen un punto clave que hace la diferencia. La seguridad informática se encarga de la seguridad del medio informático…la informática en la ciencia encargada de los procesos, técnicas y métodos que buscan procesar, almacenar y transmitir la información, mientras tanto la seguridad de la información no se preocupa solo por el medio informático, se preocupa por todo aquello que pueda contener información, en resumen, esto quiere decir que se preocupa por casi todo, lo que conlleva a afirmar que existen varias diferencias, pero lo más relevante es el universo que manejan cada uno de los conceptos en el medio informático.

Asimismo, Gómez (2014), determina que la seguridad informática es cualquier medida que impide la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su

confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

Así también, García et al., (2011), establece que preservar la información y la integridad de un sistema informático es algo importante para una empresa u organización, por lo que en pérdidas económicas y de tiempo podría suponer, sin olvidar del peligro que podría acarrear el acceso al sistema de un usuario no autorizado…así, el autor define la seguridad informática como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo.

Finalmente, la Norma ISO 27000 da un concepto de seguridad informática donde determina que esta se basa en la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas aplicados para su tratamiento. Define confidencialidad donde la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados; la integridad como el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso; y la disponibilidad como el acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos o procesos autorizados cuando lo requieran.

Haciendo referencia a todos los autores citados, es pertinente decir que cada uno tiene un concepto válido de lo que es y el objetivo de la seguridad informática; sin embargo, Gamboa (s.f.), menciona algo muy importante dentro de esta tema y es que la seguridad informática se trata sobre la protección de información de índole personal,

empresarial o gubernamental contenida no solo en la red, sino también en los dispositivos de uso diario como teléfonos celulares, tabletas, computadoras de escritorio, laptop o cualquier dispositivo digital, de amenazas que puedan poner en riesgo la información almacenada o transportada en alguno de los dispositivos antes mencionados; si bien, todos coinciden en que seguridad informática es la protección de la información, este autor hace énfasis además de la información personal que es un tema complicado que afecta a muchos.

***Ciberseguridad***

Ortega (2021), en su libro de ciberseguridad dispone que la protección de la información es una función crítica para todas las empresas, industrias y sociedades modernas. Salvaguardar la información ha sido una prioridad desde que las personas han necesitado mantener la información de una forma segura y privada. La ciberseguridad es un campo cada vez más amplio y cambiante…la ciberseguridad se ocupa de la protección de los activos digitales, incluyendo redes, hardware y software, así como la información que es procesada, almacenada en sistemas o transportada a través de entornos de información interconectados. Es el conjunto de técnicas, sistemas de gestión y otras medidas que pretenden proteger la información digital y los medios que la tratan de incidentes deliberados o accidentales.

Los autores Martin de Diego et al., (2020), definen la ciberseguridad en la actualidad, como la práctica de defender los ordenadores personales, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques malintencionados. Los autores añaden además que el término es aplicable en diversos

contextos, desde los negocios hasta la informática móvil y puede dividirse en unas categorías comunes: la seguridad de la red, la seguridad de las aplicaciones, la seguridad de la información, la seguridad operacional, la recuperación de los datos, y la educación de los usuarios finales. Adicionalmente, establecen que el panorama actual de la ciberseguridad es muy diverso, siendo complejo encontrar una clasificación única y generalmente aceptada de sus amenazas. Se pude pensar en una organización a muy alto nivel dividiendo las amenazas contra la ciberseguridad en tres grandes grupos: delito cibernético, ciberataque, ciberterrorismo. Las amenazas suelen materializarse a través de uno o más de los siguientes tipos de ataques: malware, inyecciones SQL, phishing, hombre en el medio (man in the middle), y ataques de denegación de servicio.

Es importante para el estudio, concluir diferenciando los dos términos de ciberseguridad y seguridad informática; en este sentido, la ciberseguridad en sí es la práctica de defender con tecnologías o prácticas ofensivas, los computadores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. Mientras tanto, la seguridad informática es la disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en el sistema informático de cibercriminales. En otras palabras, la seguridad informática abarca un concepto más amplio donde la ciberseguridad entra como apoyo para complementarla.

***Políticas de Seguridad***

Las políticas de seguridad informática son un conjunto de reglas, directrices y procedimientos establecidos por una organización para proteger la información y los sistemas de tecnología de la información, contra amenazas y riesgos de seguridad. Estas

políticas definen las medidas de seguridad digital que se deben implementar, los roles y responsabilidades de los usuarios, los procedimientos para la gestión de incidentes y la respuesta a eventos de amenaza contra la seguridad. Son esenciales para promover una cultura de seguridad organizacional y establecer un marco de trabajo que garantice la confiabilidad, integridad y disponibilidad de la información. Además, ayudan a cumplir con los requisitos legales y normativas relacionadas con la seguridad de la información. (DocuSign, 2023)

Para la empresa estadounidense DocuSign (2023), existen dos tipos de políticas de seguridad informática: políticas de buenas prácticas informáticas que son el conjuntos de directrices y reglas establecidas para promover el uso seguro, ético y responsable de los recursos informáticos en una organización, protegen la información confidencial, garantizan la integridad de los sistemas y promueven un ambiente de trabajo productivo, dentro de esta categoría se encuentran políticas de seguridad de contraseña, política de acceso y privilegios, política de uso aceptable, política de respaldo de datos, política de seguridad de la red, política de educación y concienciación, políticas de actualización de software. Y el otro tipo son las políticas de riesgos informáticos que son el conjunto de directrices y medidas establecidas para identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información y los sistemas informáticos de una organización, están diseñadas para minimizar las vulnerabilidades y proteger los activos de información de posibles amenazas y ataques, algunas políticas comunes relacionadas con la gestión de riesgos informáticos son: política de evaluación de riesgos, política de clasificación de la información, política de gestión de accesos, política de gestión de

parches y actualizaciones, política de gestión de contraseñas, política de gestión de incidentes, política de seguridad en la red.

Para (DocuSign, 2023), el proceso de transformación digital resulta impostergable para las organizaciones que deseen permanecer en la carrera competitiva y en este contexto, las políticas de seguridad informática son esenciales en el entorno empresarial por varias razones: protección de datos sensibles, cumplimiento de regulaciones y leyes, prevención de brechas de seguridad, protección de la propiedad intelectual, continuidad del negocio, confianza de los clientes.

**Marco Conceptual**

Para el desarrollo del presente estudio de pertinencia es necesario definir los siguientes términos:

Calidad: la calidad educativa es la que desarrolla en los estudiantes las competencias de aprendizaje, personales y sociales, que les permite actuar de manera democrática, pacífica e incluyente en la sociedad. (MEN, 2021)

Currículo: es el conjunto de criterios, planes de estudio, metodologías y procesos que contribuyen a la formación integral y a la construcción de la identidad cultural nacional, regional y local, incluyendo también los recursos humanos, académicos y físicos para poner en práctica las políticas y llevar a cabo el proyecto educativo institucional. (MEN, 2021)

Educación: la educación se define como un proceso de formación permanente, personal cultural y social que se fundamenta en una concepción integral de la persona humana, de su dignidad, de sus derechos y de sus deberes. (MEN, 2021)

Educación Superior: la educación superior se imparte en dos niveles: pregrado y posgrado. El nivel de pregrado tiene, a su vez, tres niveles de formación: Nivel Técnico Profesional (relativo a programas Técnicos Profesionales); Nivel Tecnológico (relativo a programas tecnológicos); Nivel Profesional (relativo a programas profesionales universitarios). La educación de posgrado comprende los siguientes niveles: Especializaciones (relativas a programas de Especialización Técnica Profesional, Especialización Tecnológica y Especializaciones Profesionales); Maestrías; Doctorados. Pueden acceder a los programas formales de pregrado, quienes acrediten el título de bachiller y el Examen de Estado, que es la prueba oficial obligatoria que presentan quienes egresan de la educación media y aspiran a continuar estudios de educación superior. (MEN, 2021)

Ingeniería: conjunto de conocimientos orientados a la invención y utilización de técnicas para el aprovechamiento de los recursos naturales o para la actividad industrial. (RAE, 2024)

Pertinencia: la educación requiere ser pertinente, también, a los entornos inmediatos en donde las personas viven su cotidianidad. Esta pertinencia se refiere a la adecuación de los procesos, contenidos y fines educativos a las condiciones concretas de las comunidades que son sujeto de las acciones educativas, de modo que no se les apliquen raseros universales con pretensiones de homogeneizar, sino que los proyectos formativos sean correspondientes a las características culturales, sociales y geográficas propias de su contexto. (MEN, 2021)

Registro Calificado: es la licencia que el MEN otorga a un programa de Educación Superior cuando demuestra ante el mismo que reúne las condiciones de calidad que la ley exige. (MEN, 2021)

Telecomunicación: sistema de transmisión y recepción a distancia de señales de diversa naturaleza por medios electromagnéticos. (RAE, 2024)

## Marco Contextual

### *Departamento del Putumayo*

De acuerdo a la Gobernación del Putumayo (2024), el departamento del Putumayo está situado en el sur del país en la región de la Amazonía, localizado entre 0° 26′ 18" y 0° 27′ 37" de latitud norte, y 73° 39" y 77° 4′ 58" de longitud oeste. La superficie es de 24.885 kms2 y limita por el Norte con los departamentos de Nariño, Cauca y el río Caquetá que lo separa del departamento de Caquetá, por el Este con el Departamento del Caquetá, por el Sur con el departamento del Amazonas y los ríos Putumayo y San Miguel que lo separan de las repúblicas de Perú y Ecuador, y por el Oeste con el departamento de Nariño (franja de territorio en litigio). El departamento está divido en 13 municipios: Mocoa, ciudad capital, Colón, Sibundoy, San Francisco, Santiago, Villagarzón, Puerto Guzmán, Puerto Caicedo, Puerto Asís, Puerto Leguízamo, Orito, San Miguel y Valle del Guamuez; 2 corregimientos, 56 inspecciones de policía, numerosos caseríos y sitios poblados. Los municipios están agrupados en 7 círculos notariales con un total de 7 notarías, un círculo principal de registro cuya cabecera es Mocoa y una oficina seccional con sede en Puerto Asís. Tiene distrito Judicial con sede en Pasto y dos circuitos judiciales con cabeceras en la capital y Puerto Asís. El

departamento forma la circunscripción electoral del Putumayo. El 1° de enero de 1995 tenía registrados 3.997 predios urbanos y 1.456 rurales.

***Municipio de Mocoa***

El municipio de Mocoa está ubicado en la parte norte del departamento del Putumayo, fisiográficamente comprende una variada gama de geoformas que van desde laderas altas de cordillera hasta planicies ligeramente onduladas. De su área total, 1.263 kilómetros, la mayor extensión comprende zonas de montaña, correspondientes a laderas altas de cordillera, cuyas características geomorfológicas son pendientes mayores al 75%, valles en V y suelos superficiales. Estarían ubicados en la parte alta de la cuenca del río Mocoa y el Río Cascabel, en estribaciones del Cerro Juanoy, su altura sobre el nivel de mar oscila entre 2.000 y 3.200 metros. Posteriormente se podrían identificar las zonas de Laderas Bajas de Cordillera, correspondientes a superficies de transición entre las zonas de alta montaña y la región de Piedemonte. Se caracterizan por pendientes entre 1.200 y 2.000 metros sobre el nivel del mar. Estas zonas estarían ubicadas en los nacimientos de los Ríos Pepino, Yumiyaco, Mulato, Campucana, la parte media de la subcuenca del río Mocoa y la parte alta de la serranía del Churumbelo. La unidad de relieve siguiente se denomina piedemonte cordillerano y corresponde a zonas de colinas altas y bajas, con terrazas fuertemente disectadas y con pendientes que oscilan entre 10% y 50%. Esta unidad fisiográfica, estaría ubicada en la Tebaida, Pepino, San Antonio, Monclart, en la parte media de los Ríos Pepino, Rumiyaco, Eslabón, Mocoa y en las estribaciones de la serranía de Churumbelo. La capital del departamento se podría ubicar dentro de esta zona. La altura sobre el nivel del mar estaría entre 600 y 1.200 metros. Por último, se

clasificarían como planicies ligeras y medianamente onduladas, a las geoformas que caracterizan las zonas de Puerto Limón, el Picudo y las colinas bajas del piedemonte cordillerano. La pendiente varía entre 0 y 10% de su altura sobre el nivel del mar y va desde los 400 a 600 metros. (Alcaldía de Mocoa, s.f.)

***Instituto Tecnológico del Putumayo***

El Instituto Tecnológico del Putumayo es una Institución de Educación Superior creada mediante Ley 65 de 1989 como Establecimiento Público, de carácter Académico del Orden Departamental, con Personería Jurídica, Autonomía Administrativa y Patrimonio Independiente, adscrito al departamento del Putumayo. Surge en nuestro territorio como respuesta a una necesidad académica de profesionalización, con capacidad de compromiso frente a las propuestas idóneas de desarrollo regional, en un proceso formativo para que se consoliden los discursos y responsabilidades en torno a la tarea histórica que debemos asumir.

Actúa en el ejercicio de autonomía y la libertad de enseñanza acorde a la Ley 30 de 1992. Constituido por la sede principal en la ciudad de Mocoa Sede Aire Libre Paraje Barrio Luís Carlos Galán y la Ampliación en el municipio de Colón. (ITP, 2016)

***Programa de Ingeniería de Sistemas***

Hacia los inicios de la actividad académica del Instituto Tecnológico del Putumayo, el programa inició su oferta con denominación Tecnología en Programación y Sistemas y su oferta era de manera terminal, es decir que los egresados una vez se titulaban debían buscar por su cuenta y voluntariamente el acceso mediante homologación en una universidad que le permitiera continuar su ciclo profesional. En

aras de garantizar la continuidad en la formación de sus 51 egresados, el ITP realiza un convenio marco con la Universidad Nacional Abierta y a Distancia UNAD para permitir que sus egresados continúen su proceso académico una vez realizado un semestre de nivelación. Cuando el Instituto Tecnológico del Putumayo se redefine para ofrecer programas por ciclos propedéuticos hacia el 2008, el Ministerio de Educación Nacional otorga el registro calificado al programa ingeniería de sistemas articulado por ciclos al programa tecnológico denominado entonces tecnología en programación y sistemas (SNIES 54210, 54209, 54211 y 4173) tanto para la sede Mocoa como la sede Sibundoy. En el 2015 el programa inicia nuevamente el proceso de verificación de condiciones mínimas de calidad bajo el decreto 1295 de 2010, finalmente el 1 de junio de 2016 mediante Resoluciones 10874 y 10875, se otorga la renovación del registro calificado para el programa ingeniería de sistemas articulado por ciclos al programa tecnología en desarrollo de software para la sede Mocoa. Los procesos internos para la obtención del registro calificado, definieron el cambio de la denominación en el ciclo tecnológico y la no presentación de renovación del registro para la sede Sibundoy, esperando solicitar en un tiempo futuro mediante extensión del lugar de ofrecimiento. (ITP, 2016)

**Marco Legal**

Constitución Política de Colombia 1991: artículo 27. El Estado garantiza las libertades de enseñanza, aprendizaje, investigación y cátedra. Artículo 69. Se garantiza la autonomía universitaria. Las universidades podrán darse sus directivas y regirse por sus propios estatutos, de acuerdo con la ley. La ley establecerá un régimen especial para las universidades del Estado. El Estado fortalecerá la investigación científica en las

universidades oficiales y privadas y ofrecerá las condiciones especiales para su desarrollo. El Estado facilitará mecanismos financieros que hagan posible el acceso de todas las personas aptas a la educación superior.

Ley 30 de diciembre 28 de 1992: por el cual se organiza el servicio público de la Educación Superior, sus fundamentos, objetivos, autonomía, el sistema nacional y de acreditación y otras disposiciones de la educación superior.

Ley 1341 de 2009 el gobierno Colombiano se está comprometiendo con el mejoramiento de la calidad de vida de las personas, por lo que para lograr dicho objetivo se consideró como factor importante la inclusión de las TIC como una Política del estado, por lo tanto el 30 de Junio de 2009 se creó Ley 1341, la cual define los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones (TIC), en su Artículo No. 2 establece que la investigación, el fomento, la promoción y el desarrollo de las Tecnologías de la Información y las Comunicaciones son una política de Estado que involucra a todos los 59 sectores y niveles de la administración pública y de la sociedad, para contribuir al desarrollo educativo, cultural, económico, social y político e incrementar la productividad, la competitividad, el respeto a los Derechos Humanos inherentes y la inclusión social.

Ley 1188 de 2008. Se regula el registro calificado de los programas de educación superior.

Decreto No. 1151 de 2008. Con el fin de impulsar la competitividad y el mejoramiento de la calidad de vida para la prosperidad de todos los colombianos, el

Gobierno Nacional creó la Estrategia de Gobierno en línea mediante el Decreto No. 1151 de 2008, el cual en su Artículo No. 2 fija que el objetivo de esta estrategia, el cual es contribuir con la construcción de un Estado más eficiente, más transparente y participativo, y que preste mejores servicios a los ciudadanos y a las empresas, a través del aprovechamiento de las Tecnologías de la Información y la Comunicación.

Decreto 1075 de 2015. Define y reglamenta el registro calificado de que trata la Ley 1188 de 2008.

Decreto 1330 de 2019. Por el cual se sustituye el Capítulo 2 y se suprime el Capítulo 7 del título 3 de la parte 5 del libro 2 del Decreto 1075 de 2015 – Único reglamento del Sector educación.

# Metodología

## Enfoque de Investigación

Con el objetivo de determinar la pertinencia para la apertura del programa de posgrado en Seguridad Informática en el Instituto Tecnológico del Putumayo, se acudió al enfoque de investigación cuantitativo. Sampieri et al. (2010), determina que el enfoque cuantitativo (que representa un conjunto de procesos) es secuencial y probatorio. Cada etapa precede a la siguiente y no podemos "brincar o eludir" pasos, el orden es riguroso, aunque, desde luego, podemos redefinir alguna fase. Parte de una idea, que va acotándose y, una vez delimitada, se derivan objetivos y preguntas de investigación, se revisa la literatura y se construye un marco o una perspectiva teórica. De las preguntas se establecen hipótesis y determinan variables; se desarrolla un plan para probarlas (diseño); se miden las variables en un determinado contexto; se analizan las mediciones obtenidas (con frecuencia utilizando métodos estadísticos), y se establece una serie de conclusiones respecto de la(s) hipótesis. Este tipo de enfoque de investigación se conforma de 6 fases que son:

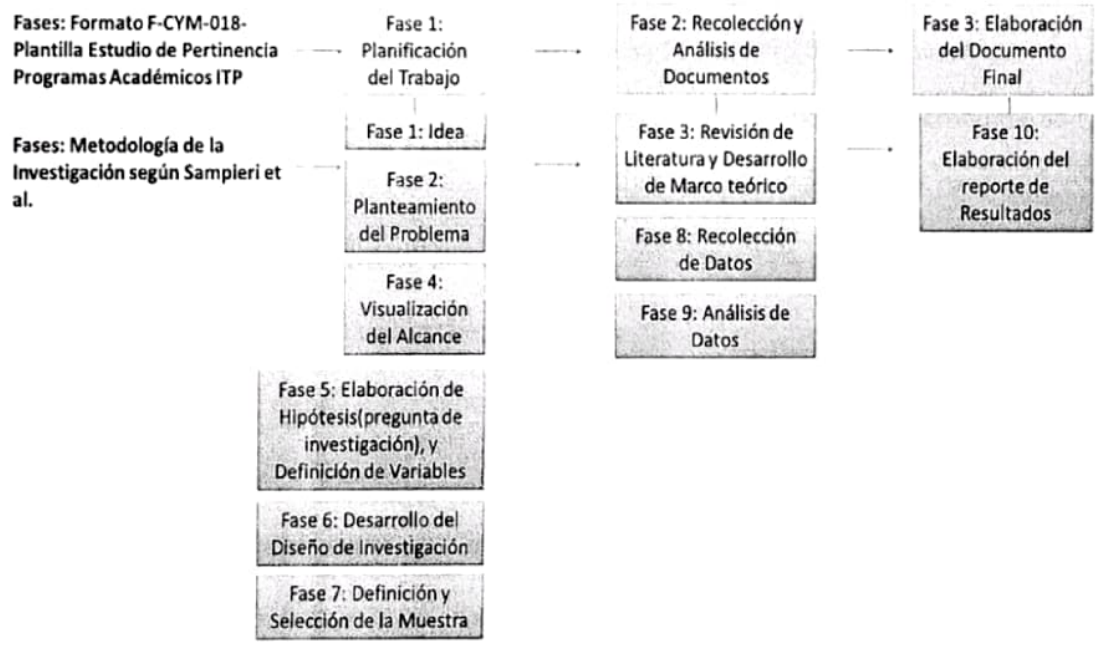
*Figura 1. Proceso Cuantitativo.*




Fuente: Libro Metodología de la Investigación, Sampieri et al. (2010).

Las fases que componen el proceso de investigación cuantitativo, están alineadas a las fases que contempla el formato establecido por el Instituto Tecnológico del Putumayo ITP, para la elaboración de estudios de pertinencia e impacto del programa (F-CYM-018-Plantilla Estudio de Pertinencia Programas Académicos). Este formato institucional tiene establecido en su diseño metodológico, tres fases: fase 1. Planificación del trabajo, fase 2. Recolección y análisis de documentos, fase 3. Elaboración del documento final. La forma como se alinean se ilustra a continuación:

***Figura 2.*** Alineación Fases Metodológicas.




Fuente: Elaboración Propia 2024.

A continuación, se describe lo que se realizó en cada una de las fases establecidas por la Institución y que se alinean con las que propone Sampieri et al. (2010):

### *Fase de Planificación del Trabajo*

Esta fase comprendió las siguientes actividades:

- Definición del estudio donde se definió la idea, título del proyecto, los integrantes, la línea de investigación, la sublínea de investigación, el lugar de ejecución, la duración del proyecto, la fecha de inicio y terminación, el tipo de proyecto y el tipo de investigación.
- Planificación del proyecto donde se definió los objetivos, el planteamiento del problema, la pregunta de investigación, la justificación, se establece una estructura conceptual a través del marco de referencia, el alcance, y la definición de la muestra.
- Definición de la metodología que se usó para el desarrollo del estudio, así como los resultados esperados, el impacto, la definición de la muestra y el cronograma de actividades.

***Fase de Recolección y Análisis de Documentos***

Esta fase comprendió las siguientes actividades:

- Recolección y uso de documentos existentes donde se analizó los datos y se ofreció resultados lógicos.
- Recolección de los datos con un orden lógico, lo que permitió encontrar hechos que sucedieron tiempo atrás, encontrar fuentes de investigación y elaborar instrumentos de investigación, etc.
- Uso de procesos como análisis, síntesis y deducción de documentos.
- Realización de forma ordenada, con una lista de objetivos específicos con el fin de construir nuevos conocimientos.

***Fase de Elaboración del Documento Final***

Esta fase comprendió las siguientes actividades considerando los objetivos del estudio:

- Determinar el estado de la oferta de educación del programa en los ámbitos nacional e internacional:
    - Análisis comparativo de mallas curriculares en el contexto internacional, nacional, regional.
    - Análisis de los perfiles profesionales, ocupacionales y modalidades en el contexto internacional y nacional.
- Identificar las necesidades del país y la región:
    - Análisis en el contexto internacional de: organización de las naciones unidas, documentos internacionales, otras comunidades académicas, ACM, IEEE.
    - Análisis en el contexto nacional de: planes y políticas nacionales MinTIC, plan de desarrollo nacional, demanda de profesionales en el área, OLE.
    - Análisis en el contexto regional de: plan de desarrollo departamental, necesidades del sector productivo.
- Establecer la oferta laboral a nivel regional:
    - Análisis de los planes regionales y locales respecto a las necesidades laborales.
    - Diseño, aplicación y análisis de la encuesta al sector productivo.
    - Análisis del nivel de empleabilidad de los egresados.
    - Diseño, aplicación y análisis de la encuesta a egresados.

**Tipo de Investigación**

El tipo de investigación de este estudio de pertinencia fue descriptiva, correlacional y explicativa. Para Sampieri et al. (2010), con frecuencia, la meta del investigador consiste en describir fenómenos, situaciones, contextos y eventos; esto es, detallar cómo son y se manifiestan. Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, esto es, su objetivo no es indicar cómo se relacionan estas… los estudios descriptivos son útiles para mostrar con precisión los ángulos o dimensiones de un fenómeno, suceso, comunidad, contexto o situación. En esta clase de estudios el investigador debe ser capaz de definir, o al menos visualizar, qué se medirá (qué conceptos, variables, componentes, etc.) y sobre qué o quiénes se recolectarán los datos (personas, grupos, comunidades, objetos, animales, hechos, etc.).

Este estudio se basó en el tipo de investigación descriptiva, porque tal como lo indica el autor referenciado, lo que se pretendió fue describir unas situaciones y se va a detallar cómo se manifiestan, esto en cuanto a las inclinaciones y preferencias de los profesionales a la hora de escoger una carrera de posgrado. Para el caso, la nueva propuesta de oferta posgradual que es una estrategia de profundización en el área de seguridad informática para las carreras relacionadas con las tecnologías de información que se puedan ofrecer en el ITP, y la que ya se oferta actualmente que es Ingeniería de Sistemas y en un futuro cercano la carrera de Ingeniería en Telecomunicaciones.

Citando nuevamente a (Sampieri et al., 2010), los estudios correlacionales tienen como finalidad conocer la relación o grado de asociación que exista entre dos o más conceptos, categorías o variables en un contexto en particular. En ocasiones sólo se analiza la relación entre dos variables, pero con frecuencia se ubican en el estudio relaciones entre tres, cuatro o más variables. Los estudios correlacionales, al evaluar el grado de asociación entre dos o más variables, miden cada una de ellas (presuntamente relacionadas) y, después, cuantifican y analizan la vinculación. Tales correlaciones se sustentan en hipótesis sometidas a prueba.

El estudio de pertinencia es correlacional en el sentido que uno de los objetivos fue precisamente conocer el grado de asociación que existe entre las mallas curriculares y perfiles a nivel internacional, nacional y regional de instituciones de educación superior de referencia, con el fin de proponer un plan de estudios para la nueva oferta de la Especialización en Seguridad Informática.

Los estudios explicativos van más allá de la descripción de conceptos o fenómenos o del establecimiento de relaciones entre conceptos; es decir, están dirigidos a responder por las causas de los eventos y fenómenos físicos o sociales. Como su nombre lo indica, su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta, o por qué se relacionan dos o más variables. (Sampieri et al., 2010)

En este sentido, este estudio fue además explicativo porque lo que se pretendió es explicar por qué el programa de Especialización en Seguridad Informática es pertinente,

o no, como propuesta de nueva oferta académica posgradual para el Instituto Tecnológico del Putumayo Mocoa.

**Diseño de Investigación**

El diseño de investigación de este estudio fue No Experimental (transversal); al respecto, Sampieri et al., (2010) lo define como la investigación que se realiza sin manipular deliberadamente variables. Es decir, se trata de estudios donde no hacemos variar en forma intencional las variables independientes para ver su efecto sobre otras variables. Lo que hacemos en la investigación no experimental es observar fenómenos tal como se dan en su contexto natural, para posteriormente analizarlos. En un experimento, el investigador construye deliberadamente una situación a la que son expuestos varios individuos. Esta situación consiste en recibir un tratamiento, una condición o un estímulo bajo determinadas circunstancias, para después evaluar los efectos de la exposición o aplicación de dicho tratamiento o tal condición. Por decirlo de alguna manera, en un experimento se "construye" una realidad. En cambio, en un estudio no experimental no se genera ninguna situación, sino que se observan situaciones ya existentes, no provocadas intencionalmente en la investigación por quien la realiza. En la investigación no experimental las variables independientes ocurren y no es posible manipularlas, no se tiene control directo sobre dichas variables ni se puede influir sobre ellas, porque ya sucedieron, al igual que sus efectos.

Este estudio se desarrolló bajo el diseño no experimental porque no se generó ninguna situación nueva sino por el contrario se analizó las existentes; es decir, no se manipularon ninguna de las variables porque estas ya sucedieron, lo que se hizo fue

analizar esas variables que permitieron dar una respuesta a la pregunta de investigación que fue ¿cuál es la pertinencia del programa de Especialización en Seguridad Informática como nueva propuesta de oferta académica posgradual en el Instituto Tecnológico del Putumayo?.

**Población y Muestra**

El tipo de muestreo al que se recurrió fue el no probabilístico, también llamado muestras dirigidas, porque, como lo determina Sampieri et al., (2010), en las muestras no probabilísticas, la elección de los elementos no depende de la probabilidad, sino de causas relacionadas con las características de la investigación o de quien hace la muestra. Aquí el procedimiento no es mecánico ni con base en fórmulas de probabilidad, sino que depende del proceso de toma de decisiones de un investigador o de un grupo de investigadores y, desde luego, las muestras seleccionadas obedecen a otros criterios de investigación. Este tipo de muestreo supone un procedimiento de selección informal.

En este sentido, las características de quienes hicieron parte de la muestra por parte del sector productivo fueron las empresas que, por su razón social y características particulares, son susceptibles, de tener en un futuro, un especialista en seguridad informática del ITP. Por parte de los egresados, se cuenta con un grupo de WhatsApp liderado por el Director de Programa de Ingeniería de Sistemas del ITP, el cual hizo una invitación masiva a la colaboración para el diligenciamiento de la encuesta, obteniendo como resultado 50 egresados encuestados.

**Técnica e Instrumento**

La encuesta es la técnica más utilizada para la obtención de información, por ello para el estudio se consideró pertinente utilizarla. El instrumento al que se recurrió fue el cuestionario.

## Resultados

El desarrollo del estudio de pertinencia para la apertura del programa de posgrado en Seguridad Informática en el Instituto Tecnológico del Putumayo, contempló en primera instancia, la determinación del estado de la oferta de educación del programa en los ámbitos nacional e internacional; por otro lado, se identificó las necesidades del país y la región; finalmente, se estableció la oferta laboral a nivel regional.

### Estado de la Oferta de Educación del Programa en los Ámbitos Nacional e Internacional

#### *Análisis Comparativo de Mallas Curriculares en el Contexto Internacional, Nacional, Regional*

El estudio de pertinencia para la apertura del programa de posgrado en Seguridad informática en el Instituto Tecnológico del Putumayo, contempló como primer objetivo específico el de analizar las mallas curriculares a nivel internacional, nacional y regional, de las Instituciones de Educación Superior que ofertan en la actualidad el programa de Especialización en Seguridad Informática.

Las Instituciones de Educación Superior que se tuvieron en cuenta fueron aquellas que, en sus páginas institucionales, disponen de información pertinente para el fin del estudio de pertinencia. De cada una de estas universidades de nivel nacional e internacional, se indagó y se extrajo sus respectivas mallas académicas del programa afín. Con estos documentos se realizó un análisis exhaustivo que condujo a la obtención de información pertinente en cuanto a créditos académicos por semestre y las áreas de conocimiento. A continuación, se relaciona la información:

**Tabla 1.** *Lista de IES a Nivel Nacional e Internacional.*

| No. | Enlace | Instituciones | Ofertas Académicas | Semestres | Modalidad |
|---|---|---|---|---|---|
| 1 | chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://virtual.uniminuto.edu/wp-content/uploads/2023/08/especializacion-en-seguridad-informatica-01-08-23.pdf?_ga=2.105731587.1698629454.1717531994-293630121.1717083168&_gac=1.120567162.1717531994.Cj0KCQjw9vqyBhCKARIsAIlcLMGTnMH9flkhBIlavhB6vWiT-kI5mEaYSak2kyilMfgYgh-vxRnApIsaAt05EALw_wcB | UNIMINUTO | Especialización en Seguridad Informática | 2 | V |
| 2 | https://estudios.unad.edu.co/plan-de-estudios-especializacion-en-seguridad-informatica | UNAD | Especialización en Seguridad Informática | 2 | V |
| 3 | https://www.unipiloto.edu.co/programas/especializaciones/especializacion-en-seguridad-informatica/ | Universidad Piloto de Colombia | Especialización en Seguridad Informática | 2 | P |
| 4 | https://www.upb.edu.co/es/postgrados/especializacion-seguridad-informatica-medellin | Universidad Pontificia Bolivariana UPB | Especialización en Seguridad Informática | 2 | P |
| 5 | https://ucompensar.edu.co/programas/especializacion-en-seguridad-informatica/ | Compensar | Especialización en Seguridad Informática | 2 | P |
| 6 | https://ucc.edu.co/programas/posgrados/Paginas/cali/especializacion-en-seguridad-de-la-informacion-cali.aspx | Universidad Cooperativa de Colombia | Especialización en Seguridad Informática | 2 | P |
| 7 | https://americana.edu.co/barranquilla/especializacion-en-seguridad-informatica/ | Corporación Universitaria Americana | Especialización en Seguridad Informática | 2 | P |
| 8 | https://www.ucatolica.edu.co/portal/Especializaci%C3%B3n/especializacion-en-seguridad-de-la-informacion/ | Universidad Católica de Colombia | Especialización en Seguridad de la Información | 2 | P |

| | | | | | |
|---|---|---|---|---|---|
| 9 | https://unir.edu.co/especializaciones/especializacion-seguridad-informatica/ | Fundación Universitaria Internacional de la Rioja (España) | Especialización en Seguridad Informática | 2 | V |
| 10 | chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ibero.mx/sites/default/files/especialidad-en-seguridad-de-la-informacion2.pdf | Universidad Iberoamericana (La Ibero) (México) | Especialidad en Seguridad de la Información | 2 | P |

Fuente: Elaboración Propia 2024.

Como se evidencia en la anterior tabla, las Instituciones de Educación Superior tenidas en cuenta para realizar el análisis y comparación de las respectivas mallas académicas a nivel nacional fueron: UNIMINUTO, UNAD, Universidad Piloto de Colombia, Universidad Pontificia Bolivariana UPB, Compensar, Universidad Cooperativa de Colombia, Corporación Universitaria Americana y Universidad Católica de Colombia. A nivel internacional se tuvo en cuenta la Fundación Universitaria Internacional de la Rioja de España y la Universidad Iberoamericana La Ibero de México.

Los créditos académicos que se contemplan en cada una de estas Instituciones de Educación Superior, se relacionan en la siguiente tabla.

***Tabla 2.*** *Créditos Académicos por Semestre.*

| **Semestres** | |
|---|---|
| **I** | **II** |
| **UNIMINUTO** | |
| 24 Créditos Total: | |
| Componente de Fundamentación: 6 créditos | |

Componente de Profundización: 15 créditos

Componente de Investigación: 3 créditos

| **UNAD** | |
|---|---|
| 13 Créditos | 12 Créditos |

Créditos Obligatorios: 19

Créditos Electivos: 6

Total de Créditos: 25

| **Universidad Piloto de Colombia** |
|---|
| 27 Créditos Total: |
| Profundización: 20 créditos |
| Investigación: 5 créditos |
| Electiva: 2 créditos |

| **Universidad Pontificia Bolivariana UPB** | |
|---|---|
| 13 Créditos | 14 Créditos |

Disciplinar: 23 Créditos

Investigativo: 2 Créditos

Básico Formación Humanista: 2 Créditos

| **Compensar** | |
|---|---|
| 13 Créditos | 13 Créditos |

| **Universidad Cooperativa de Colombia** | |
|---|---|
| 12 Créditos | 12 Créditos |

**Corporación Universitaria Americana**

28 Créditos Total

| Universidad Católica de Colombia | |
|---|---|
| 15 Créditos | 11 Créditos |
| **Fundación Universitaria Internacional de la Rioja de España** | |
| 12 Créditos | 12 Créditos |
| **Universidad Iberoamericana de México** | |
| 17 Créditos | 17 Créditos |

Fuente: Elaboración Propia 2024.

Con base en los datos anteriores se puede realizar desde ya las recomendaciones para que sean tenidas como base en la propuesta de malla académica del programa, por ejemplo, en la cantidad de créditos de las universidades analizadas, se evidencia que existe un promedio de 27 créditos académicos distribuidos en 2 semestres (1 año), lo cual es coherente con los lineamientos curriculares institucionales que establece un rango entre 26 a 30 créditos para el nivel de programas de especialización profesional.

Adicionalmente, se obtuvo la siguiente información en la distribución de los créditos de los datos analizados y las recomendaciones del caso:

- Formación en Fundamentación: Proponer un componente de fundamentación con aproximadamente 6-8 créditos, para asegurar una base sólida en conceptos básicos de seguridad informática.
- Profundización: Un componente de profundización con 15-20 créditos, permitiendo a los estudiantes especializarse en áreas avanzadas y técnicas específicas de seguridad informática.

- Investigación: Asignar 3-5 créditos a componentes de investigación para fomentar la capacidad de los estudiantes en la realización de estudios y proyectos de investigación en seguridad informática.
- Electivos: Incluir 2-5 créditos en electivos para ofrecer flexibilidad y permitir a los estudiantes seleccionar cursos según sus intereses y necesidades profesionales.
- Formación Humanista/Ética, considerar la inclusión de 2 créditos para formación integral del ser.

Por último, se requiere de una estructura equilibrada en términos de carga académica por semestre, asegurando que los estudiantes puedan manejar efectivamente el programa sin sobrecarga. Una posible distribución podría ser entre 12 a 15 créditos por semestre, dependiendo del total de créditos propuestos al final. No hay que olvidar que el ITP establece 4 créditos como obligatorios para alcanzar el nivel B1 de inglés para programas profesionales y de posgrado.

Por otra parte, se analizó las unidades de formación que se estipulan en las respectivas mallas académicas de los programas e instituciones mencionadas, se relacionan a continuación, seguido del análisis correspondiente.

***Tabla 3.*** *Unidades de Formación por Institución.*

| **Semestres** | |
|---|---|
| **I** | **II** |
| **UNIMINUTO** | |
| Componente de Fundamentación: - seguridad informática, - gestión de seguridad de la información | |

| |
|---|
| Componente de Profundización: - sistemas de detección de intrusos, - ingeniería social, - criptografía, - análisis forense, - electiva<br>Componente de Investigación: - investigación |
| **UNAD** |
| - Estrategia y gobierno corporativo<br>- Fundamentos y modelos de seguridad informática<br>- Fundamentos de intrusión y testing<br>- Trabajo de grado I<br>- Estándares, normatividad y regulación de la seguridad informática<br>- Electiva I<br>- Administración y gestión del riesgo<br>- Análisis forense<br>- Infraestructuras seguras<br>- Trabajo de grado II<br>- Electiva II<br>- Electiva III |
| **Universidad Piloto de Colombia** |
| Profundización: - modelos formales y criptografía (introducción a la seguridad y criptografía), - gestión de la seguridad y el riesgo (gestión de la seguridad y seguridad en aplicaciones), - técnicas de detección (seguridad operativa y detección de intrusos), - informática forense (informática forense)<br>Investigación: - investigación I, - Investigación II<br>Electiva: - electiva |
| **Universidad Pontificia Bolivariana UPB** |
| - Fundamentos de redes y seguridad<br>- Seguridad criptográfica<br>- Seguridad en diseño de aplicaciones y bases de datos |

| | |
|---|---|
| - Seguridad de la infraestructura<br>- Aseguramiento de sistemas operativos<br>- Aspectos legales de la seguridad<br>- Auditoria de la seguridad | - Análisis forense digital<br>- Gestión estratégica de la seguridad<br>- Seminario de actualización<br>- Seminario de investigación<br>- Electiva de formación humanista y ética |
| **Compensar** | |
| - Aplicación de métodos criptográficos<br>- Modelos estándares de seguridad informática<br>- Regulación y legislación en seguridad informática<br>- Transversal institucional<br>- Electiva I | - Hacking ético<br>- Análisis forense y delitos informáticos<br>- Cyberseguridad y cyberdefensa<br>- Electiva II<br>- Seminario de grado |
| **Universidad Cooperativa de Colombia** | |
| - Contexto de la seguridad de la información<br>- Criptografía<br>- Seguridad en aplicaciones<br>- Gestión de riesgos de la información | - Definición de modelos de seguridad<br>- Gestión estrategias de la seguridad<br>- Informática forense |

| | |
|---|---|
| | - Aspectos legales de la seguridad de la información |
| **Corporación Universitaria Americana** | |
| - Fundamentos de comunicaciones y seguridad<br>- Aspectos legales y éticos<br>- Análisis de riesgos y test de penetración<br>- Criptografía<br>- Electiva I<br>- Seminario de investigación I | - Seguridad en infraestructuras telemáticas<br>- Seguridad en el desarrollo de aplicaciones<br>- Sistemas de gestión de seguridad de la información<br>- Gestión de incidentes y computación forense<br>- Electiva II<br>- Seminario de investigación II |
| **Universidad Católica de Colombia** | |
| - Económico – administrativa: - gerencia de proyectos<br>- Gobierno y gestión de la seguridad de la información: - normas y estándares para la gestión de la seguridad de la información, - gestión de riesgos de la seguridad de la información | - Seguridad en TIC: - informática forense y gestión de incidentes de seguridad<br>- Profesional: - ética aplicada, - seminario de trabajo de grado<br>- Electivo: - electiva II |

| | |
|---|---|
| - Seguridad en TIC: - vulnerabilidades, seguridad en redes y sistemas operativos<br>- Electivo: - electiva I | |
| **Fundación Universitaria Internacional de la Rioja de España** | |
| - Hacking ético<br>- Informática forense y respuesta ante incidentes<br>- Desarrollo seguro de software y auditoría<br>- Seguridad en redes y análisis inteligente de amenazas | - Gobierno de la ciberseguridad y análisis de riesgos<br>- Seguridad en sistemas, aplicaciones y el big data<br>- Ciberdelitos y regulación de la ciberseguridad<br>- Electiva |
| **Universidad Iberoamericana de México** | |
| - Administración de riesgos de tecnología de información<br>- Auditoria en tecnología de información<br>- Gestión dl servicio de tecnología de información<br>- Gestión de incidentes | - Seguridad de tecnología de información<br>- Certificación y estándares de tecnología de información<br>- Dirección de proyectos de tecnología de información<br>- Tópicos de seguridad de TI |
| - Verano: - herramientas de seguridad de la información, - buenas prácticas de seguridad de la información | |

Fuente: Elaboración Propia 2024.

Con base en los datos de las diferentes universidades, se obtiene algunos aspectos relevantes sobre una malla académica de 2 semestres, con un máximo de 5 materias por semestre. Las mallas analizadas cubren los aspectos fundamentales, avanzados, y de investigación necesarios para una formación integral en seguridad informática.

Si el ITP lo considera puede tomar como base la siguiente propuesta de malla académica:

- Primer Semestre

✓ Fundamentos de Seguridad Informática

Descripción: Introducción a los principios y conceptos básicos de la seguridad informática.

Universidades Referencia: UNIMINUTO, UNAD, Universidad Pontificia Bolivariana UPB, Corporación Universitaria Americana.

✓ Criptografía

Descripción: Estudio de técnicas de criptografía y su aplicación en la protección de la información.

Universidades Referencia: Universidad Piloto de Colombia, Compensar, Universidad Cooperativa de Colombia, Corporación Universitaria Americana.

✓ Gestión de Seguridad de la Información

Descripción: Gestión de la seguridad en organizaciones, incluyendo la evaluación de riesgos y la implementación de políticas de seguridad.

Universidades Referencia: UNIMINUTO, Universidad Piloto de Colombia, Universidad Católica de Colombia.

- ✓ Aspectos Legales y Éticos en Seguridad Informática

Descripción: Marco legal y ético relacionado con la seguridad informática, incluyendo normativas y regulaciones.

Universidades Referencia: Universidad Pontificia Bolivariana UPB, Compensar, Universidad Cooperativa de Colombia, Corporación Universitaria Americana.

- ✓ Sistemas de Detección de Intrusos

Descripción: Técnicas y herramientas para la detección y prevención de intrusiones en sistemas de información.

Universidades Referencia: UNIMINUTO, Universidad Piloto de Colombia.

- Segundo Semestre

- ✓ Análisis Forense

Descripción: Técnicas de análisis forense digital para la investigación de incidentes de seguridad.

Universidades Referencia: UNIMINUTO, UNAD, Universidad Piloto de Colombia, Universidad Pontificia Bolivariana UPB, Compensar.

- ✓ Seguridad en Redes y Sistemas Operativos

Descripción: Protección y aseguramiento de redes y sistemas operativos contra amenazas y vulnerabilidades.

Universidades Referencia: Universidad Pontificia Bolivariana UPB, Fundación Universitaria Internacional de la Rioja de España, Corporación Universitaria Americana.

- ✓ Desarrollo Seguro de Software

Descripción: Prácticas y técnicas para el desarrollo de aplicaciones seguras y la auditoría de código.

Universidades Referencia: Fundación Universitaria Internacional de la Rioja de España, Corporación Universitaria Americana.

- ✓ Ciberseguridad y Ciberdelitos

Descripción: Estudio de las amenazas cibernéticas, ciberdelitos y las estrategias de defensa.

Universidades Referencia: Fundación Universitaria Internacional de la Rioja de España, Universidad Iberoamericana de México.

- ✓ Proyecto de Investigación en Seguridad Informática

Descripción: Desarrollo de un proyecto de investigación que permita aplicar los conocimientos adquiridos a un problema específico en seguridad informática.

Universidades Referencia: UNAD, Universidad Piloto de Colombia, Universidad Pontificia Bolivariana UPB, Corporación Universitaria Americana.

Resumen de la Malla Académica Propuesta:

Primer Semestre: Fundamentos de Seguridad Informática, Criptografía, Gestión de Seguridad de la Información, Aspectos Legales y Éticos en Seguridad Informática, Sistemas de Detección de Intrusos.

Segundo Semestre: Análisis Forense, Seguridad en Redes y Sistemas Operativos, Desarrollo Seguro de Software, Ciberseguridad y Ciberdelitos, Proyecto de Investigación en Seguridad Informática.

Esta malla académica asegura una formación integral, abarcando tanto los aspectos teóricos y prácticos como los de investigación necesarios para un posgrado en seguridad informática, sin embargo, debe incluirse un curso de inglés nivel B1 como lo establecen los lineamientos curriculares del ITP.

***Análisis de los Perfiles profesionales, Ocupacionales y Modalidades en el Contexto Internacional y Nacional***

La presente investigación contempló como objetivo específico analizar el programa de posgrado en Seguridad Informática para ofertar en el Instituto Tecnológico del Putumayo teniendo en cuenta su contexto nacional e internacional. Una de las actividades desarrolladas para el logro del propósito mencionado, fue analizar los perfiles profesionales y ocupacionales del programa, en relación a los de otras universidades de Colombia y de otros países. Como resultado de este proceso se realizó un rastreo documental de ocho universidades colombianas que fueron: UNIMINUTO, UNAD, Universidad Piloto de Colombia, Universidad Pontificia Bolivariana UPB, Compensar, Universidad Cooperativa de Colombia, Corporación Universitaria Americana y Universidad Católica de Colombia. A nivel internacional se hizo rastreo documental de: Fundación Universitaria Internacional de la Rioja de España y la Universidad Iberoamericana La Ibero de México. De estas instituciones de educación, se extrajo información pertinente en cuanto a sus perfiles profesionales y ocupacionales, con el fin de hacer un análisis comparativo.

Como producto de la investigación se obtuvo un análisis de perfiles que se relaciona en la siguiente matriz y una matriz de rasgos representativos:

***Tabla 4.*** Análisis de Perfiles.

| Universidades | Ofertas Académicas | Perfil Profesional/Perfil de Egreso/ Perfil Ocupacional |
|---|---|---|
| UNIMINUTO | Especialización en Seguridad Informática | Perfil del egresado: el egresado del programa Especialización en Seguridad Informática al culminar su proceso formativo, estará en capacidad de:<br>Construir soluciones y procesos de gestión de seguridad de sistemas de información a través del diseño, creación implementación y medición de políticas y esquemas de seguridad de los datos para determinar las necesidades de seguridad tecnológicas de hardware y software en la protección de la información. |
| UNAD | Especialización en Seguridad Informática | Perfil del Egresado: el profesional egresado del programa de especialización en Seguridad Informática de la UNAD estará en la capacidad de:<br>• Analizar, gestionar y controlar sistemas en la organización, basado en modelos, estándares, regulaciones y normas para la determinación, planeación e implementación de estrategias, políticas y planes de seguridad informática, alineados al fortalecimiento de la organización.<br>• Analizar, asegurar y auditar sistemas cibernéticos y la relación con su entorno para la determinación, planeación e implementación de planes de recuperación y respuesta proveyendo su correcta y segura disponibilidad<br>Este especialista podrá desempeñarse en cargos como:<br>• Gerente / Director ejecutivo de Seguridad informática<br>• Director de proyectos de seguridad informática<br>• Estratega de seguridad informática<br>• Experto consultor o asesor en seguridad informática<br>• Investigador forense en seguridad informática<br>• Auditor de sistemas de seguridad informática |
| Universidad Piloto de Colombia | Especialización en Seguridad Informática | 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<br>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 |

| | | | |
|---|---|---|---|
| | | 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. | posiciones relacionadas con:<br>• Administrador de seguridad de la información.<br>• Director de proyectos tecnológicos.<br>• 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.<br>• Director del área de Tecnologías de la Información y las Comunicaciones.<br>• Estratega de Seguridad de la Información.<br>• Docente Experto en Seguridad Informática. |
| Universidad Pontificia Bolivariana UPB | Especialización en Seguridad Informática | Perfil del egresado: el Especialista en Seguridad Informática de la UPB tendrá las capacidades y competencias para:<br>• Comprender y dialogar con otros saberes para generar conocimientos innovadores y ofrecer soluciones a problemáticas, condiciones de riesgo y situaciones desde una perspectiva ética, política y científica.<br>• Usar los sentidos, la imaginación, el razonamiento y el pensamiento para explicar, comprender, generar y aplicar soluciones a las necesidades de su entorno profesional amplio, en los cuales la seguridad es un atributo importante y soportado en el enfoque sistémico y la responsabilidad social.<br>• Desarrollar procesos de investigación, y desarrollo tecnológico de manera metódica, organizada, sistémica y funcional de tal manera que permitan resolver problemas del ámbito de su formación de forma innovadora, con base en el reconocimiento y aplicación de los referentes éticos y responsables de su disciplina. | |

| | | |
|---|---|---|
| | | • Desarrollar procesos de solución de problemas y desarrollo de sistemas de manera científicamente válida.<br>Los campos de acción del egresado de la Especialización son los siguientes:<br>• Formulación, evaluación, ejecución y dirección de proyectos de desarrollo tecnológico en las áreas de seguridad informática, auditoría de la seguridad, auditoría de sistemas de TI, gestión de riesgo, formación profesional y técnica.<br>• Diseño e implementación de soluciones a problemas en diferentes campos de la Seguridad informática.<br>• Asesoría y consultoría en diversos campos de la Seguridad Informática, dentro de organizaciones gubernamentales y no gubernamentales.<br>• Ejecución y dirección de procesos forenses y criminológicos.<br>• Formulación de normativas y métodos para procesos de aseguramiento o detección de anomalías asociados al área de seguridad o a procesos en los cuales la seguridad es un argumento de valor. |
| Compensar | Especialización en Seguridad Informática | El especialista en seguridad Informática egresado de la Fundación Universitaria Compensar es un profesional con habilidades para definir estrategias relacionadas con infraestructura tecnológica, capaz de implementar alternativas para mitigar los riesgos, amenazas y vulnerabilidades, identificar controles asociados a tecnologías de la información y las comunicaciones y realizar pruebas de penetración (pentesting), recolección de evidencia digital y análisis forense. Igualmente, es capaz de plantear alternativas de base tecnológica pertinentes, viables y transformadoras, a través de procesos que generan valor a la sociedad. |
| Universidad Cooperativa de Colombia | Especialización en Seguridad Informática | Perfil de egresado:<br>• Experto en Ciberseguridad: El profesional especializado en seguridad de la información posee conocimientos especializados en las más recientes amenazas cibernéticas, tácticas de hacking y medidas de protección. Su pericia contribuye significativamente a preservar la integridad, confidencialidad y disponibilidad de los datos.<br>• Gestión de Riesgos Tecnológicos: Exhibe destrezas avanzadas en la identificación y evaluación de riesgos tecnológicos. Puede diseñar e implementar estrategias efectivas para reducir la exposición de la organización a |

| | | | |
|---|---|---|---|
| | | amenazas digitales y garantizar la continuidad del negocio.<br>• Auditoría de Sistemas y Redes: Está habilitado para llevar a cabo auditorías minuciosas de sistemas y redes, detectando vulnerabilidades y asegurando la conformidad con los estándares de seguridad. Su enfoque proactivo desempeña un papel crucial en la prevención de posibles brechas de seguridad.<br>• Desarrollo de Políticas de Seguridad: Cuenta con la capacidad de crear e implementar políticas y procedimientos de seguridad de la información. Esto abarca la formulación de pautas claras para el manejo de datos sensibles, la gestión de contraseñas y la respuesta a incidentes de seguridad.<br>• Formación en Seguridad: Fomenta la conciencia en seguridad entre los empleados mediante programas educativos y campañas de sensibilización. El especialista en seguridad de la información desempeña un papel crucial en el establecimiento de una cultura organizacional orientada a la protección de la información y la prevención de ataques cibernéticos. | |
| Corporación Universitaria Americana | Especialización en Seguridad Informática | Perfil profesional: el Especialista en Seguridad Informática estará en capacidad de:<br>• Definir políticas de seguridad en las organizaciones.<br>• Definir los procedimientos para aplicar la política de seguridad informática.<br>• Definir la misión de seguridad informática de la organización en conjunto con las autoridades de la misma.<br>• Seleccionar los mecanismos y herramientas adecuados que permitan aplicar las políticas dentro de la misión establecida.<br>• Aplicar una metodología de análisis de riesgo para evaluar la seguridad | Perfil ocupacional:<br>• Administrador de Seguridad de la Información.<br>• Administrador de Seguridad Informática.<br>• Analista de Seguridad TI.<br>• Auditor de TI.<br>• Consultor de Seguridad Informática.<br>• Director de Seguridad Informática.<br>• Gestor de Seguridad de la Información TI.<br>• Ingeniero de Seguridad en Redes de Telecomunicaciones.<br>• Líder de Seguridad y Cumplimiento TI.<br>• Oficial de Seguridad TI. |

| | | | |
|---|---|---|---|
| | | informática en la organización.<br>• Diseñar sistemas informáticos teniendo en cuenta las características de seguridad necesarias.<br>• Promover la aplicación de auditorías enfocadas a la seguridad, para evaluar las prácticas de seguridad informática dentro de la organización.<br>• Realizar análisis de vulnerabilidades y test de penetración a los sistemas informáticos de las organizaciones.<br>• Llevar a cabo análisis forense sobre la evidencia digital, luego de la ocurrencia de un incidente.<br>• Crear un grupo de respuesta a incidentes de seguridad, para atender los problemas relacionados a la seguridad informática dentro de la organización.<br>• Crear y vigilar los lineamientos necesarios que coadyuven a tener los servicios de seguridad en la organización. | |
| Universidad Católica de Colombia | Especialización en Seguridad de la Información | El Especialista en Seguridad de la Información estará en capacidad de:<br>• Proponer, plantear, formular y ejecutar soluciones a problemas relativos a la seguridad de redes, para proteger la información en las organizaciones.<br>• Diseñar sistemas seguros para la | El Especialista en Seguridad de la Información podrá desempeñarse en los siguientes cargos:<br>• Administrador de seguridad informática.<br>• Oficial de seguridad informática.<br>• Consultor en seguridad informática. |

| | | | |
|---|---|---|---|
| | | gestión de la información.<br>• Diseñar e implementar arquitecturas para transacciones electrónicas seguras.<br>• Comprender y aplicar modelos, marcos de referencia, buenas prácticas y estándares internacionales relacionados con seguridad, para identificar los riesgos y controles asociados a tecnologías de la información y las comunicaciones.<br>• Identificar riesgos asociados a las tecnologías emergentes y a los nuevos modelos de servicios tecnológicos, para evaluar impactos que afecten la operación. | • Gerente o interventor de proyectos de seguridad informática. |
| Fundación Universitaria Internacional de la Rioja (España) | Especialización en Seguridad Informática | Salidas profesionales: el egresado de la Especialización en Seguridad Informática de la Fundación Universitaria Internacional de la Rioja, se habrá formado con alta calidad, sello de excelencia y exigencia académica, y podrá desempeñarse en organizaciones en cargos tales como:<br>• Gerente de Departamento Informático<br>• Director de Departamento de Seguridad<br>• Director de Sistemas Informáticos<br>• Director de Investigaciones y Desarrollo<br>• Director de Políticas y Planeación<br>• Director de Desarrollo de Proyectos<br>• Gerente de Ingeniería y Proyectos<br>• Administrador de Sistemas Informáticos<br>• Analista de Redes<br>• Auditor de TI<br>• Profesional de Redes Computacionales | |
| Universidad Iberoamericana (La Ibero) (México) | Especialidad en Seguridad de la Información | Perfil de egreso: el Especialista de la Seguridad de la Información es un profesional capaz de integrar: la auditoría, los riesgos, la criptografía y la forencia de TI para lograr detectar y controlar vulnerabilidades en los sistemas organizacionales. | |

Fuente: Elaboración Propia 2024.

A continuación, se extrae los aspectos más representativos de cada perfil consultado, y se resaltan aquellos componentes que podrían hacer parte del perfil de egreso del programa de posgrado en Especialización de Seguridad Informática del Instituto Tecnológico del Putumayo.

***Tabla 5.*** Rasgos Representativos del Análisis de Perfiles.

| **Habilidades y Competencias** | | |
|---|---|---|
| **Habilidad/Competencia** | **Descripción** | **Universidades de Referencia** |
| Diseño y Gestión de Políticas de Seguridad | Capacidad para definir, implementar y evaluar políticas y procedimientos de seguridad informática en organizaciones. | Universidad Pontificia Bolivariana (UPB), Universidad Piloto de Colombia |
| Gestión de Riesgos Tecnológicos | Identificación, evaluación y mitigación de riesgos asociados a tecnologías de la información y comunicaciones. | Universidad Piloto de Colombia, UNIMINUTO |
| Análisis Forense y Auditoría de Sistemas | Realización de auditorías de sistemas y redes para detectar vulnerabilidades y asegurar la conformidad con estándares de seguridad. | Universidad Cooperativa de Colombia, Corporación Universitaria Americana |

| | | |
|---|---|---|
| Desarrollo de Soluciones Tecnológicas | Diseño y creación de sistemas seguros, soluciones innovadoras y arquitecturas para transacciones electrónicas seguras. | Fundación Universitaria Internacional de la Rioja de España, Universidad Iberoamericana de México |
| Consultoría y Asesoría en Seguridad Informática | Asesoramiento en el diseño, implementación y gestión de proyectos y servicios relacionados con la seguridad de la información. | Universidad Católica de Colombia, UNAD |
| Educación y Sensibilización en Seguridad | Promoción de la conciencia en seguridad informática entre empleados a través de programas educativos y campañas de sensibilización. | Universidad Pontificia Bolivariana (UPB), Universidad Cooperativa de Colombia |

**Roles Ocupacionales**

| Rol Ocupacional | Descripción | Universidades de Referencia |
|---|---|---|
| Director o Gerente de Seguridad Informática | Liderar y gestionar departamentos de seguridad informática, asegurando la protección de los activos digitales de la organización. | UNIMINUTO, Universidad Piloto de Colombia |

| | | |
|---|---|---|
| Consultor o Asesor en Seguridad Informática | Proveer consultoría especializada para la implementación de estrategias y políticas de seguridad informática. | Universidad Católica de Colombia, UNAD |
| Auditor de TI | Realizar auditorías exhaustivas para asegurar el cumplimiento de las normas y estándares de seguridad en sistemas y redes. | Universidad Cooperativa de Colombia, Corporación Universitaria Americana |
| Analista de Seguridad TI | Analizar y gestionar la seguridad de los sistemas de información y las redes, identificando y mitigando riesgos potenciales. | Universidad Pontificia Bolivariana (UPB), Fundación Universitaria Internacional de la Rioja de España |
| Investigador Forense en Seguridad Informática | Realizar investigaciones forenses para identificar la causa y el impacto de incidentes de seguridad, recolectando y preservando evidencia digital. | UNIMINUTO, UNAD |
| Administrador de Seguridad de la Información | Gestionar la seguridad de la información dentro de la organización, asegurando la | Universidad Piloto de Colombia, Universidad Cooperativa de Colombia |

| | | |
|---|---|---|
| | integridad, confidencialidad y disponibilidad de los datos. | |
| Estratega de Seguridad de la Información | Desarrollar y dirigir estrategias de seguridad a nivel organizacional, alineando las políticas de seguridad con los objetivos del negocio. | Universidad Pontificia Bolivariana (UPB), Universidad Iberoamericana de México |
| Docente y Formador en Seguridad Informática | Enseñar y capacitar a futuros profesionales en seguridad informática, promoviendo la investigación y el desarrollo en el campo. | Universidad Pontificia Bolivariana (UPB), Universidad Cooperativa de Colombia |

Fuente: Elaboración propia 2024.

De acuerdo a lo anterior, en general el perfil de egreso del especialista en seguridad informática se caracteriza por una sólida formación en la gestión de la seguridad de la información, la capacidad de diseñar e implementar políticas y soluciones tecnológicas, y la habilidad para realizar auditorías y análisis forense. Los egresados están preparados para asumir roles de liderazgo, consultoría, auditoría y formación, contribuyendo significativamente a la protección de los sistemas de información y la mitigación de riesgos en organizaciones de diversos sectores.

## Necesidades del país y la Región

### *Análisis en el Contexto Internacional de Planes y Programas de Organizaciones Internacionales*

Para el logro del propósito del presente estudio de pertinencia, es importante valorar los retos, oportunidades y necesidades del programa y sus profesionales egresados en las áreas relacionados con la seguridad informática a nivel internacional. Para ello, fue necesario acudir a fuentes de información digital que brindaron información pertinente para el estudio, como la Organización de las Naciones Unidas ONU, el Banco Mundial, entre otros.

Como resultado del análisis realizado, se obtuvo una matriz DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas), la cual resume el propósito de esta actividad.

***Tabla 6.*** Matriz de Retos, Oportunidades y Necesidades del Programa a Nivel Internacional.

| | **Positivos** | **Negativos** |
|---|---|---|
| **Factores Internos** | **Fortalezas** | **Debilidades** |
| | El mundo empresarial, altamente competitivo y proclive a riesgos, se ha volcado hacia la búsqueda de seguridad para sus datos. Esta demanda ha permitido un crecimiento exponencial de todas carreras relacionadas con la protección de las comunicaciones. Es una buena salida que los profesionales o interesados en la informática profundicen en sus estudios. En la práctica, si el total de licenciados, ingenieros y técnicos no alcanza para satisfacer las necesidades del mercado, los profesionales especializados se convierten en personal muy valorado por parte de prácticamente todas las industrias actuales. (ceupe, 2020) | Hay más vacantes, impulsadas por una necesidad cada vez más latente, sin embargo, el crecimiento no es tan acelerado en el número de profesionales que egresan de universidades e institutos técnicos en estas áreas. (ceupe, 2020)<br><br>La escasez de talento sigue siendo un problema preocupante. Además de ello, los continuos y crecientes ataques, cada vez más frecuentes, más evasivos, más sofisticados y que llegan a través de muchas más vías, supone un reto para las empresas que aún no están al 100% preparadas. Por ejemplo, ahora, el SEO "poisoning", está resultando un problema con páginas infectadas que aparecen en los primeros resultados de los buscadores, pasando |

| | | |
|---|---|---|
| | La seguridad informática ha surgido como una necesidad, debido a los intensos cambios en el sector productivo y, a la manera en cómo vive la sociedad mundial gracias a la transformación digital. Por este motivo, la información se ha convertido en uno de los activos principales de las empresas e individuos y, para mantener sus datos resguardados, deben invertir en este tipo de seguridad. La seguridad informática se encarga de prevenir y detectar el uso no autorizado de un sistema informático e implica la protección contra intrusos que pretendan utilizar las herramientas y/o datos empresariales maliciosamente o con intención de lucro ilegítimo. (UdeCataluña, 2024) | desapercibidas como tales". (Revista BYTE, 2024)<br><br>En toda empresa lo más preciado que se tiene es la información. Se necesita cómo salvaguardarla, no solamente cuando está almacenada en un lugar, también si se está transmitiendo por medio de internet o en el ciberespacio. (Universidad Galileo, 2024) |
| **Factores Externos** | **Oportunidades** | **Amenazas** |
| | Un reciente informe de INCIBE señala que se necesitarán más de 83 000 profesionales en el sector, siendo el actual número de especialistas ligeramente superior a los 42.000. (Cámara de Comercio Bilbao, 2024)<br><br>¿Qué se necesitará para que los países cosechen los beneficios de la digitalización y participen de lleno en la economía digital mundial? Crear sistemas digitales seguros y fiables: en un mundo que se está digitalizando, el fortalecimiento de la capacidad en áreas como la ciberseguridad y la protección de los datos personales se ha vuelto más importante que nunca. (Banco Mundial, 2024)<br><br>Se busca: millones de expertos en ciberseguridad. Salario: lo que pidas. Una serie de graves violaciones de la seguridad digital ocurridas el año pasado son un llamado de atención a las empresas de Estados Unidos sobre la necesidad de invertir en ciberseguridad. (CNN, 2021)<br><br>Actualmente, muchos puestos de trabajo en estas áreas están vacantes (alrededor de 3.4 millones en todo el mundo), por lo que las instituciones deben equipar a los estudiantes para | El último informe de Verizon, el Data Breach Report 2021, reveló que 'el phishing y el ransomware son dos amenazas cada día más peligrosas' y ambas amenazas han reportado un incremento en comparación con el año anterior: phishing en un 11 % y ransomware un 6 %. (E&N, 2023)<br><br>De acuerdo con la Interpol en su informe: "Interpol Cybercrime: Covid-19 Impact 2020", las principales amenazas que en la actualidad acechan a las empresas son en un 59% el phishing, scam y fraude, seguido del malware y ransomware que representan un 36%, dominios maliciosos un 22% y por último las fake news con un 14%. La mayoría de los ataques (65%) tienen como finalidad un incentivo económico, un 30% afectar la reputación de las empresas, un 5% acciones de espionaje y un 3% otras finalidades. (E&N, 2023)<br><br>Los programas espía y de desinformación basados en inteligencia artificial van en aumento, por lo que urge regular este ámbito, según expertos independientes en derechos humanos designados por la ONU. (ONU, 2023) |

| | | |
|---|---|---|
| | satisfacer esta demanda. (Universidad Galileo, 2024)<br><br>El informe anual de Adecco señala que las profesiones más demandadas en 2024 serán los ingenieros de IA y ML, los expertos en ciberseguridad (a medida que avanzan las amenazas y se vuelven más complejas) y los desarrolladores de software específico. (Bit Life media, 2024)<br><br>La demanda de profesionales de seguridad informática está en constante aumento, y esta tendencia continuará en el futuro cercano. Según el informe de ciberseguridad de Cisco 2021, el 80% de las empresas experimentaron un aumento en los ataques cibernéticos durante la pandemia, lo que ha llevado a un aumento en la demanda de profesionales en esta área. Además, se espera que la demanda de empleos en seguridad informática aumente un 31% para 2029, según el Buró de Estadísticas Laborales de EE. UU. (Corporación Universitaria Americana,2021) | El viernes se produjo un nuevo recordatorio del riesgo de los ciberataques, ya que Microsoft dijo que los cibercriminales que estaban detrás de la brecha de 2020, Solar Winds, lanzaron un nuevo ataque a más de 150 agencias gubernamentales, grupos de reflexión y otras organizaciones a nivel mundial. (CNN, 2021) |

Fuente: Elaboración Propia 2024.

El análisis de la matriz de retos, oportunidades y necesidades del programa de posgrado en seguridad informática a nivel internacional resalta varios aspectos críticos para el desarrollo y fortalecimiento de este campo a nivel global, entre los cuales se tiene:

- Factores Internos

✓ Fortalezas:

Alta Demanda en el Mercado: La creciente necesidad de seguridad en el mundo empresarial, impulsada por la transformación digital, ha generado una demanda exponencial de profesionales especializados en seguridad informática. Las empresas valoran altamente a los especialistas capaces de proteger sus datos y comunicaciones, lo que convierte esta área en una salida profesional prometedora.

Crecimiento de Carreras Relacionadas: La expansión de carreras en seguridad informática se ve respaldada por la urgente necesidad de proteger información sensible en diversas industrias, desde la financiera hasta la sanitaria.

- ✓ Debilidades:

Escasez de Profesionales: A pesar del aumento de vacantes, la cantidad de profesionales que egresan de universidades e institutos técnicos es insuficiente para satisfacer la demanda del mercado. Este déficit es una preocupación persistente. Incremento de Amenazas: Las empresas enfrentan retos significativos debido a ataques cibernéticos cada vez más sofisticados y frecuentes, como el SEO poisoning, que implica páginas infectadas apareciendo en los primeros resultados de buscadores sin ser detectadas.

- Factores Externos

- ✓ Oportunidades:

Incremento en la Necesidad de Profesionales: Se prevé que se necesitarán más de 83,000 profesionales en el sector de la seguridad informática, según INCIBE. Esta necesidad subraya la importancia de capacitar a más especialistas para cerrar la brecha existente.

Participación en la Economía Digital: La creación de sistemas digitales seguros es crucial para que los países puedan cosechar los beneficios de la digitalización y participar plenamente en la economía digital mundial.

Altos Salarios y Demanda: La urgencia por contratar expertos en ciberseguridad es tal que las ofertas laborales en este campo permiten a los profesionales negociar altos salarios, destacando la relevancia y la demanda constante por estos expertos.

- ✓ Amenazas:

Aumento de Ciberataques: La pandemia ha acelerado los ataques cibernéticos, con un 80% de las empresas reportando incrementos en incidentes de seguridad. Phishing y ransomware se han vuelto particularmente prevalentes, representando una amenaza creciente para las organizaciones.

Impacto Económico y de Reputación: La mayoría de los ataques cibernéticos tienen como objetivo un incentivo económico, pero también buscan dañar la reputación de las empresas, realizar espionaje o difundir desinformación.

Regulación y Tecnología: La proliferación de programas espía y desinformación basada en inteligencia artificial demanda una regulación urgente para proteger los derechos humanos y la integridad de los datos.

A nivel internacional la seguridad informática se establece como un campo esencial y en constante evolución, con una demanda creciente que ofrece numerosas oportunidades para los profesionales que se forman en esta área. Sin embargo, la falta de personas capacitadas y el mejoramiento de las técnicas de las amenazas cibernéticas presentan retos significativos. Para enfrentar estos desafíos, es necesario que, a nivel de instituciones educativas como el ITP, se generen procesos de formación y capacitación y a nivel de gobierno, se trabaje hacia el desarrollo de políticas y tecnologías que fortalezcan la ciberseguridad, garantizando así un entorno digital más seguro.

### *Análisis en el Contexto Nacional de Planes y Políticas Nacionales*

Para el logro del propósito del presente estudio de pertinencia, es importante valorar los retos, oportunidades y necesidades del programa y sus profesionales egresados en las áreas relacionados con la seguridad informática a nivel nacional. Para ello, fue necesario acudir a fuentes de información digital que brindaron información pertinente para el estudio, como la MinTIC, Plan Nacional de Desarrollo "Colombia, corporaciones, potencia mundial de la vida" Asociación Colombiana de Informática Sistemas y Tecnologías Afines ACIS, entre otros.

Como resultado del análisis realizado, se obtuvo una matriz DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas), la cual resume el propósito de esta actividad.

***Tabla 7.*** Matriz de Retos, Oportunidades y Necesidades del Programa a Nivel Nacional.

| | **Positivos** | **Negativos** |
|---|---|---|
| **Factores Internos** | **Fortalezas** | **Debilidades** |
| | La formación en CiberHub que desarrollaremos con BIOS busca responder a un déficit crítico del país, que carece de alrededor de 15.000 especialistas en ciberseguridad, y se proyecta que necesitará 10.000 más en los próximos dos a tres años. Desde el Gobierno del Cambio trabajamos para cerrar esa brecha. Este programa le apunta a formar a 2.000 agentes en la primera instancia, ofreciendo conocimientos a través de una plataforma virtual de primer nivel, empleada para entrenar fuerzas de ciberseguridad a nivel mundial. (MinTIC, 2023)<br><br>El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) expide la Resolución 500 de 2021, "por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital". (MinTIC, 2023) | En 2021 los ciberataques a las redes corporativas aumentaron 50% por frente al 2020. Es vital conocer las tendencias cibernéticas. (La República, 2022)<br><br>Las tres primeras consecuencias de esta brecha, de acuerdo con el estudio, incluyen sistemas mal configurados con una incidencia de 32%; no tener tiempo suficiente para una evaluación y gestión de riesgos adecuados, con 30%; y la tardanza para aplicar parches en sistemas críticos, con 29%. (FayerWayer, 2022) |

| | | |
|---|---|---|
| | La seguridad informática es esencial para proteger los sistemas y datos críticos, como información personal, datos financieros y registros médicos. Al trabajar en este campo, estás ayudando a proteger a las personas y organizaciones de los ataques cibernéticos malintencionados. (Corporación Universitaria Americana, 2021) | |
| **Factores Externos** | **Oportunidades** | **Amenazas** |
| | Según Siguard, el 90% de los ataques informáticos en las compañías ocurren por falta de capacitación al personal. Es por eso que, además de la adquisición de softwares o prestadores de servicios de seguridad, las empresas también deben invertir para que el talento humano sepa cómo prevenir y reaccionar ante algún ataque. (Caracol Radio, 2023)<br><br>Consideramos importante el fortalecimiento de la educación en tecnología, temas de ética de las tecnologías emergentes y de ciberseguridad, como elementos importantes del desarrollo digital. (PND, 2022-2026)<br><br>A medida que las amenazas cibernéticas continúan evolucionando, la demanda de profesionales altamente capacitados en este campo es cada vez mayor. Al obtener una especialización en seguridad de la información, te conviertes en un defensor activo de la integridad de la información y la infraestructura digital. (Politécnico Grancolombiano, 2023)<br><br>Colombia es cada día más consciente de la necesidad de reforzar su ciberseguridad frente a los ataques de los hackers. Fruto de esa realidad, fue la renovación por parte de los ministerios de las TIC y de Defensa, y el Departamento de Planeación, del documento CONPES, que estimaba una inversión de 85.000 millones de pesos en seguridad digital para el país, tal y como anunció enter.co a mediados de 2016. (ACIS, 2022) | El último informe de Verizon, el Data Breach Report 2021, reveló que 'el phishing y el ransomware son dos amenazas cada día más peligrosas' y ambas amenazas han reportado un incremento en comparación con el año anterior: phishing en un 11 % y ransomware un 6 %. (E&N, 2023)<br><br>De acuerdo con la Interpol en su informe: "Interpol Cybercrime: Covid-19 Impact 2020", las principales amenazas que en la actualidad acechan a las empresas son en un 59% el phishing, scam y fraude, seguido del malware y ransomware que representan un 36%, dominios maliciosos un 22% y por último las fake news con un 14%. La mayoría de los ataques (65%) tienen como finalidad un incentivo económico, un 30% afectar la reputación de las empresas, un 5% acciones de espionaje y un 3% otras finalidades. (E&N, 2023)<br><br>En 2023 se evidenció un aumento de los ciberataques en Colombia, representando una seria amenaza para las empresas. Según IBM Security, desde 2022 Colombia se posicionó como el segundo país en Latinoamérica en número de intentos de ciberataques recibidos, con un total de 20.000 millones. (Impacto TIC, 2023) |

| | |
|---|---|
| | La demanda de profesionales de seguridad informática está en constante aumento, y esta tendencia continuará en el futuro cercano. Según el informe de ciberseguridad de Cisco 2021, el 80% de las empresas experimentaron un aumento en los ataques cibernéticos durante la pandemia, lo que ha llevado a un aumento en la demanda de profesionales en esta área. Además, se espera que la demanda de empleos en seguridad informática aumente un 31% para 2029 (Corporación Universitaria Americana, 2021) |

Fuente: Elaboración Propia 2024.

Los retos, oportunidades y necesidades del programa de seguridad informática en Colombia se basan en un entorno de aspectos críticos que requieren atención tanto en el ámbito formativo como en el operativo, por ejemplo, se extraen los siguientes datos relevantes:

- Fortalezas Internas

✓ Desarrollo de Programas Formativos Especializados:

La creación del programa CiberHub en colaboración con BIOS busca cerrar la brecha crítica de aproximadamente 15,000 especialistas en ciberseguridad, proyectándose una necesidad adicional de 10,000 profesionales en los próximos años. Este esfuerzo, impulsado por el Gobierno del Cambio, está diseñado para formar a 2,000 agentes inicialmente, utilizando una plataforma virtual de alto nivel reconocida internacionalmente.

✓ Marco Regulatorio Sólido:

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha establecido lineamientos claros mediante la Resolución 500 de 2021, que define

estándares para la estrategia de seguridad digital y adopta un modelo de seguridad y privacidad, fortaleciendo así la infraestructura normativa del país en este ámbito.

- Debilidades Internas

✓ Aumento de Ciberataques y Vulnerabilidades:

Los ciberataques a redes corporativas aumentaron un 50% en 2021 en comparación con 2020. Las principales consecuencias de la brecha incluyen sistemas mal configurados, falta de tiempo para una adecuada gestión de riesgos, y tardanza en la aplicación de parches en sistemas críticos. Estos factores resaltan la urgencia de mejorar la capacidad de respuesta y la gestión de la seguridad informática.

- Oportunidades Externas

✓ Capacitación y Educación en Ciberseguridad:

El 90% de los ataques informáticos en las compañías se deben a la falta de capacitación del personal. Esto destaca la necesidad de invertir no solo en tecnologías de seguridad, sino también en la formación continua del talento humano para prevenir y reaccionar eficazmente ante amenazas.

✓ Inversión en Seguridad Digital:

La renovación del documento CONPES y la inversión de 85,000 millones de pesos en seguridad digital refuerzan el compromiso del país con la ciberseguridad. Esta inversión es crucial para mejorar las capacidades de defensa contra ciberataques y asegurar una infraestructura digital robusta.

- Amenazas Externas

✓ Evolución y Sofisticación de Amenazas:

Informes recientes destacan un incremento en amenazas como phishing y ransomware, con un aumento del 11% y 6% respectivamente. Además, la Interpol ha identificado el phishing, el malware y el ransomware como las principales amenazas, que en su mayoría buscan incentivos económicos, pero también pueden afectar la reputación y la seguridad de las empresas.

- ✓ Aumento de Ciberataques en Colombia:

En 2023, Colombia experimentó un aumento significativo en ciberataques, posicionándose como el segundo país en Latinoamérica con el mayor número de intentos de ciberataques, alcanzando los 20,000 millones. Esta situación subraya la necesidad urgente de fortalecer las defensas cibernéticas a nivel nacional.

A nivel de Colombia la seguridad informática tiene retos significativos, pero también oportunidades importantes, uno de ellos es la alta demanda de profesionales capacitados y la necesidad de robustecer las infraestructuras de seguridad. El gobierno debe invertir en educación, capacitación continua y fortalecimiento de las políticas regulatorias para contrarrestar el aumento de los ciberataques. El compromiso del gobierno y las instituciones educativas es fundamental para cerrar la brecha de talento y desarrollar una defensa efectiva contra las amenazas cibernéticas, asegurando así la integridad y la seguridad de los sistemas y datos críticos en el país.

***Análisis en el Contexto Regional de Planes de Desarrollo***

Para el logro del propósito del presente estudio de pertinencia, es importante valorar los retos, oportunidades y necesidades del programa y sus profesionales egresados en las áreas relacionados con las redes y las telecomunicaciones a nivel regional. Para

ello, fue necesario acudir, como fuentes de información, al Plan Estratégico de Tecnologías de la Información del Putumayo 2021-204, medios de comunicación digital local, entre otros.

Como resultado del análisis realizado, se obtuvo una matriz DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas), la cual resume el propósito de esta actividad.

***Tabla 8.*** Matriz de Retos, Oportunidades y Necesidades del Programa a Nivel Regional.

| | **Positivos** | **Negativos** |
|---|---|---|
| **Factores Internos** | **Fortalezas** | **Debilidades** |
| | En el mes de febrero se realizó un Taller de Seguridad Digital organizado por Colnodo y el Fondo Noruego para los Derechos Humanos en Villagarzón, Putumayo, en el marco del proyecto de "Formación en Seguridad Digital a organizaciones de sociedad civil". Un encuentro que reunió organizaciones indígenas, ambientalistas y comunitarias de la región. La importancia de la Seguridad Digital en el trabajo de las comunidades fue el tema principal de esta sesión, un espacio que reunió varios temas y prácticas relevantes para salvaguardarse en el ecosistema digital. (Colnodo, 2023) | El incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo. (PETI Mocoa 2021-2024) |
| **Factores Externos** | **Oportunidades** | **Amenazas** |
| | La ingeniería en desarrollo y gestión de software orientada a la seguridad informática cada día toma más relevancia en el mundo actual. La constante evolución de las aplicaciones y sistemas digitales aumenta la demanda de profesionales capacitados en seguridad en desarrollo de software y protección de datos. Las empresas ya no sólo buscan servicios tercerizados de protección, sino que prefieren contar en sus equipos con expertos en seguridad | La Contraloría General de la República, en colaboración con la Gobernación del Putumayo, ha logrado restablecer con éxito una suma significativa de más de $3.502 millones de recursos públicos, previamente víctimas de un sofisticado ataque cibernético. Este esfuerzo conjunto ha dado como resultado la recuperación íntegra de los fondos robados, incluyendo la restitución de los correspondientes intereses, por parte de la entidad financiera involucrada. Este acontecimiento |

| | | |
|---|---|---|
| | informática que puedan prevenir, atender y solucionar cualquier tipo de amenaza cibernética, garantizando así la integridad de sus datos e información. Actualmente, las organizaciones pequeñas, medianas y grandes, de todos los sectores e industrias, dependen del uso de software seguros y confiables para que su operación sea eficiente. El software es fundamental en todas las áreas de una empresa, por lo tanto, contar con profesionales en seguridad en desarrollo de software y seguridad informática es primordial para que los sistemas de las compañías sean resistentes a ataques y vulneraciones. Es por eso que los profesionales en ingeniería en desarrollo y gestión de software deben ser cada vez más especializados, pues no sólo se encargan de implementar aplicaciones y sistemas informáticos, sino que abordan y enfrentan los desafíos de seguridad que día a día parecen ser más complejos y sofisticados.(IBERO, 2024) | resalta la importancia de contar con mecanismos de seguridad sólidos en la gestión de recursos públicos y subraya la necesidad de una supervisión y respuesta efectivas en situaciones de riesgo cibernético. (Valor & Dinero, 2024)<br><br>El último ataque perpetrado en el año 2022 en Colombia, lo sufrió la gobernación de Putumayo el 25 de diciembre, donde fue sustraído más de 3.100 millones de pesos de una de las cuentas que pertenecían a los recursos del Fondo Territorial de Pensionados (FONPET) Y estos fueron distribuidos a 10 cuentas bancarias en todo el país. El ataque que más de utiliza por los ciberdelincuentes es el ransonware, ya que a través de este pueden secuestrar información y de esta manera pedir grandes cantidades de dinero a las entidades. Los ciberdelincuente no solo atacan a grandes empresas, sino que, medianas y pequeñas empresas también se ven involucradas en estos ciberdelitos. (Information Technology, 2022) |

Fuente: Elaboración Propia 2024.

Del análisis de la matriz de retos, oportunidades y necesidades para el programa de posgrado de seguridad informática en el Putumayo, se tiene la existencia de fortalezas internas como la implementación de programas de formación en seguridad digital, como el taller organizado por Colnodo y el Fondo Noruego para los Derechos Humanos, que ha capacitado a organizaciones locales en prácticas esenciales para la protección en el entorno digital, pero esto solo es una capacitación y no un programa de formación profesional. Ahora bien, también existe debilidades significativas, como el incremento de amenazas cibernéticas a medida que más personas y empresas permanecen con alta

actividad en internet. Esta situación exige una protección y el fortalecimiento de las capacidades locales para gestionar riesgos de manera efectiva, de ahí que, formar profesionales especializados en este campo es de gran aporte por parte del ITP al departamento.

En términos de oportunidades, la creciente demanda de profesionales especializados en seguridad informática es notable. A medida que en el Putumayo crecen las empresas, éstas relativamente buscarán contratar con expertos para garantizar la seguridad de sus sistemas y datos. También es importante resaltar los esfuerzos exitosos de recuperación de recursos robados en ataques cibernéticos, como la colaboración entre la Contraloría General de la República y la Gobernación del Putumayo, lo cual destaca la importancia de contar con mecanismos de seguridad sólidos y respuestas eficaces ante incidentes, y esto lo hace un profesional especializado.

El programa de posgrado en seguridad informática que podría ser ofrecido por el ITP, se enfrenta a un entorno lleno de desafíos, pero también de oportunidades significativas. Se requiere de la combinación de un plan de estudios acorde a las necesidades y la inversión en tecnologías de seguridad que permita a sus egresados aportar en el cuidado del activo informático.

**Oferta Laboral a Nivel Regional:**

***Análisis de los Planes Regionales y Locales Respecto a las Necesidades Laborales***

Con el fin de determinar la pertinencia para la apertura del programa de posgrado en Seguridad Informática en el Instituto Tecnológico del Putumayo, es necesario realizar un análisis de los planes regionales y locales respecto a las necesidades laborales; sin

embargo, a la fecha, el departamento del Putumayo y sus trece municipios: Mocoa, Santiago, San Francisco, Colón, Sibundoy, Villagarzón, Orito, Puerto Asís, Puerto Guzmán, Valle del Guamuez, Puerto Leguízamo, Puerto Caicedo, y San Miguel, sus planes de desarrollo aún se encontraban en discusión en mesas de trabajo y no había acceso a ellos. Por este motivo, el desarrollo de este objetivo no se pudo llevar a cabo.

No obstante, a nivel nacional se hizo una revisión documental y se encontró lo siguiente: el Consejo Privado de Competitividad y su "Informe Nacional de Competitividad 2023-2024", buscando promover la educción dual, el CPC, Confecámaras y Swisscontact desarrollaron una encuesta para medir las necesidades de talento humano, establece que las tecnologías que impactarán la creación de empleo en el país están relacionadas con el cifrado y la ciberseguridad, las tecnologías de educación y el desarrollo de la fuerza laboral, seguidas de las tecnologías de gestión ambiental. Según Manpower Group (2023), en los 27% 14%-0,8-0,6-0,4-0,2 Global 0 Colombia 0,2 28% últimos años se han incrementado las dificultades para encontrar el talento calificado que necesita el sector productivo, pues entre 2013 y 2023 la brecha se amplió en un 34 %, por lo que hoy en día seis de cada diez empresarios creen que no es posible llenar una vacante.

***Diseño, Aplicación y Análisis Encuesta Sector Productivo***

Con el propósito de determinar la pertinencia para la apertura del programa de posgrado en Seguridad Informática en el Instituto Tecnológico del Putumayo, fue necesario identificar los requerimientos del sector productivo del departamento del Putumayo frente al área de la seguridad informática.

Para el desarrollo de esta actividad se acudió a la encuesta como instrumento de recolección de información que permitió determinar las pretensiones frente al área mencionada. Las empresas que se tuvieron en cuenta fueron únicamente aquellas que por su razón social son susceptibles de integrar dentro de su talento humano, especialistas en el área de la seguridad informática.

El cuestionario aplicado comprendió un total de nueve preguntas; las cuatro primeras enfocadas al aspecto personal del encuestado, las demás al análisis de los requerimientos como empresarios, empleadores o jefes de talento humano, frente al área de seguridad informática. Se encuestaron en total 12 de 20 empresas pertenecientes a los diferentes municipios del departamento del Putumayo que atendieron al llamado y a la colaboración.

El cuestionario fue lanzado mediante medio tecnológico usando contactos directos de las empresas por parte de la Dirección del Programa de Ingeniería de Sistemas del ITP. La recolección se hizo usando el formulario de google, mediante el link https://forms.gle/qagkDfCXPcE2QMmH7

El formulario permaneció activo 24 horas, tiempo que se consideró suficiente por la efectividad del medio de difusión.

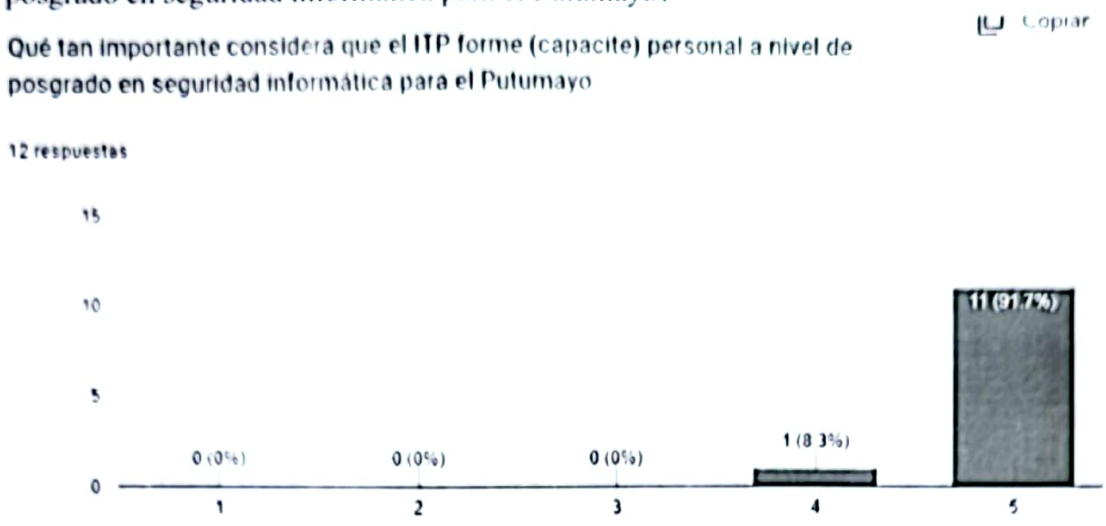
Las empresas que hicieron parte de la encuesta fueron:

1. Aguas la Cristalina E.S.P
2. INQTEL S.A.S
3. Sistemas y Videovigilancia AYM S.A.S
4. El Inge S.A.S

5. DYNETSA S.A.S
6. MOVISTAR
7. Secretaria de Salud Del Putumayo
8. Laboratorio Buitrago SAS
9. Secretaria de Educación Departamental
10. Empresa de Energía del Putumayo S.A ESP
11. Instituto Tecnológico del Putumayo
12. TECNOBOOT S.A.S
13. HSE INGENIERIA SAS – No respondió
14. IE GORETTI MOCOA – No respondió
15. HOSPITAL JMH – No respondió
16. ISANET S.A.S – No respondió
17. COMPUMASTER S.A.S – No respondió
18. PROINTEL S.A.S – No respondió
19. IE PIO XII MOCOA – No respondió
20. CLARO – No respondió

Entre el personal que dio respuesta a la encuesta se encontraban: propietarios, jefe de personal, gerente, ingeniero de sistemas, líder de proceso, líder TIC, profesional de apoyo a centro de control.

***Figura 3.*** ¿Qué tan importante considera que el ITP forme (capacite) personal a nivel de posgrado en seguridad informática para el Putumayo?




Fuente: Elaboración Propia 2024.

El 58,3% de las empresas encuestadas pertenecen al sector privado, seguido del 33,3% del sector público, quienes en su mayoría (83,3%) cuentan con un área TIC atendida por 1 a 3 personas en promedio, la cual es considerada de gran importancia para el funcionamiento de la empresa. Adicionalmente, se reconoce en alto nivel la importancia no solo de la seguridad informática para las empresas, sino en que definitivamente están de acuerdo en que el ITP forme a profesionales especializados en este campo; para ello, se considera unos niveles de importancia sobre las competencias o habilidades que deberían tenerse en cuenta. En la siguiente tabla se ilustra lo mencionado.

En los anexos se puede evidenciar los resultados completos de las otras preguntas, pero que en todo caso ya fue interpretado sus resultados anteriormente.

Documentos anexos:

- **Anexo 1.** Tabulación Encuesta Empleadores.

A continuación, se presenta un análisis de las respuestas a la pregunta sobre la importancia de las competencias o habilidades en el nivel de formación posgrado en seguridad informática. Las competencias o habilidades fueron propuestas con base en los datos recopilados en el análisis de perfiles, mallas de programas similares ofrecidos en Colombia y en análisis de retos, oportunidades que tendría el programa.

Para mayor comprensión del lector, el nivel de importancia se ha resaltado en 3 colores, verde, amarillo y rosa, respecto a la cantidad de respuestas obtenidas por cada área y el nivel correspondiente; siendo verde un área o componente que por encima de la mitad de encuestados han señalado como de "Muy Alta" importancia, amarillo de entre 3 y 6 respuestas obtenidas para un nivel "Alto", color rosa menores a 3 respuestas para un nivel "Medio" hacia abajo. Cabe aclarar que esta dinámica, es solamente de ayuda interpretativa, no corresponde a una metodología en especial, pero constituye para los autores una forma de evidenciar las tendencias de las posibles ocupaciones, áreas y componentes a la hora de establecer más adelante un perfil de egreso, competencias y unidades de formación para el plan de estudios.

***Tabla 9.*** ¿Cuáles de las siguientes competencias o habilidades considera importantes en la formación a nivel posgrado del profesional en seguridad informática?

| **Área o Componente para posgrado en seguridad informática** | **Nivel de Importancia** | | | | |
|---|---|---|---|---|---|
| | **Muy Alta** | **Alta** | **Media** | **Baja** | **Muy Baja** |
| Conocimiento técnico profundo: Entender los sistemas operativos, redes, protocolos de | 7 | 5 | 0 | 0 | 0 |

| | | | | | |
|---|---|---|---|---|---|
| comunicación y tecnologías de seguridad es fundamental para identificar vulnerabilidades y aplicar soluciones adecuadas. | | | | | |
| Análisis de riesgos: Ser capaz de evaluar y analizar los riesgos de seguridad de una organización, sus activos y las posibles amenazas que enfrenta. | 9 | 3 | 0 | 0 | 0 |
| Gestión de incidentes: Saber cómo responder eficazmente a incidentes de seguridad, desde la detección hasta la contención y la recuperación. | 10 | 2 | 0 | 0 | 0 |
| Penetration testing (pruebas de penetración): Conocer y aplicar técnicas de hacking ético para identificar y corregir debilidades en sistemas y redes antes de que puedan ser explotadas por atacantes reales. | 9 | 3 | 0 | 0 | 0 |
| Conciencia de la legislación y regulaciones: Estar al tanto de las leyes y regulaciones relacionadas con la privacidad y la seguridad de la información, especialmente aquellas que afectan a la industria en la que trabaja. | 7 | 5 | 0 | 0 | 0 |
| Habilidades de comunicación: Poder comunicar de manera efectiva los riesgos de seguridad y las medidas necesarias tanto a colegas técnicos como a personal no técnico dentro de la organización. | 6 | 6 | 0 | 0 | 0 |

| | | | | | |
|---|---|---|---|---|---|
| Habilidades de gestión de proyectos: Ser capaz de planificar, ejecutar y controlar proyectos de seguridad informática, asegurando que se cumplan los plazos y objetivos establecidos. | 8 | 4 | 0 | 0 | 0 |
| Habilidades de investigación: Estar dispuesto y ser capaz de mantenerse actualizado sobre las últimas amenazas y tendencias en seguridad informática, así como investigar nuevas tecnologías y soluciones de seguridad. | 8 | 4 | 0 | 0 | 0 |
| Ética profesional: Mantener altos estándares éticos y actuar de manera responsable en el manejo de la información confidencial y en la ejecución de tareas de seguridad informática. | 10 | 2 | 0 | 0 | 0 |
| Capacidad para adaptarse y aprender: Dado que el campo de la seguridad informática está en constante evolución, es crucial tener la capacidad de adaptarse rápidamente a nuevos desafíos y aprender nuevas habilidades y técnicas según sea necesario. | 7 | 5 | 0 | 0 | 0 |

Fuente: Elaboración Propia 2024.

El análisis técnico centrado en la evaluación de la importancia de las competencias y habilidades que deben considerarse al formular un plan de estudios para el programa de posgrado en seguridad informática destaca las siguientes áreas, junto con el nivel de importancia asignado a cada una:

- ✓ Conocimiento Técnico Profundo: Considerado esencial para entender sistemas operativos, redes, protocolos de comunicación y tecnologías de seguridad. La evaluación muestra que es altamente importante, con 7 votos para "Muy Alta" y 5 para "Alta".
- ✓ Análisis de Riesgos: La capacidad de evaluar y analizar riesgos de seguridad es crucial, con 9 votos para "Muy Alta" y 3 para "Alta".
- ✓ Gestión de Incidentes: Esta habilidad se destacó como fundamental, con 10 votos para "Muy Alta" y 2 para "Alta", indicando una necesidad crítica de saber cómo responder a incidentes de seguridad.
- ✓ Penetration Testing: Con 9 votos para "Muy Alta" y 3 para "Alta", es vital conocer y aplicar técnicas de hacking ético para identificar y corregir debilidades en sistemas y redes.
- ✓ Conciencia de la Legislación y Regulaciones: Estar al tanto de las leyes y regulaciones es importante, con 7 votos para "Muy Alta" y 5 para "Alta".
- ✓ Habilidades de Comunicación: La capacidad de comunicar riesgos y medidas de seguridad es considerada importante, con una distribución equilibrada: 6 votos para "Muy Alta" y 6 para "Alta".
- ✓ Habilidades de Gestión de Proyectos: Evaluada como altamente importante, con 8 votos para "Muy Alta" y 4 para "Alta".
- ✓ Habilidades de Investigación: Mantenerse actualizado sobre amenazas y tendencias es importante, con 8 votos para "Muy Alta" y 4 para "Alta".

- ✓ Ética Profesional: Esta competencia es considerada crítica, con 10 votos para "Muy Alta" y 2 para "Alta".
- ✓ Capacidad para Adaptarse y Aprender: La adaptabilidad y el aprendizaje continuo son cruciales, con 7 votos para "Muy Alta" y 5 para "Alta".

Con los datos anteriores se puede recomendar que, al momento de formular el plan de estudios para el programa de posgrado en seguridad informática, se tenga en cuenta las siguientes áreas y competencias mencionadas:

- ✓ Priorizar la Gestión de Incidentes y la Ética Profesional: Ambas áreas recibieron la mayor cantidad de votos en la categoría "Muy Alta". Esto sugiere que el programa debe incluir módulos extensivos y detallados sobre la gestión de incidentes de seguridad y la ética profesional en el campo.
- ✓ Incluir Formación en Análisis de Riesgos y Penetration Testing: Estas competencias también son altamente valoradas y deben ser componentes fundamentales del plan de estudios. Se debe asegurar que los estudiantes adquieran habilidades prácticas en evaluación de riesgos y técnicas de pruebas de penetración.
- ✓ Desarrollar un Conocimiento Técnico Sólido: Es crucial que los estudiantes comprendan profundamente los sistemas operativos, redes, y tecnologías de seguridad, aunque esto deberían tenerlo desde el pregrado.
- ✓ Asegurar Conocimiento de Legislación y Regulaciones: Dado el alto nivel de importancia asignado, el programa debe incluir cursos que cubran las leyes y regulaciones relevantes en seguridad informática, con énfasis en la aplicación práctica en diferentes empresas.

- ✓ Fortalecer las Habilidades de Comunicación y Gestión de Proyectos: Para preparar a los estudiantes para roles de liderazgo, el programa debe incluir capacitación en comunicación efectiva y gestión de proyectos, permitiendo que los graduados puedan dirigir equipos y proyectos de seguridad informática.
- ✓ Fomentar la Investigación y el Aprendizaje Continuo: La seguridad informática es un campo en constante evolución. El plan de estudios debe incluir actividades y proyectos de investigación, además de fomentar una cultura de aprendizaje continuo para mantenerse al día con las nuevas amenazas y tecnologías, y en este aspecto es indispensable que se apliquen resultados de aprendizaje mediante el modelo pedagógico acogido por el ITP que es constructivista.
- ✓ Adaptabilidad: El programa debe desarrollar la capacidad de los estudiantes para adaptarse a nuevos desafíos y aprender nuevas habilidades.

Para finalizar algunos empresarios mencionaron otras habilidades, áreas o componentes que consideran necesarias para la formación del profesional especializado, entre ellas: Ciberseguridad, forense digital, seguridad en redes de dispositivos móviles, IoT y sistemas embebidos. Arquitectura de seguridad en el desarrollo de software, conocimiento profundo en el despliegue y seguridad de infraestructura tecnológica y seguridad en la nube.

***Análisis Nivel de Empleabilidad de los Egresados***

Finalmente, y con el objetivo de determinar la pertinencia para la apertura del programa de posgrado en Seguridad Informática en el Instituto Tecnológico del Putumayo, fue necesario realizar un análisis del nivel de empleabilidad de los egresados

en el área. Para ello, se realizó una exploración documental de algunas Instituciones de Educación Superior en Colombia, que ofertan la Especialización en Seguridad Informática, sin embargo, no se encontró, al menos de manera oficial, documentos con algún tipo de estudio estadístico respecto a la empleabilidad de sus egresados.

Las Instituciones de Educación Superior tenidas en cuenta fueron: Universidad Piloto de Colombia, Institución Universitaria ITM, Politécnico Grancolombiano Institución Universitaria, Colegio Oficial Ingenieros de Telecomunicación, Universidad Católica de Colombia, y Universidad Politécnica de Cartagena.

Ante esta situación se recurre al sistema de información de consulta pública como lo es el Observatorio Laboral para la Educación del Ministerio de Educación Nacional, y se obtiene los siguientes datos:

- ✓ Tasa de Cotizantes - Recién graduados entre el año 2020 - Vinculados en el año 2021

***Tabla 10.*** Tasa de Cotizantes.

Graduados en el año 2020 - Vinculados en el año 2021

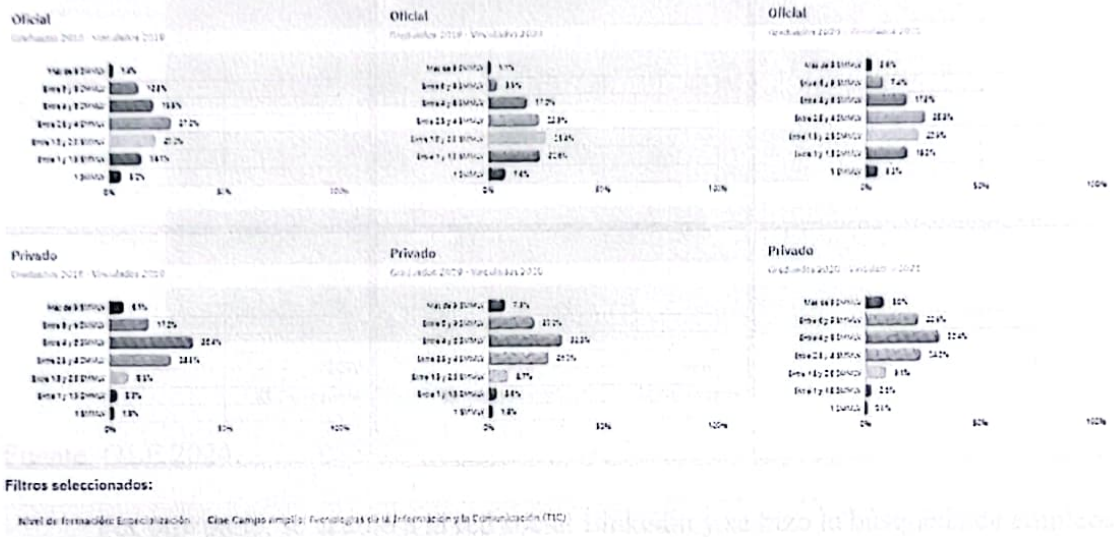
| Total | Tasa de cotizantes | Sector oficial | Sector privado | Pregrado | Posgrado | Masculino | Femenino |
|---|---|---|---|---|---|---|---|
| 426.735 | 75,1% | 69,3% | 79,1% | 70,3% | 90,2% | 76,1% | 74,4% |
| 320.599 | 4,6% | 6,0% | 3,4% | 4,6% | 1,7% | 4,5% | 4,8% |
| | | 120.257 | 200.342 | 226.668 | 93.931 | 158.162 | 162.417 |

Fuente: OLE 2024.

En el nivel de posgrado un total de 93.931 cotizantes en su mayoría en el sector privado. Además, con base en el Ingreso Base de Cotización de los Recién graduados, en el nivel de formación Especialización en el campo CINE Tecnologías de la Información y la Comunicación TIC, que es donde se encuentra el posgrado en seguridad informática, se encuentra, durante los años 2019, 2020 y 2021, el registro de ingresos promedios de

entre 2.5 a 6 salarios mínimos, con mayor presencia de profesionales especializados en el sector privado, lo que supone un dato favorable para los profesionales que desean realizar una especialización y tener vinculación laboral.

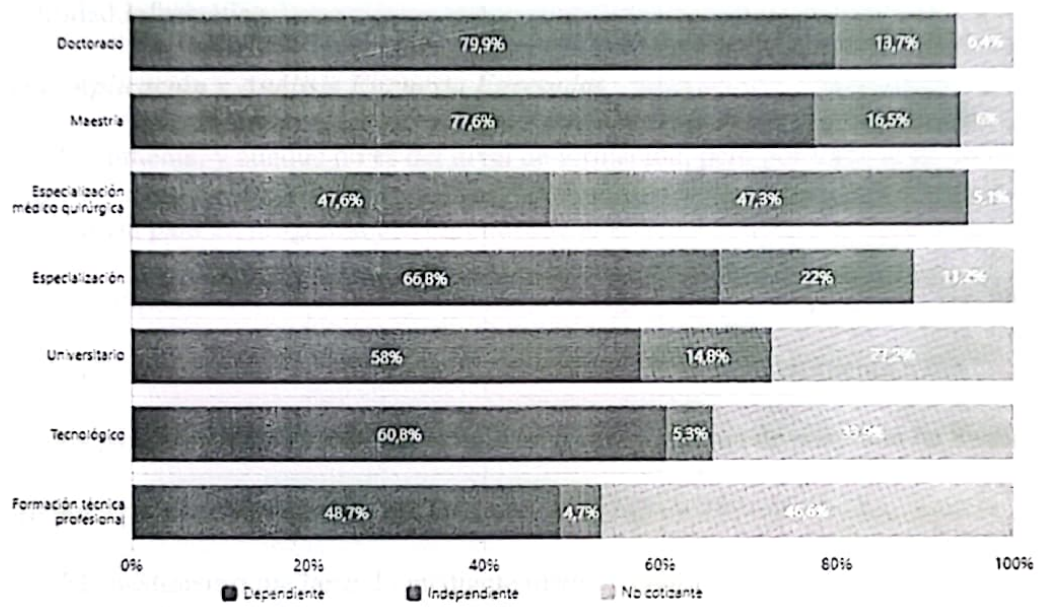
***Figura 4.*** Ingreso base años 2019-2021.




Fuente: OLE 2024.

Ahora bien, como se evidencia en la ilustración siguiente existe un número bastante alto de cotizantes dependientes en el nivel académico de especialización, lo que significa que están empleados en el sector productivo. Estos datos generan confianza para las personas que desean especializarse, sabiendo que el esfuerzo puede ser compensado en el campo laboral.

***Figura 5.*** Graduados Según Tipo de Cotizante y Nivel de Formación.




Fuente. OLE 2024.

Por otra parte, se acudió a la red social Linkedin y se hizo la búsqueda de empleos para profesionales en seguridad informática del cual se obtuvo un total de 226 empleos de Seguridad Informática en Colombia, en empresas como: Coomeva Valle del cauca Magneto Valle del cauca, Fenal Colombia Santander, Impadoc SAS Valle del cauca, Advanced Fertility Center of Texas Bogotá, Pepe Ganga Bogotá, Domina Entrega Total SAS Medellín, entre otras. De las cuales 112 empresas requieren que la vinculación sea presencial, 61 remoto y 53 vinculación híbrida, con un nivel de experiencia: sin experiencia 41 solicitudes, nivel intermedio 85 y algo de responsabilidad 34, entre otros casos.

En la bolsa de empleo virtual Computrabajo también se realizó la consulta y se obtuvieron resultados similares, con 64 ofertas en el último mes (mayo 2024), con

salarios de entre 3 a 8 millones de pesos para profesionales especializados en el campo de la seguridad informática.

***Diseño, Aplicación y Análisis Encuesta Egresados***

Finalmente, y aunque no es del nivel de formación, pero por tratarse de un estudio de pertinencia para un programa correspondiente al área del conocimiento de la ingeniería, arquitectura, urbanismo y afines, que es igual al área del programa vigente que tiene el ITP, denominado Ingeniería de Sistemas del ITP, se tuvo en cuenta a sus egresados para preguntarles sobre la viabilidad de un programa de posgrado en Seguridad Informática para ser ofertado por el ITP.

El cuestionario fue lanzado mediante medio tecnológico usando el grupo de WhatsApp de egresados del programa de Ingeniería de Sistemas bajo el liderazgo de la Dirección del Programa. La recolección se hizo usando el formulario de google, mediante el link https://forms.gle/wbwUxaA4nr9kApfQ6

El formulario permaneció activo 24 horas, tiempo que se consideró suficiente por la efectividad del medio de difusión.

A continuación, se presentan los resultados de un total de 50 egresados que respondieron: en su mayoría los encuestados fueron hombres (74%) residentes en la ciudad de Mocoa (80%), quienes egresados en promedio entre 3 a 4 años (84%) de ambos programas que ofrece el ITP, tecnología en desarrollo de software e ingeniería de sistemas. A los egresados se les realizó además algunas preguntas enfocadas en conocer el nivel de importancia que le dan a aspectos sobre el objeto de estudios, se les pidió

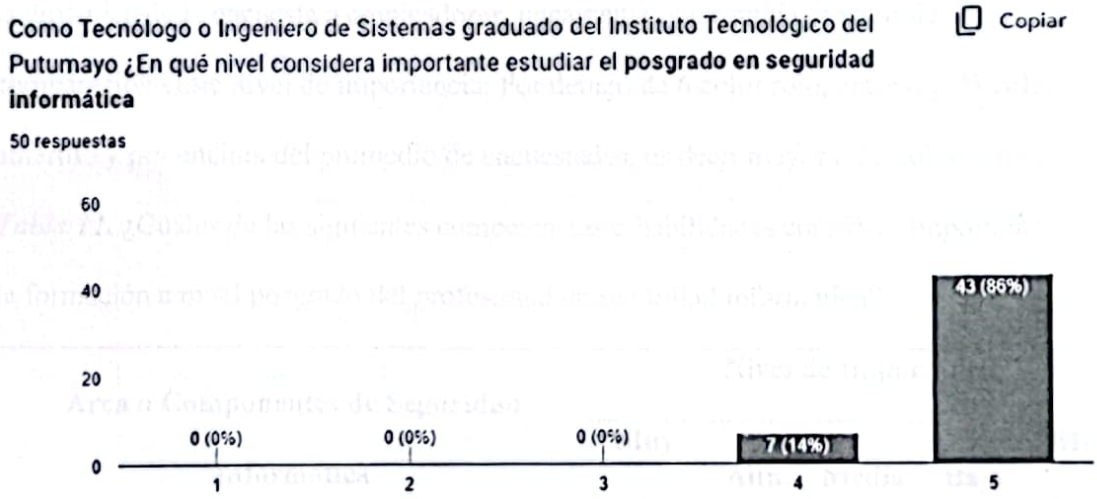
calificar de 1 a 5 el nivel de importancia, donde 1 es muy baja importancia, 2 bajo, 3 medio, 4 alto, 5 muy alta importancia.

Cabe mencionar que el total de los resultados de la encuesta se encuentran como documentos anexos a este documento.

Documentos anexos:

- **Anexo 2.** Tabulación Encuesta Egresados.

***Figura 6.*** ¿Cómo Ingeniero de Sistemas graduado del Instituto Tecnológico del Putumayo ¿en qué nivel considera importante estudiar el posgrado en seguridad informática?




Fuente: Elaboración Propia 2024.

Se evidencia el alto nivel de importancia que existe al considerar el posgrado en seguridad informática como un tema de interés, el cual tiene como preferencia (64%) la modalidad presencial "fines de semana", aunque el 36% prefiere la modalidad virtual, aspecto que la institución deberá tener en cuenta para formular un plan de estudios con estrategias pedagógicas que incluyan en alto porcentaje la virtualidad. Cuando se les

preguntó sobre si recomendarían a un egresado a un particular con un título de pregrado estudiar el posgrado en seguridad informática el 98% respondió que sí, lo que corrobora el interés de la formación y el sentido de pertenencia para la institución.

Aunque los egresados consideran que el valor a pagar por semestre del posgrado sería de 1.5 salarios mínimos (74%), será la institución quien realice el estudio financiero para establecer el valor de matrícula el programa.

A continuación, se realiza el análisis sobre la pregunta de cuáles áreas o componentes se consideran importantes en la formación de un profesional especializado en seguridad informática y al final se realiza una conclusión general. Se realizó siguiendo la dinámica de la encuesta a empleadores, úncamente que cambia el valor de comparación entre nivel de importancia: Por debajo de 6 color rojo, entre 6 y 25 color amarillo y por encima del promedio de encuestados, es decir mayor a 25 color verde.

***Tabla 11.*** ¿Cuáles de las siguientes competencias o habilidades considera importantes en la formación a nivel posgrado del profesional en seguridad informática?

| **Área o Componentes de Seguridad Informática** | **Nivel de Importancia** | | | | |
|---|---|---|---|---|---|
| | **Muy Alta** | **Alta** | **Media** | **Baja** | **Muy Baja** |
| Conocimiento técnico profundo: Entender los sistemas operativos, redes, protocolos de comunicación y tecnologías de seguridad es fundamental para identificar | 33 | 15 | 1 | 0 | 1 |

| | | | | | |
|---|---|---|---|---|---|
| vulnerabilidades y aplicar soluciones adecuadas. | | | | | |
| Análisis de riesgos: Ser capaz de evaluar y analizar los riesgos de seguridad de una organización, sus activos y las posibles amenazas que enfrenta. | 32 | 16 | 1 | 0 | 1 |
| Gestión de incidentes: Saber cómo responder eficazmente a incidentes de seguridad, desde la detección hasta la contención y la recuperación. | 33 | 15 | 1 | 0 | 1 |
| Penetration testing (pruebas de penetración): Conocer y aplicar técnicas de hacking ético para identificar y corregir debilidades en sistemas y redes antes de que puedan ser explotadas por atacantes reales. | 38 | 10 | 1 | 0 | 1 |
| Conciencia de la legislación y regulaciones: Estar al tanto de las leyes y regulaciones relacionadas con la privacidad y la seguridad de la información, especialmente aquellas que afectan a la industria en la que trabaja. | 31 | 14 | 4 | 0 | 1 |
| Habilidades de comunicación: | 23 | 21 | 5 | 0 | 1 |

| | | | | | |
|---|---|---|---|---|---|
| Poder comunicar de manera efectiva los riesgos de seguridad y las medidas necesarias tanto a colegas técnicos como a personal no técnico dentro de la organización. | | | | | |
| Habilidades de gestión de proyectos: Ser capaz de planificar, ejecutar y controlar proyectos de seguridad informática, asegurando que se cumplan los plazos y objetivos establecidos. | 30 | 14 | 5 | 0 | 1 |
| Habilidades de investigación: Estar dispuesto y ser capaz de mantenerse actualizado sobre las últimas amenazas y tendencias en seguridad informática, así como investigar nuevas tecnologías y soluciones de seguridad. | 29 | 17 | 3 | 0 | 1 |
| Ética profesional: Mantener altos estándares éticos y actuar de manera responsable en el manejo de la información confidencial y en la ejecución de tareas de seguridad informática. | 24 | 18 | 7 | 0 | 1 |
| Capacidad para adaptarse y aprender: | 31 | 15 | 2 | 1 | 1 |

| |
|---|
| Dado que el campo de la seguridad informática está en constante evolución, es crucial tener la capacidad de adaptarse rápidamente a nuevos desafíos y aprender nuevas habilidades y técnicas según sea necesario. |

Fuente: Elaboración Propia 2024.

Con base en los datos obtenidos se puede determinar la importancia de las competencias y habilidades consideradas necesarias para la formación de profesionales en seguridad informática a nivel de posgrado. Los datos reflejan las opiniones de los encuestados respecto al nivel de importancia de cada área o componente, clasificado en una escala de "Muy Alta" a "Muy Baja".

- ✓ Conocimiento Técnico Profundo: Este componente es esencial para identificar vulnerabilidades y aplicar soluciones adecuadas, con 33 votos para "Muy Alta", 15 para "Alta", 1 para "Media" y 1 para "Muy Baja".
- ✓ Análisis de Riesgos: La habilidad de evaluar y analizar los riesgos de seguridad es crucial, con 32 votos para "Muy Alta", 16 para "Alta", 1 para "Media" y 1 para "Muy Baja".
- ✓ Gestión de Incidentes: Considerado altamente importante para la respuesta eficaz a incidentes de seguridad, con 33 votos para "Muy Alta", 15 para "Alta", 1 para "Media" y 1 para "Muy Baja".

- ✓ Penetration Testing: Este componente se destaca como extremadamente importante, con 38 votos para "Muy Alta", 10 para "Alta", 1 para "Media" y 1 para "Muy Baja".
- ✓ Conciencia de la Legislación y Regulaciones: Importante para entender las leyes y regulaciones en seguridad de la información, con 31 votos para "Muy Alta", 14 para "Alta", 4 para "Media" y 1 para "Muy Baja".
- ✓ Habilidades de Comunicación: La capacidad de comunicar riesgos y medidas de seguridad es valorada con 23 votos para "Muy Alta", 21 para "Alta", 5 para "Media" y 1 para "Muy Baja".
- ✓ Habilidades de Gestión de Proyectos: Evaluada como importante, con 30 votos para "Muy Alta", 14 para "Alta", 5 para "Media" y 1 para "Muy Baja".
- ✓ Habilidades de Investigación: La disposición para mantenerse actualizado y la habilidad de investigar nuevas amenazas y soluciones es importante, con 29 votos para "Muy Alta", 17 para "Alta", 3 para "Media" y 1 para "Muy Baja".
- ✓ Ética Profesional: Considerada crucial, con 24 votos para "Muy Alta", 18 para "Alta", 7 para "Media" y 1 para "Muy Baja".
- ✓ Capacidad para Adaptarse y Aprender: Enfatiza la importancia de la adaptabilidad y el aprendizaje continuo, con 31 votos para "Muy Alta", 15 para "Alta", 2 para "Media", 1 para "Baja" y 1 para "Muy Baja".

Si el ITP decide tener en cuenta lo anterior se recomienda incorporar componentes fundamentales en el plan de estudios, tenientes al conocimiento técnico profundo y gestión

de incidentes, dado que ambos recibieron la mayoría de los votos en la categoría "Muy Alta". También el componente de penetration testing, análisis de riesgos.

No se puede dejar a un lado el incluir legislación y regulaciones pues los estudiantes deben estar bien informados sobre las leyes y regulaciones relevantes en seguridad de la información, con un enfoque en la aplicación práctica en diversas empresas tanto públicas como privadas.

Como parte de la formación integral se debe desarrollar habilidades de comunicación: Dada la importancia de la comunicación efectiva, el plan de estudios debe procurar aspectos que mejoren la capacidad de los estudiantes para comunicar riesgos y soluciones de seguridad tanto a colegas técnicos como a personal no técnico; además fomentar la gestión de proyectos y las habilidades investigativas para poder adaptarse, como por ejemplo en la implementación de medidas de seguridad.

Finalmente, los egresados mencionan otras habilidades, áreas o componentes que se consideran necesarias para la formación del profesional, que sean de ayuda al departamento del Putumayo y el país: "Considero que para el posgrado en seguridad informática se debe tener en cuenta la parte forense muy importante para realizar análisis de rastreos y otros. Ante un mundo cambiante y dinámico en el área, es fundamental ofrecer especializaciones que sean a lugar con estos cambios y sobre todo ante las miles de amenazas que día a día surgen en este campo, por ello para mí es de mayor importancia ofrecer el posgrado que el pregrado a corto tiempo."

Todos estos aspectos analizados serán tenidos en cuenta para plantear una propuesta de plan de estudios ajustado a los lineamientos curriculares del ITP y que será

entregado como anexo a este documento, sin embargo, se resume en los siguientes aspectos:

Documentos anexos:

- **Anexo 3.** Propuesta Plan de Estudios Posgrado en Seguridad Informática.

***Tabla 12.*** Propuesta de unidades de formación y su descripción para el programa especialización profesional en seguridad informática.

| **Semestre 1** | | |
|---|---|---|
| **Unidad de Formación** | **Descripción** | **Créditos** |
| Fundamentos de Seguridad Informática | Conceptos básicos y avanzados de seguridad informática, incluyendo principios y prácticas esenciales. | 2 |
| Análisis y Gestión de Riesgos | Métodos y técnicas para identificar, evaluar y gestionar riesgos de seguridad. | 2 |
| Legislación y Normativas en Seguridad Informática | Estudio de leyes y regulaciones relevantes en el ámbito de la ciberseguridad. | 2 |
| Pruebas de Penetración y Hacking Ético | Técnicas y herramientas para realizar pruebas de penetración y evaluaciones de seguridad. | 3 |
| Ética y Profesionalismo en Seguridad Informática | Exploración de dilemas éticos y desarrollo de una conducta profesional en el campo de la seguridad. | 2 |
| Electiva Profundización 1 | | 1 |
| | **Total** | **12** |

**Semestre 2**

| Unidad de Formación | Descripción | Créditos |
|---|---|---|
| Respuestas y Gestión de Incidentes | Estrategias y tácticas para responder y gestionar incidentes de seguridad. | 2 |
| Seguridad en Redes y Sistemas | Protección y defensa de redes y sistemas contra amenazas cibernéticas. | 2 |
| Criptografía Aplicada | Principios y aplicaciones de criptografía en la protección de datos. | 2 |
| Seguridad en Aplicaciones y Desarrollo Seguro | Prácticas y técnicas para desarrollar aplicaciones seguras y proteger el software contra vulnerabilidades. | 3 |
| Investigación en Ciberseguridad | Metodologías de investigación y análisis de las últimas tendencias y amenazas en ciberseguridad. | 2 |
| Electiva Profundización 2 | | 1 |
| | **Total** | **12** |

Con base en los lineamientos curriculares del ITP se requiere incluir los componentes de líneas de profundización "electivas" y el requisito de inglés B1 (4 Créditos).

## Conclusiones

En Colombia la alta demanda y escasez de profesionales especializados ante la creciente transformación digital permite evidenciar la necesidad de profesionales en seguridad informática. A nivel Putumayo y teniendo en cuenta la cantidad de egresados encuestados y que están interesados en el posgrado podría ser insuficiente medida para concluir que efectivamente se requiere de esta especialización, lo que sí es claro, es que existe una brecha significativa en el mercado laboral ante la escasez de profesionales capacitados, lo cual es una preocupación alta para las empresas, de ahí que un programa de posgrado con modalidad virtual y con un valor de matrícula bajo, podría ser la mejor opción para captar estudiantes desde todo el País.

El plan de estudios del programa debe tener en cuenta las competencias en áreas como conocimiento técnico profundo, análisis de riesgos, gestión de incidentes y pruebas de penetración, las cuales son consideradas altamente importantes, y siendo las pertinentes para un programa de posgrado ofertado por el ITP.

Ante eventos como la pandemia, las empresas y las personas hicieron más uso de las tecnologías, lo que en consecuencia aumentó los ciberataques, de ahí que se resalta la necesidad urgente de fortalecer las defensas cibernéticas. En Colombia, por ejemplo, los ciberataques han aumentado significativamente, posicionando al país como uno de los más afectados en Latinoamérica. Esto exige una mejor preparación en educación y capacitación en ciberseguridad, el Instituto Tecnológico del Putumayo con la oferta de este posgrado, desde el sur de Colombia, podría hacer la diferencia.

El programa de especialización profesional en seguridad informática es pertinente académica y estratégicamente para que el Instituto Tecnológico del Putumayo ayude a

cerrar la brecha que existe en Colombia de personal capacitado en el área, procurando evitar ciberataques, salvaguardando la información valiosa para las personas y empresas; dando la oportunidad a egresados del programa ingeniería de sistemas del ITP y demás profesionales interesados, de poder cursar un posgrado en su territorio.

Se evidencia la pertinencia y necesidad de un programa de posgrado en seguridad informática, alineado con las demandas del mercado y las necesidades específicas de protección de datos y sistemas en un entorno digital en constante evolución. El plan de estudios presentado es el resultado de los análisis realizados y es una guía indispensable para la institución.

## Recomendaciones

Aunque los egresados prefieren la modalidad presencial los fines de semana para el programa de posgrado, los autores recomiendas que el plan de estudios tenga en cuenta el uso de la modalidad virtual, dado que el programa de posgrado es llamativo a muchos profesionales que tal vez no vivan en la ciudad de Mocoa.

El plan de estudios entregado es una guía basada en los análisis propios del desarrollo del proyecto, se recomienda que un experto la pueda validar y con ello establecer unos criterios más centrados en las necesidades de la región, ya que para el desarrollo de este documento no fue posible contar con información valiosa como el plan de desarrollo departamental, aspecto que fue mencionado anteriormente.

La institución debe adelantar un estudio financiero para determinar la viabilidad de establecer un valor de matrícula acorde a las condiciones económica de la región.

## Limitaciones

Para la fecha de la realización del proyecto no fue posible tener acceso a los planes regionales y locales respecto a las necesidades laborales; dado que estos se encontraban en discusión en mesas de trabajo.

## Referencias

Alcaldía de Mocoa . (2021). *Plan Estratégico de Tecnologías de la Información 2021-2024*. Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mocoa-putumayo.gov.co/Transparencia/PlaneacionGestionyControl/PLAN%20TIC%20MOCOA%202021%20-%202024.pdf

Asociación Colombiana de Informática Sistemas y Tecnologías Afines. (2022). *Crece la demanda de profesionales especializados en seguridad informática en Colombia.* Obtenido de https://www.acis.org.co/portal/content/crece-la-demanda-de-profesionales-especializados-en-seguridad-inform%C3%A1tica-en-colombia

Banco Mundial. (04 de abril de 2024). *Desarrollo digital*. Obtenido de ¿Qué se necesitará para que los países cosechen los beneficios de la digitalización y participen de lleno en la economía digital mundial?: https://www.bancomundial.org/es/topic/digitaldevelopment/overview

Bit Life media . (2024). *Así está enfrentando la UE la escasez de expertos en tecnología y ciberseguridad (y qué planes hay de futuro)*. Obtenido de La situación de futuro: https://bitlifemedia.com/2024/02/ue-escasez-expertos-tecnologia-ciberseguridad-planes-futuro/

Cable News Network CNN. (30 de mayo de 2021). *Se busca: millones de expertos en ciberseguridad. Salario: lo que pidas*. Obtenido de https://cnnespanol.cnn.com/2021/05/30/se-busca-millones-expertos-ciberseguridad-salario-trax/

Cámara de Comercio, Industria, Servicios y Navegación de Bilbao. (31 de enero de 2024). *La demanda de expertos en ciberseguridad para este 2024 duplicará al número de especialistas*. Obtenido de https://formacion.camarabilbao.com/blog/crece-demanda-profesionales-expertos-ciberseguridad-202401311519/

Caracol Radio . (30 de mayo de 2023). *Los cinco grandes retos para fortalecer la ciberseguridad en Colombia*. Obtenido de Capacitación en las compañías: https://caracol.com.co/2023/05/30/los-cinco-grandes-retos-para-fortalecer-la-ciberseguridad-en-colombia/

Colnodo. (15 de marzo de 2023). *Comunidades en Putumayo comienzan a navegar por internet seguros: Escuela de Seguridad Digital brinda herramientas para protegerse en línea.* Obtenido de https://www.colnodo.apc.org/es/experiencias/comunidades-en-putumayo-comienzan-a-navegar-por-internet-seguros-escuela-de-seguridad-digital-brinda-herramientas-para

Consejo Privado de Competitividad. (2023). *Informe Nacional de Competitividad 2023-2024.* Obtenido de Adopción Tecnológica: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://compite.com.co/wp-content/uploads/2023/11/CPC_INC_MERCADO-LABORAL_DOBLE.pdf

Corporación Universitaria Americana . (2020). *Especialización en Seguridad Informática*. Obtenido de https://americana.edu.co/barranquilla/especializacion-en-seguridad-informatica/

Corporación Universitaria Americana. (2021). *4 razones para especializarse en Seguridad Informática*. Obtenido de Mayor demanda laboral: https://americana.edu.co/barranquilla/4-razones-para-especializarse-en-seguridad-informatica/

Corporación Universitaria Americana. (2021). *4 razones para especializarse en Seguridad Informática*. Obtenido de Mayor demanda laboral: https://americana.edu.co/barranquilla/4-razones-para-especializarse-en-seguridad-informatica/#:~:text=La%20seguridad%20inform%C3%A1tica%20es%20esencial,de%20los%20ataques%20cibern%C3%A9ticos%20malintencionados.

Corporación Universitaria Minuto de Dios UNIMINUTO. (2022). *Especialización en Seguridad Informática*. Obtenido de Presentación del programa : https://www.uniminuto.edu/oferta-academica/especializacion-en-seguridad-informatica/especializacion-en-seguridad-informatica

European Business School ceupe. (2020). *4 razones para estudiar un Máster en Seguridad de la Información y Tecnología*. Obtenido de 4 Motivos para estudiar un Máster en Seguridad de la Información: https://www.ceupe.com/blog/razones-para-estudiar-un-master-en-seguridad-de-la-informacion-tecnologia.html

FayerWayer. (15 de octubre de 2022). *Ciberseguridad en América Latina: Al alza la demanda de especialistas pero la oferta no se pone al día*. Obtenido de La demanda laboral en seguridad cibernética aún supera la oferta en un contexto donde los ciberataques y el trabajo remoto han hecho indispensable proteger la información: https://www.fayerwayer.com/internet/2022/10/15/ciberseguridad-

en-america-latina-al-alza-la-demanda-de-especialistas-pero-la-oferta-no-se-pone-al-dia/

Fundación Universitaria Internacional de la Rioja. (2024). *Especialización en Seguridad Informática*. Obtenido de https://unir.edu.co/especializaciones/especializacion-seguridad-informatica/#pensum

Fundamentación Universitaria Compensar. (2021). *Especialización en Seguridad Informática*. Obtenido de https://ucompensar.edu.co/programas/especializacion-en-seguridad-informatica/

IBERO. (4 de abril de 2024). *Importancia de la seguridad informática como campo de estudio en ingeniería de software*. Obtenido de La seguridad informática como campo de estudio en ingeniería de software: https://www.ibero.edu.co/blog/articulos/importancia-de-la-seguridad-informatica-como-campo-de-estudio-en-ingenieria-de-software

Information Technology . (2022). *10 reconocidas instituciones de Colombia hackeadas en el 2022*. Obtenido de Ataques cibernéticos a empresas respecto al año anterior: https://nsit.com.co/10-reconocidas-instituciones-de-colombia-hackeadas-en-el-2022/

La República. (22 de enero de 2022). *Los retos de ciberseguridad a los que tendrán que enfrentar las compañías en 2022*. Obtenido de https://www.larepublica.co/internet-economy/los-retos-de-ciberseguridad-a-los-que-tendran-que-enfrentar-las-companias-en-2022-3290319

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) . (15 de abril de 2021). *MinTIC expide la resolución que establece los lineamientos y estándares para la estrategia de seguridad digital.* Obtenido de https://gobiernodigital.mintic.gov.co/portal/Noticias/162625:MinTIC-expide-la-resolucion-que-establece-los-lineamientos-y-estandares-para-la-estrategia-de-seguridad-digital

MinTIC. (04 de diciembre de 2023). *MinTIC y Bios inician formación en ciberseguridad con cifra récord de inscritos*. Obtenido de La formación, que busca robustecer la capacidad del país para la defensa digital, inició la semana pasada: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/327078:MinTIC-y-Bios-inician-formacion-en-ciberseguridad-con-cifra-record-de-inscritos

Organización de las Naciones Unidas . (2 de junio de 2023). *IA: La regulación es esencial para frenar la vigilancia y la desinformación, aseguran expertos.* Obtenido de Deben trazarse líneas rojas urgentemente: https://news.un.org/es/story/2023/06/1521657

Politécnico Grancolombiano POLI. (07 de noviembre de 2023). *¿Vale la pena especializarse en Seguridad de la Información?* Obtenido de Protegerás el futuro : https://www.poli.edu.co/blog/poliverso/especializaci%C3%B3n-en-ciberseguridad-o-seguridad-de-la-informacion

Revista BYTE. (2024). Los retos de la ciberseguridad para las empresas españolas. *Revista BYTE*, 1.

Revista Estrategia y Negocios . (2021). Crece la demanda de profesionales en seguridad informática. *Revista Estrategia y Negocios* , 1.

Universidad Católica de Colombia. (2019). *Especialización en Seguridad de la Información*. Obtenido de https://www.ucatolica.edu.co/portal/Especializaci%C3%B3n/especializacion-en-seguridad-de-la-informacion/

Universidad Cooperativa de Colombia. (2021). *Especialización en Seguridad de la Información*. Obtenido de https://ucc.edu.co/programas/posgrados/Paginas/monteria/especializacion-en-seguridad-para-la-Informacion-monteria.aspx

Universidad Galileo. (2024). *Experto en ciberseguridad: Una profesión con alta demanda en la industria, según reportes*. Obtenido de https://www.galileo.edu/fisicc/historias-de-exito/experto-en-ciberseguridad-una-profesion-con-alta-demanda-en-la-industria-segun-reportes/

Universidad Iberoamericana de México. (2019). *Especialidad en Seguridad de la Información* . Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ibero.mx/sites/default/files/especialidad-en-seguridad-de-la-informacion2.pdf

Universidad Nacional Abierta y a Distancia. (2018). *Especialización en Seguridad Informática*. Obtenido de https://estudios.unad.edu.co/plan-de-estudios-especializacion-en-seguridad-informatica

Universidad Piloto de Colombia . (2013). *Especialización en Seguridad Informática .* Obtenido de https://www.unipiloto.edu.co/programas/especializaciones/especializacion-en-seguridad-informatica/

Universidad Pontificia Bolivariana . (2017). *Especialización en Seguridad Informática.* Obtenido de https://www.upb.edu.co/es/postgrados/especializacion-seguridad-informatica-medellin

Valor & Dinero. (21 de febrero de 2023). *Éxito en la recuperación de fondos públicos tras ataque cibernético en el Putumayo*. Obtenido de https://valorydinero.com/2023/09/06/exito-en-la-recuperacion-de-fondos-publicos-tras-ataque-cibernetico-en-el-putumayo/

# Anexos

**Anexo 1.** Tabulación Encuesta Empleadores.

**Anexo 2.** Tabulación Encuesta Egresados.

**Anexo 3.** Propuesta Plan de Estudios Especialización en Seguridad Informática.