Línea de Investigación en CIBERSEGURIDAD

Universidad Nacional Abierta y a Distancia
Vicerrectoría de Innovación y Emprendimiento
Escuela de Ciencias Básicas Tecnología e Ingeniería

Universidad Nacional Abierta y a Distancia (UNAD)

Vicerrectoría de Innovación y Emprendimiento - VIEM
Ing. Andrés Ernesto Salinas
Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería - ECBTI
Ing. Claudio Camilo González Clavijo
Decano

Línea de Investigación en:
CIBERSEGURIDAD

Especialización en Seguridad Informática - ESI
Ing. Sonia Ximena Moreno Molano
Líder de Programa
Líder de Cadena de Formación de Sistemas

Grupo de Byte InDesign
María Consuelo Rodríguez - Líder Grupo Byte InDesing
Semillero de Investigación Ceros y Unos

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD
Luis Fernando Zambrano Hernández
Director – Docente Especialización en Seguridad Informática

John Fredy Quintero Tamayo
Analista 1 - Docente Especialización en Seguridad Informática

Hernando Peña Hidalgo
Analista 2 - Docente Especialización en Seguridad Informática

Néstor Raúl Cárdenas
Analista 3 - VIEM

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico**: csirt@unad.edu.co**
Página web: **https://csirt.unad.edu.co**

En el contexto actual de creciente digitalización y la evolución constante de las tecnologías de la información y comunicación, la ciberseguridad se ha convertido en una preocupación fundamental para las organizaciones y los individuos. Siguiendo las directrices del documento de Cibersecurity Curricula 2017[1], es imperativo establecer líneas de investigación en ciberseguridad que permitan desarrollar estrategias de prevención, detección y respuesta ante las múltiples amenazas que se presentan en el entorno digital. La creación de estas líneas de investigación son cruciales para impulsar la formación de profesionales altamente capacitados en la disciplina, así como para fomentar el desarrollo de soluciones innovadoras y eficientes que garanticen la protección de los activos digitales y la integridad de la información.

El Centro de Respuestas a Incidentes Informáticos – CSIRT Académico UNAD, busca aportar en la construcción del conocimiento de la disciplina de la Ciberseguridad articulando su quehacer en términos de respuesta a incidentes y cooperación con proceso de I+D+i, lo cual de como resultado la propuesta de tópicos de investigación que puedan ser abordados en conjunto con la academia.

Este documento está dirigido a escuelas, programas, grupos de investigación, semilleros y en general a toda la plataforma UNADISTA y a sus partes interesadas, para que, desde la disciplina de la Ciberseguridad y a través de espacios de educación y de I+D+i se aporte a la construcción de nuevo conocimiento en áreas específicas de la ciberseguridad.

[1] https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Contenido

Introducción

La era digital actual, caracterizada por la rápida evolución de las tecnologías de la información y comunicación, ha transformado la forma en que la sociedad se comunica. Sin embargo, este entorno digital interconectado también ha dado lugar a un aumento de amenazas y riesgos cibernéticos, lo que ha llevado a la Ciberseguridad a ser una prioridad fundamental para las organizaciones, gobiernos, la educación y los individuos. En este contexto, la creación de líneas de investigación en Ciberseguridad es de suma importancia, ya que permite a través de la generación de nuevo conocimiento enfrentar los desafíos emergentes y garantizar la protección y resiliencia en el ciberespacio.

Dado que la ciberseguridad abarca diversas áreas, como la protección de datos y privacidad, redes y sistemas seguros, inteligencia artificial y machine learning aplicados a la ciberseguridad, criptografía cuántica, seguridad en la nube y dispositivos móviles, y seguridad en sistemas críticos e IoT, es esencial promover la investigación interdisciplinaria y especializada para abordar cada uno de estos campos de manera efectiva. Además, la creación de líneas de investigación en ciberseguridad fomenta la formación de profesionales altamente capacitados y el desarrollo de soluciones innovadoras y eficientes que protejan los activos digitales y la integridad de la información.

Por lo tanto, impulsar la investigación en ciberseguridad no solo contribuye en la prevención, detección y respuesta ante las múltiples amenazas que se presentan en un entorno digital, sino que también a través de procesos de I+D+i facilita la adaptación a las tendencias tecnológicas emergentes y la creación de un entorno seguro y confiable para todos. En así que para el CSIRT Académico UNAD, la investigación en ciberseguridad no solo permitirá estar actualizados en cuanto a tendencias de amenazas y detección de vulnerabilidades a partir de la construcción de bases de datos de conocimiento y de sus lecciones aprendidas, sino que también permitirá contribuir en desarrollar las habilidades y conocimientos necesarios para abordar estas amenazas de manera efectiva con el fin de tomar medidas preventivas.

En este sentido, la necesidad de sustentar el quehacer diario del CSIRT Académico UNAD y el desarrollo de capacidades que apalanque la necesidad de crear herramientas de software, procesos o modelos enfocados en ciberseguridad a través de una línea de investigación, contribuye en la recopilación y análisis de datos de incidentes de seguridad que soportan la generación de métricas que puede proporcionar información valiosa sobre las amenazas y los riesgos. Así mismo contribuye en generar alianzas que conlleven a la colaboración entre otros equipos de investigación en ciberseguridad.

Metodología

El presente documento, se construye aplicando una metodología de investigación cualitativa, el cual utiliza documentos, de orden primario, secundario y de fuentes de información para obtener datos y responder a la pregunta de investigación.

En este orden, la información que es objeto de análisis corresponde a:

- Información internacional que presenten el estado actual y tópicos de investigación y tendencias asociadas con la disciplina de la ciberseguridad
- Información regional y local que presente hacia donde está orientándose la Ciberseguridad en un contexto académico y científico en la región

De esta forma, es como se da respuesta a la propuesta para creación de una línea de investigación que gire en torno a la disciplina de la Ciberseguridad y cómo está puede impactar en los procesos de I+D+i que viene adelantando el Centro de Respuestas a Incidentes informáticos – CSIRT Académico UNAD, la Escuela de Ciencias Básicas Tecnología e Ingeniería – ECBTI y sus programas académicos asociados a la cadena de formación de Sistemas y de ETR.

En este orden de ideas la aplicación de la metodología de investigación de análisis documental se desarrolla a partir de los siguientes capítulos:

Tabla 1: Capítulos y recursos usados para la construcción del documento

Capitulo	Actividad	Recurso usado
I	Reconocimiento	Documento maestro para la construcción del dispositivo CSIRT Académico UNAD (VIEM) Documento maestro programa de Maestría en ciberseguridad Documento maestro programa de Especialización en Seguridad Informática Política
II	Líneas de investigación actuales planteadas por la ECBTI	Líneas de investigación propuestas por las Cadenas de formación de la Escuela de Ciencias Básicas Tecnología e Ingeniería – ECBTI Líneas de investigación de Escuelas de la UNAD que impacten a la disciplina de la Ciberseguridad
III	Propuesta para la creación de la línea de investigación en Ciberseguridad	Análisis de la información recolectada
IV	Características especificas	
V	Fundamentos teóricos y epistemológicos	Bases de datos documentales (Scopus, IEEE)
VI	Contextualización de la línea de investigación	Documentos de proyección y planeación relacionados con la investigación en Ciberseguridad y currículos académicos en: Europa, Asía y América

		Documentos de proyección y planeación relacionados con la investigación en Ciberseguridad en: MINCIENCIAS, Universidades, Sector empresarial y partes interesadas
VII	Objetivos de la línea de investigación	Estatuto de investigación Análisis documental
VIII	Transdisciplinariedad de la línea de investigación en ciberseguridad	Consulta literaria
IX	Metas previstas	Lineamientos de MINCIENCIAS
X	Bibliografía	Recursos consultados

Elaboración propia.

Reconocimiento

Teniendo presente los lineamientos relacionados con Investigación e Innovación, la Universidad Nacional Abierta y a Distancia – UNAD dispone:

Acuerdo 024 del 17 Abril de 2012.	• Por el cual se reglamenta el Estatuto de Investigación UNAD[2] • Capítulo V: DE LAS LINEAS Y PROYECTOS DE INVESTIGACIÓN. Artículo 24
Acuerdo 005 del 19 de Abril de 2016.	• Por el cual se reglamentan las Líneas de Investigación UNAD[3] • Capítulo III: DE LA CONSTRUCCIÓN DE LAS LINEAS DE INVESTIGACIÓN. Artículo 8.
Acuerdo 001 DEL 26 DE ENERO DE 2021[4]	• Por el cual se adopta la Política de Innovación y Emprendimiento de la Universidad Nacional • Capítulo II: DE LA INNOVACIÓN Artículo 11[5].

Para la Universidad Nacional Abierta y a Distancia, el Centro de Respuestas a Incidentes Informáticos –CSIRT Académico UNAD representa el resultado de un trabajo coordinado entre la Escuela de Ciencias Básicas Tecnología e Ingeniería y la Vicerrectoría de Innovación y emprendimiento. Esta unidad desarrolla procesos de I+D+i y soporta la prevención y respuesta ante eventos o incidentes informáticos que puedan afectar el entorno digital UNADISTA. Por esta razón, el CSIRT consciente de su responsabilidad, impacta no solo a la Universidad en términos de ciencia, tecnología e innovación, sino en ser una unidad productiva que ofrece servicios de Ciberseguridad, acompañando a sus aliados estratégicos de los diferentes sectores económicos y partes interesadas, en la búsqueda de capacidades de cooperación y colaboración.

Es preciso indicar que los procesos de I+D+i son una transversal que se desarrolla a partir del liderazgo académico que realiza la ECBTI y del liderazgo Administrativo y Tecnológico que realiza la VIEM. (ver ilustración 1) Y que las acciones generadas en el monitoreo, detección, respuesta y recuperación de eventos o incidentes, contribuyen en la construcción de escenarios propicios para profundizar sobre temas relacionados con nuevas amenazas y tendencias de ciberataques.

En este sentido la propuesta de I+D+i va más allá de del quehacer diario. Para el CSIRT, los procesos académicos en conjunto con las capacidades tecnológicas y la investigación adquieren la relevancia que significa y contribuye en la construcción del conocimiento de esta disciplina teniendo presente:

---

[2] https://investigacion.unad.edu.co/images/investigacion/Acuerdo%20024%20Abril%2017%20de%202012.pdf

[3] https://investigacion.unad.edu.co/images/investigacion/ACUERDO_005_2016_04_19_LINEAS_DE_INVESTIGACIN_1.pdf

[4] https://sgeneral.unad.edu.co/images/documentos/consejoSuperior/acuerdos/2021/COSU_ACUE_001_26012021.pdf

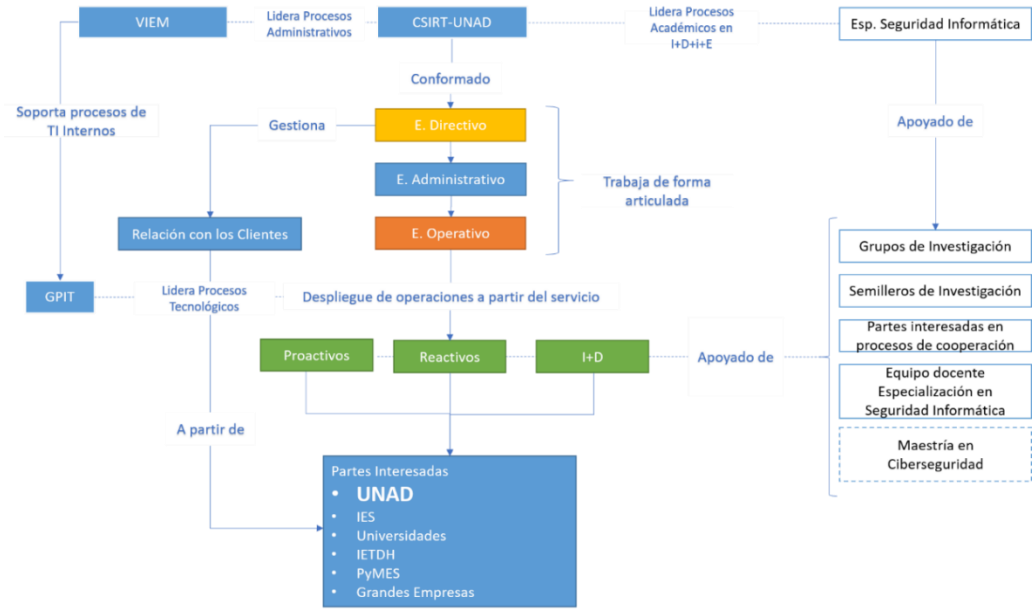
[5] Articulación de Resultados de Investigación e Innovación: Promover y gestionar en articulación son el Sistema de Gestión de la Investigación SIGI las relaciones entre la universidad y el contexto externo (Empresa, Estado, Sociedad) que promuevan el emprendimiento de los resultados derivados de la investigación e innovación

Investigación: Eje articulador para el desarrollo de proyectos de investigación con los programas académicos que estén alienados con esta disciplina (Especialización en Seguridad Informática, Maestría en Ciberseguridad, Ingeniería de Sistemas, Ingeniería en Telecomunicaciones, Ingeniería Electrónica, Tecnología en Desarrollo de Software Etc.), generando productos tales como artículos de investigación, working paper, participación en eventos académicos como simposios, conversatorios, foros, ponencias y patentes que permitan visibilizar los resultados obtenidos.

Innovación: Eje impulsor de procesos de mejora y transformación a partir de la apropiación de entornos digitales seguros. Esto, con el fin de fortalecer el desarrollo de los procesos académicos y administrativos tanto internos como de comunidades objetivo, teniendo presente el desarrollo de estrategias que tengan como propósito el dar como resultado una innovación aplicada que contribuya en identificar las necesidades de partes interesadas contribuyendo en dar claridad y mirada renovada a los procesos del aseguramiento de la información.

Desarrollo: Eje generador de productos o patentes (prototipado o software) que contribuyen en el aseguramiento de entornos digitales tales como: políticas, proceso, procedimientos, software para el análisis de riesgos, metodologías para el aseguramiento de entornos digitales, desarrollo de prototipos de herramientas de seguridad, soportado por la infraestructura tecnológica de CSIRT.

Ilustración 1: Diagrama de operaciones del dispositivo CSIRT Académico UNAD



Recuperado de Documento maestro de consolidación de dispositivo CSIRT Académico UNAD

La figura anterior, presenta el modelo de operación del dispositivo CSIRT Académico UNAD, el cual se apalanca por los siguientes componentes:

Administrativo (VIEM-ECBTI):

Generación de convenios, alianzas y prestación de servicios a partir del despliegue de servicios a partes interesadas o comunidades objetivo como son instituciones de educación superior, PyMEs o entes territoriales

Tecnológico (GPIT-ECBTI):

- Aseguramiento del entorno digital de la Universidad a partir del endurecimiento de su infraestructura de hardware y de software
- Apalancamiento e impulso de procesos de la mejora y transformación a partir de la apropiación de entornos digitales seguros, con el fin de fortalecer el desarrollo de los procesos académicos y administrativos tanto internos como de comunidades objetivo, teniendo como base un enfoque estratégico de innovación aplicada que desde su estrategia contribuya en la mejora continua del portafolio de servicios endureciendo la experiencia adquirida por el CSIRT Académico UNAD, las bases de datos de conocimiento construidas en el modelo de madurez soportado por el uso de tecnologías emergentes que se aplican para dar respuestas a las necesidades del ámbito de actuación del CSIRT
- Implementación de ambientes y tecnologías seguras para dar respuesta a las necesidades de la Universidad y de los programas académicos asociados a esta disciplina

Académico (VIEM - ECBTI):

- Generación de proyectos de investigación con los programas académicos que estén alienados a la disciplina (Especialización en Seguridad Informática y Maestría en Ciberseguridad).
- Generación de patentes (prototipado o software) que contribuyan en el aseguramiento de entornos digitales
- Generación de espacios de proyección con comunidades, donde el eje central de participación académica y científica sea la educación, difusión o divulgación de información relacionada con ciberseguridad. Con el fin de contribuir en alcanzar lo propuesto por los objetivos de desarrollo sostenible – ODS como son: (4) Educación de calidad, (9) Industria, Innovación e infraestructura, (17) Alianzas para Lograr los Objetivos
- Apoyar en las zonas en las cuales hace presencia la universidad, procesos de transformación para el fortalecimiento de entornos digitales seguros a empresas y entes territoriales a partir de: educación continuada, asesorías, consultorías y auditorias, impactando en los ODS (8) Trabajo Decente y Crecimiento Económico y (9) Industria, Innovación e Infraestructura

Problema

Actualmente la Escuela de Ciencias Básicas Tecnología e Ingeniería cuenta con 6 cadenas de formación las cuales "*han sido concebidas teniendo en cuenta las necesidades científicas y sociales que se han identificado dentro de los diferentes contextos regionales, nacionales e internacionales a partir de un análisis realizado por investigadores integrantes de los grupos de investigación de cada uno de los programas académicos.*" [6] De estas, las cadenas de formación en sistemas y de Electrónica, telecomunicaciones y redes, cuentan con líneas de investigación que dan soporte a la construcción de procesos de I+D+i en áreas específicas del conocimiento como ingeniería de software, gestión de sistemas , infraestructura tecnológica y seguridad en redes y automatización de herramientas lógicas; que aunque en la temática propuesta abordan temas relacionados con ciberseguridad, ninguna de ellas permite profundizar en esta disciplina de tal forma que se pueda dar respuesta a las necesidades de ciberseguridad que requiere el país, tal como lo plantea (Sanabria & Ospina, 2020).

A partir de lo anterior se plantea la pregunta problema:

¿Cómo la consolidación de una línea de investigación en Ciberseguridad da respuesta a las necesidades y desafíos que requiere esta disciplina y como ésta se articula con los programas de la ECBTI y sus productos derivados desarrollados a través de proyectos de I+D+i?

[6] https://academia.unad.edu.co/investigacion-ecbti/cadenas-de-formacion

Justificación

La UNAD considera la investigación como una responsabilidad fundamental, con el objetivo de generar y adquirir conocimiento aplicado y trabajar en conjunto con diferentes actores del ecosistema gubernamental, universitario, empresarial y social, para lograr cambios en las realidades territoriales. Además, busca fomentar la innovación, la inclusión y el desarrollo regional, a través de la investigación-creación, que se enfoca en expresar las necesidades de las regiones.

A partir de lo anterior y con base en la necesidad expresada, El Centro de Respuestas a Incidentes Informáticos CSIRT Académico UNAD plantea en conjunto con la Escuela de Ciencias Básicas Tecnología en Ingeniería y la Vicerrectoría de Innovación y Emprendimiento la consolidación de la línea de investigación en Ciberseguridad, que tiene como propósito: Desarrollar proyectos de I+D+i relacionados con esta disciplina del conocimiento, que sean gestados a través de los programas que componen la cadena de formación de sistemas y de ETR, los grupos y semilleros de investigación, los egresados y en si a toda la plataforma humana Unadista y sus partes interesadas, con el propósito de aportar en la construcción del conocimiento.

Es importante mencionar que la creación de una línea de investigación en ciberseguridad también permitiría a la UNAD abordar aspectos éticos y legales relacionados con la ciberseguridad, lo que es fundamental en un entorno donde la privacidad y la protección de datos personales son de gran importancia. Además, la ciberseguridad no solo afecta a las empresas y organizaciones, sino también a los individuos en su vida cotidiana, lo que hace que la formación de profesionales en ciberseguridad sea relevante para toda la sociedad.

Así mismo, el desarrollar proyectos de investigación en áreas como la criptografía, la seguridad en la nube, la seguridad en dispositivos móviles, la seguridad en redes, entre otros temas relevantes en la actualidad, permite la colaboración con empresas y organizaciones para el desarrollo de soluciones de ciberseguridad específicas para sus necesidades y la realización de pruebas y evaluaciones de seguridad. Teniendo presente que la ciberseguridad es un campo en constante evolución y desarrollo que permite estar a la vanguardia en tendencias y avances en este campo. Esto impacta de forma directa en la actualización constante de los planes de estudio de los programas a fin.

Líneas de investigación actuales planteadas por la ECBTI, para dar respuesta a necesidades de TI

Descripción de líneas, sublíneas y grupos de investigación-creación del Programa.

La Escuela de Ciencias Básicas, Tecnologías e Ingeniería - ECBTI, a través de las cadenas de formación cuenta con sus propias temáticas de investigación, las cuales se enmarcan en las Líneas de investigación. En términos de la disciplina de la Ciberseguridad, el trabajo de investigación lo ha venido realizando de forma significativa el programa de Especialización en Seguridad Informática, el cual ha venido aportando a la línea de investigación de Gestión de Sistemas y a la línea de investigación de Infraestructuras tecnológicas y seguridad en redes, esta última asociada a la cadena de formación de ETR.

Líneas, Sublíneas y temáticas de investigación Investigación-creación del programa que se articulan con la disciplina de la Ciberseguridad.
La siguiente tabla presenta las líneas de investigación y cuáles de estas se han articulado a desde temáticas asociadas a la Ciberseguridad.

*Es importante mencionar que los objetivos planteados no profundizan áreas de la Ciberseguridad concretos.

Tabla 2: Líneas de investigación asociadas a las cadenas de Sistemas y ETR

Cadena	Línea de Investigación	Objetivos	Articulación
Sistemas	Gestión de Sistemas	● Apoyar el desarrollo productivo, tecnológico y social empresarial a través del análisis, diseño, implementación o administración de sistemas de información y las TIC que estén basados en la plantificación, dirección, control, evaluación y realimentación de actividades procedimentales.	SI
	Ingeniería del software	● Desarrollar experiencias de orden formativo y disciplinar en el campo de la investigación, con base a la construcción de software de forma sistémica y estructurada de acuerdo a los principios propios de la ingeniera de software.	NO
ETR	Infraestructura Tecnológica y Seguridad en Redes	● Utilizar herramientas de software para diseño, administración, operación, seguridad y mantenimiento de redes para su óptimo funcionamiento. ● Transferir y apropiar conocimientos y habilidades para el diseño, instalación, operación y mantenimiento de redes de última tecnología (NGN) ● Aplicar los diferentes protocolos e infraestructura para la provisión de servicios telemáticos a los sitios desprovistos de los mismos, dirigidos a la población con mayores necesidades.	SI
	Automatización y herramientas lógicas	● Realizar investigación aplicada en el área de automatización, control industrial e instrumentación para determinar las condiciones y áreas de aplicación, en los diferentes	NO

		• sectores del ámbito nacional.	

Recuperado de: https://academia.unad.edu.co/investigacion-y-productividad-ecbti/lineas

La siguiente tabla presenta como se han venido articulando temáticas de investigación generadas en los cursos y proyectos realizados en el programa de Especialización en Seguridad Informática con las líneas de anteriormente mencionadas.

Tabla 3: temáticas de ciberseguridad asociadas a las líneas de investigación de la ECBTI

Línea de Investigación	Temática de Investigación
Gestión de sistemas	Marcos de Ciberseguridad
	Gestión de la ciberseguridad con estándares internacionales
	Programas y políticas de seguridad de la información
	Procesos y fases de la auditoria de sistemas de información
	Controles Internos de sistemas de Información
	Aplicación de la analítica predictiva en la detección de fraudes
	Enfoque híbrido humano-bot para la detección de ataques cibernéticos
	Métricas de análisis predictivo de la seguridad cibernética.
	Análisis predictivo de riesgos cibernéticos
	Análisis de comportamiento de entidades y usuarios predictivos
	Técnicas de aprendizaje supervisado y no supervisado aplicado en la detección de ataques y anomalías
	Uso del aprendizaje automático para la búsqueda de vulnerabilidades en la red
	Técnicas de aprendizaje profundo basado en redes neuronales para detección de comportamientos maliciosos.
	Generación y priorización de alertas de seguridad en IDS mediante técnicas de aprendizaje automático.
	Análisis de tráfico en la red
	Planeación de proyectos de ciberseguridad
	Auditoria de Ciberseguridad
	Aplicación de Controles de Ciberseguridad
	Modelos de retorno de inversión en la seguridad de la información
	Metodologías para el análisis de riesgos cibernéticos
	Soluciones de orquestación, automatización y respuesta de seguridad (SOAR)
	Arquitectura Zero Trust (ZTNA)
	Seguridad y Resiliencia
	Resiliencia Organizacional.
	Continuidad de Negocio
	Aspectos legales de orden nacional e internacional en el ámbito de la Ciberseguridad
	Propiedad Intelectual y protección jurídica del software
	Protección de datos: fundamentos, obligaciones de registro y medidas de seguridad
	Contratación y acuerdos de niveles de servicio
	Controles de Seguridad Críticos y las capacidades operativas como eje de las estrategias de ciberdefensa.
	Elementos de los roles de ciberseguridad
	Plan de recuperación de desastres y gestión para la continuidad de negocio
	Estándares, modelos y metodologías enfocados en la gestión de incidentes

	cibernéticos
	Planes de contingencia y continuidad
	Equipos de Respuesta a Incidentes Informáticos
	Políticas y Estrategias Nacionales de ciberataque y ciberdefensa
	Estándares, marcos de trabajo y buenas prácticas para el aseguramiento de entornos computacionales en la nube
	Modelo de responsabilidad compartida en la nube
	Modelos y Metodologías para el diseño de arquitecturas seguras
	Indicadores de Compromiso e Indicadores de Ataque
	Estándares para la evaluación de seguridad en infraestructuras
	Metodologías de Pruebas de Penetración
	Estándares, marcos de trabajo y metodologías de desarrollo de software seguro
Línea de Investigación	**Temática de Investigación**
Infraestructura Tecnológica y Seguridad en Redes	Técnicas para la comprensión de amenazas (Honeypot)
	Despliegue y virtualización de infraestructuras seguras
	Security Servers mediante X-road
	Técnica para la reducción de amenazas (WAF - SD-WAN)
	Infraestructuras seguras en smart cities
	Aseguramiento de infraestructuras en redes y sistemas SCADA
	Infraestructuras seguras en la nube usando Blockchain
	Defensa en redes IoT usando técnicas de Machine Learning
	Técnicas de Endurecimiento en Infraestructuras de TI
	Vectores y técnicas de ataque
	Técnicas de reconocimiento
	Estrategias de defensa
	Monitoreo y herramientas preventivas
	Indicadores, métricas y bases de datos de conocimiento
	Herramientas para Pruebas de Penetración
	Criptoanálisis
	Protección de la información digital
	Clonación cuántica
	Protocolos para la distribución de claves cuánticas
	Ataques a protocolos de distribución de claves cuánticas
	Nuevas técnicas de Cifrado
	Criptografía Cuántica
	Criptografía en las Comunicaciones
	Arquitectura segura para infraestructura TI en la nube
	Modelos de despliegue seguro en la nube
	Herramientas de gestión para el aseguramiento de la información en la Nube
	Infraestructura lógica enfocada en Sistemas de Información para la Gestión de Eventos - SIEM bajo licencia Open Source
	Técnicas de ciberataque
	Tácticas, técnicas y procedimientos de ciberdefensa
	Proceso de análisis Matriz ATT&CK de Mitre
	Ciberamenazas persistentes avanzadas
	Operaciones ofensivas y defensivas en el ciberespacio
	Técnica de anti-análisis y evasión
	Gestión de vulnerabilidades en aplicaciones
	Técnicas y herramientas para el desarrollo seguro

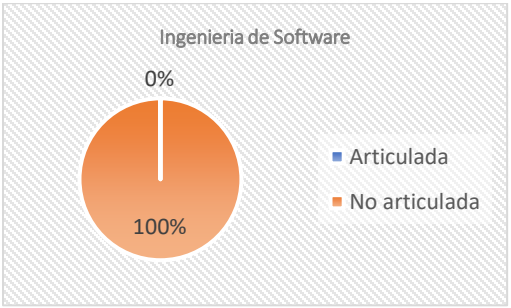
	Técnicas de explotación del Software
	Mecanismos de Consenso en Blockchain
	Algoritmos Criptográficos Hash para crear bloques
	Contratos inteligentes
	Arboles de Blockchain
	Interoperabilidad en Blockchain
	Inteligencia Artificial aplicada al análisis forense
	Herramientas de análisis forense (Comerciales - Open Source) efectividad, características, comparaciones
	Técnicas antiforense
	Técnicas forenses en Entornos "Cloud"
	Técnicas forenses en dispositivos móviles

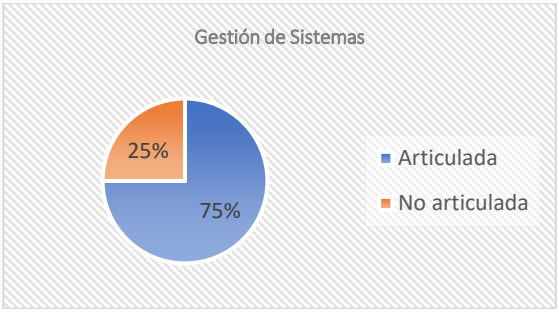
Fuente. ECBTI, 2021 (Documento maestro Maestría en CIberseguridad)

Al realizar análisis a cada una de las temáticas abordadas por cada una de las líneas de investigación y teniendo presente los productos de investigación soportados en cada una de ellas, se puede indicar que el impacto y usabilidad de las líneas propuestas no abarcan las necesidades de investigación que se viene desarrollando a través de proyectos de investigación.

Las siguientes ilustraciones presentan el porcentaje de articulación que cada una de las líneas con relación a la disciplina de la Ciberseguridad. Siendo las líneas de Gestión de sistemas y de infraestructura tecnológica y seguridad en redes impactadas con un 25% en relación con las temáticas propuestas (Ver anexo 1).

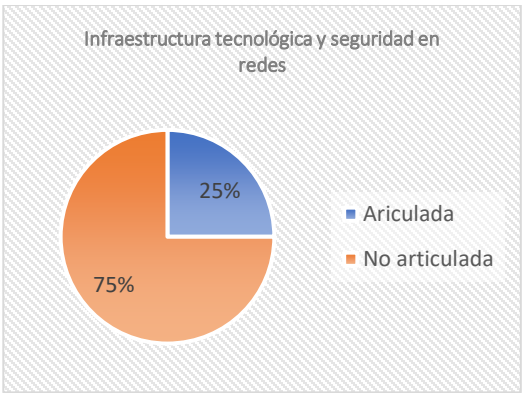
Ilustración 2: Relación de temáticas de las líneas asociadas a la cadena de formación de sistemas con Ciberseguridad.

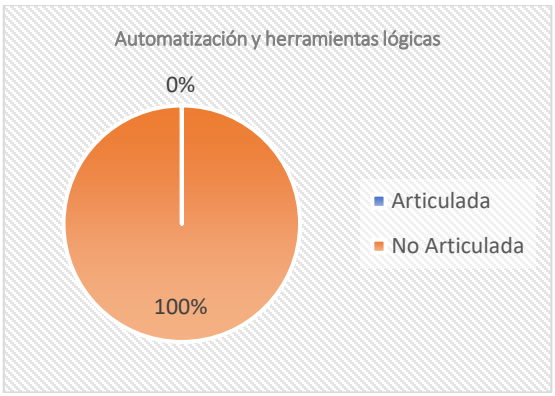




Elaboración propia

Ilustración 3: Relación de temáticas de las líneas asociadas a la cadena de formación de ETR con Ciberseguridad





Elaboración propia

Es de anotar que el programa de Especialización en Seguridad Informática, ha venido aportando productos asociados al objeto de estudio de la Ciberseguridad a través del desarrollo de sus opciones de grado de Monografía, Proyecto Aplicado y Seminario Especializado, apalancando los productos obtenidos a las líneas de investigación de Gestión de Sistemas, e Infraestructura Tecnológica y Seguridad en Redes tal como se observa en la siguiente tabla.

Tabla 4: Opciones de Grado Estudiantes Especialización en Seguridad Informática de acuerdo a Líneas de Investigación:

Tipo de Opción de Grado por Línea	Cantidad de Trabajos
Monografía	245
Gestión de Sistemas	122
Infraestructura tecnológica y seguridad en redes	123
Proyecto Aplicado	262
Gestión de Sistemas	163
Infraestructura tecnológica y seguridad en redes	99
Seminario Especializado	99
Infraestructura tecnológica y seguridad en redes	99
Total general	**606**

Fuente. Repositorio Institucional, Fecha de corte a diciembre de 2021

Propuesta para la creación de la línea de Investigación en Ciberseguridad

Línea[7]:

Ciberseguridad

Temas de Investigación:

Ciberseguridad Estratégica
Ciberseguridad Operativa
Desarrollo de capacidades de Ciberseguridad

Campo del conocimiento:

Ingeniería De Sistemas, Telemática Y Afines[8]

Núcleos problémicos asociados:

Especialización en Seguridad Informática	NP1: Estrategia, gobierno y dirección de seguridad informática NP2: Modelos defensivos y ofensivos en el aseguramiento, manejo y respuesta para la seguridad informática
Maestría en Ciberseguridad	NP1 – Estrategia, gobierno y dirección de ciberseguridad NP2 – Modelos defensivos y ofensivos en el aseguramiento, integración, manejo y respuesta para la aplicación de la ciberseguridad

Programas que se articulan con la línea de investigación (Ver anexo 2):

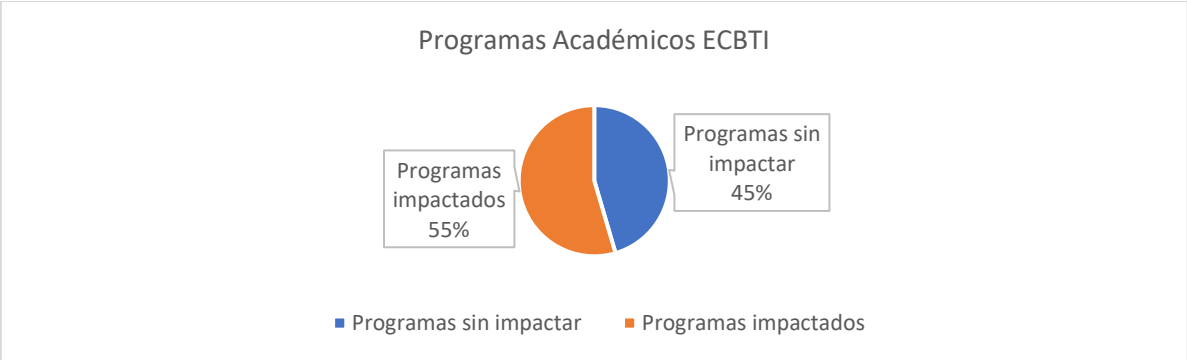
De acuerdo a la revisión curricular de los programas ofertados por la ECBTI, se identifica que de 22 programas existentes con registro calificado activo, se aporta con productos de I+D+i en 12 de programas, a través de la articulación de temáticas relacionadas con ciberseguridad y desde proyectos interdisciplinares en donde la pertinencia de la ciberseguridad sea un factor importante.

- Total de programas de la ECBTI: 22
- Total de programas impactados: 12
- Total de programas sin impactar: 10

[7] Son los ejes temáticos y/o problémicos que por su dimensión engloban la actividad investigativa a nivel institucional o a nivel de escuela

[8] https://snies.mineducacion.gov.co/1778/articles-398980_recurso_1.pdf

Ilustración 4: Porcentaje de programas de la ECBTI impactados por la línea de investigación en Ciberseguridad



Elaboración propia

A continuación, se relaciona lista de programas de la ECBTI impactados

Programa	Cadena	
	Sistemas	ETR
Tecnología en Desarrollo de Software	X	
Tecnología en Gestión de Redes Inalámbricas		X
Tecnología en Automatización Electrónica Industrial		X
Ingeniería Multimedia	X	
Ingeniería de Sistemas	X	
Ingeniería de Telecomunicaciones		X
Ingeniería Electrónica		X
Especialización en Redes de Nueva Generación		X
Especialización en Seguridad Informática		X
Maestría en Diseño de Experiencia de Usuario	X	
Maestría en Gestión de Tecnología de Información	X	
Maestría en Ciberseguridad	X	

Elaboración propia

Grupos que soportan la línea de investigación

Grupo	Byte in Design
GRUPLAC	https://scienti.minciencias.gov.co/gruplac/jsp/visualiza/visualizagr.jsp?nro=00000000002262
Líder	María Consuelo Rodríguez Niño
Clasificación	A
Área de conocimiento	Ingeniería y Tecnología -- Ingenierías Eléctrica, Electrónica e Informática -- Ingeniería de Sistemas y Comunicaciones

Relación de docentes investigadores

Nombre Del Profesor	Nivel de formación	Área de conocimiento
Diana Marcela Vásquez Bravo	Doctor	Ingeniería del Software
Gilberto Pedraza García	Doctor	Ingeniería de Software
John Freddy Quintero Tamayo	Maestría	Pentesting y seguridad operativa
Luis Fernando Zambrano Hernandez	Maestría	Ciberseguridad - Análisis de Riesgos Informáticos - Equipos de Respuesta a Incidentes Informáticos

Hernando José Peña Hidalgo	Maestría	Seguridad informática, infraestructura, desarrollo de software seguro
Edgar Mauricio López Rojas	Maestría	Ingeniería de Sistemas, seguridad informática, Redes e infraestructura
Joel Carroll Vargas	Maestría	Seguridad en infraestructura de TI
Eduard Antonio Mantilla Torres	Maestría	Seguridad de la información
Edgar Roberto Dulce Villarreal	Maestría	Seguridad Informática, Telecomunicaciones y Blockchain
Christian Reynaldo Angulo Rivera	Maestría	Ciberseguridad
Alexander Larrahondo Núñez	Maestría	Gestión de seguridad de la información
Katerine Marceles Villalba	Maestría	Ingeniería - Ciberseguridad
Yolima Esther Mercado Palencia	Maestría	Seguridad de la información
Andrés Ernesto Salinas Duarte	Maestría	Seguridad Informática
Sonia Ximena Moreno Molano	Maestría	Seguridad Informática

Semilleros de investigación enfocados en Ciberseguridad

A través de la Especialización en Seguridad Informática, se han consolidado dos semilleros que giran en torno a realizar procesos de investigación e investigación formativa en ciberseguridad

Semillero de Investigación Ceros y Unos	Objetivo: Fomentar las habilidades investigativas en áreas de la Ingeniería relacionadas con ciberseguridad, desarrollo de software y multimedia, que permita al estudiante adquirir competencias argumentativas para la construcción y desarrollo de proyectos de I+D+i Número de estudiantes inscritos: 18 Proyectos desarrollados: 3 Trabajo de grado: 4 Proyectos en desarrollo: 2
Semillero de Investigación Cibercosmonautas	Objetivo: Fomentar el ejercicio de investigación en estudiantes y docentes de la escuela de ciencias básicas tecnología e ingeniería que permita promover acciones para el mejoramiento de la ciberseguridad, gestión de sistemas, software y tecnologías de la educación. Número de estudiantes inscritos: 10

Características Especificas

A continuación, se presenta la articulación entre la línea de investigación en Ciberseguridad con las líneas de acción propuestas por MINCIENCIAS

Tabla 5: Articulación de la línea de investigación en Ciberseguridad con las líneas de acción propuestas por Minciencias

Línea de investigación	Líneas de acción propuestas por Minciencias	Articulación
Ciberseguridad	Participación ciudadana en CTI	Teniendo presente que la UNAD "busca contribuir al desarrollo humano sostenible en todas sus dimensiones, a partir de marcos de referencia territorial y regional, con el propósito de contribuir con el liderazgo social, orientado por el bienestar integral de las comunidades y la transformación social equitativa de Colombia[9] (UNAD, 2019). Estatuto Organizacional. En este sentido La línea se articula con: **SINEC**: Contribuyendo con información que aporten en la formulación de proyectos y a la gestión de estándares institucionales **SINEP**: Aportando con información que permitan la equidad de oportunidades **SISSU**: Apoyando las estrategias las que permitan dinamizar las dimensiones UNADISTAS **OIR**: Realizando acciones que aporten en el desarrollo de los territorios desde la promoción y el fomento de oportunidades. **ECBTI**: Impactando a través de procesos de I+D+i los programas que se articulan con la ciberseguridad en especial los programas de Especialización en Seguridad Informática y Maestría en Ciberseguridad **CSIRT:** Articulando el quehacer diario de este dispositivo con acciones de I+D+i con el fin de dar desarrollo a sus capacidades
	Comunicación con enfoque en Ciencia, Tecnología y Sociedad (CTS)	Puesto que la Ciberseguridad en una necesidad que impacta a partes interesadas como comunidad científica, sector productivo, gestores de política en CTI, ciudadanos y el sector académico, de forma particular el programa de Especialización en Seguridad Informática y la Maestría en Ciberseguridad de la UNAD. Con base en la comunicación la difusión de la información generada a través de procesos de I+D+i, propiciar mediaciones que involucran su participación
	Gestión del conocimiento	Aportando al desarrollo de capacidades en Ciberseguridad (estratégicas y operativas) no solo de la Universidad sino de las partes interesadas, teniendo como base la gestión de nuevo conocimiento y el conocimiento de frontera, con el fin de seguir construyendo conocimiento a partir de la solución de

[9] https://sgeneral.unad.edu.co/images/documentos/consejoSuperior/acuerdos/2019/COSU_ACUE_039_20190312.pdf

		problemas reales y de la aplicación de las bases de datos del conocimiento y de las lecciones aprendidas por el CSIRT Académico UNAD
	Intercambio del conocimiento	Dada la importancia de generar estrategias o alianzas para lograr los objetivos en términos de Ciberseguridad, el intercambio de conocimiento generado en procesos de I+D+i es un factor crucial. De esta forma se da respuesta a las necesidades del sector, a lo planteado por ITU (ITU, 2022)[10] y a la misión UNADISTA a partir del desarrollo de las capacidades del CSIRT y de la articulación con la ECBTI en términos de CTeI. Esto con el fin de establecer alianzas para afianzar el desarrollo de capacidades en ciberseguridad de las organizaciones

Elaboración propia

Articulación de la línea de investigación en Ciberseguridad con el metasistema Unadista

	Misión UNADISTA	PEE	e-MPU
Línea de investigación en Ciberseguridad	La ciberseguridad se convierte en un aspecto crucial para garantizar la protección y privacidad de los datos de toda la plataforma humana UNADISTA. En este sentido, la investigación en ciberseguridad contribuye en identificar y abordar las amenazas cibernéticas específicas que enfrenta la Universidad y a desarrollar soluciones efectivas para proteger la infraestructura de tecnología de la información y sus sistemas de información.	Teniendo presente los tres objetos de conocimiento definidos por la ECBTI (Ciencias Básicas, La Tecnología y la Ingeniería), la ciberseguridad En las Ciencias Básicas, juega un papel importante en la protección de los datos y la información utilizados en investigaciones científicas y experimentos lo que permite una investigación científica más precisa y segura, apoyada por tecnologías que garantizan la calidad y seguridad de los productos y servicios tecnológicos, fomentando así la confianza y el crecimiento en la industria tecnológica. Así mismo, en la Ingeniería, la ciberseguridad es fundamental para la protección de los sistemas y la infraestructura crítica	Sabiendo que el modelo se enfoca en el aprendizaje autónomo, significativo y colaborativo, la investigación en ciberseguridad se relaciona directamente con el modelo pedagógico Unadista, ya que permite fomentar el desarrollo de habilidades y competencias en los estudiantes que les permiten ser sujetos activos y críticos en la protección de la información y los activos digitales en la sociedad.

[10] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/513560_2S.pdf

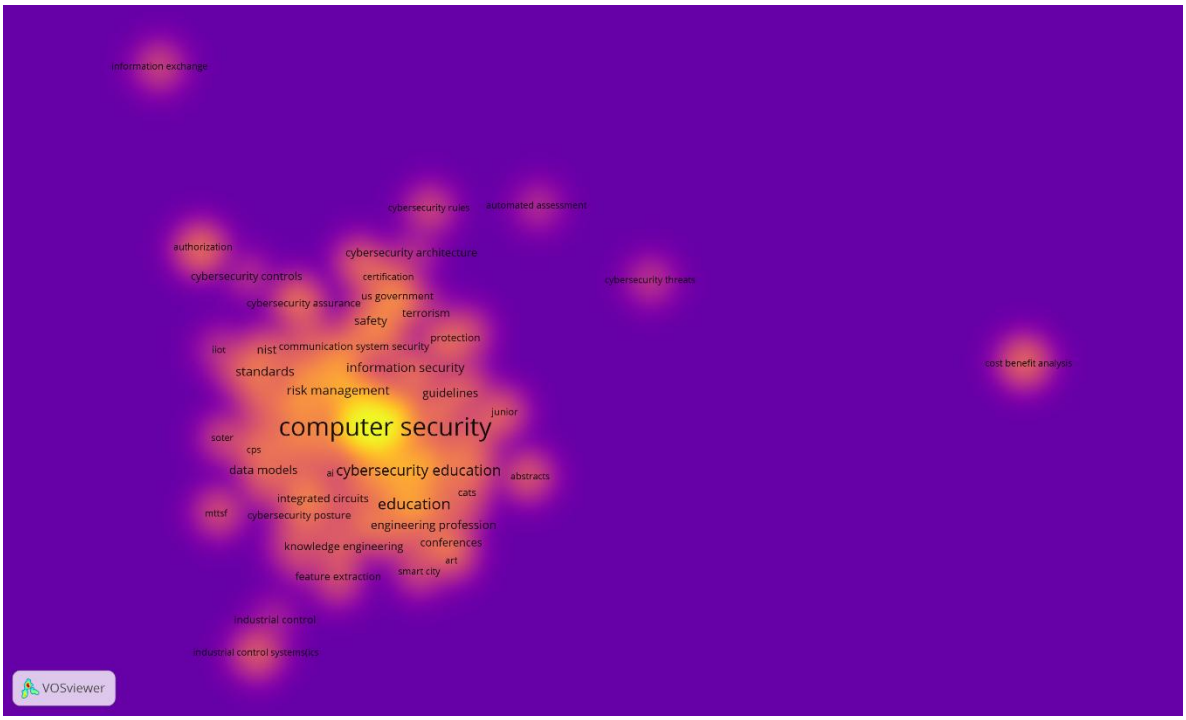
Fundamentos Teóricos y Epistemológicos

Análisis Literario

Al realizar búsqueda relacionada con el término "**Cybersecurity**" en dos de las bases de datos más relevantes de orden académico y científico para los últimos tres años, se identifican los siguientes tópicos:

Base de datos documental **IEEE**
Total de documentos analizados: 9151

Ilustración 5: Tópicos de interés investigados y publicados en IEEE



Fuente. El Autor

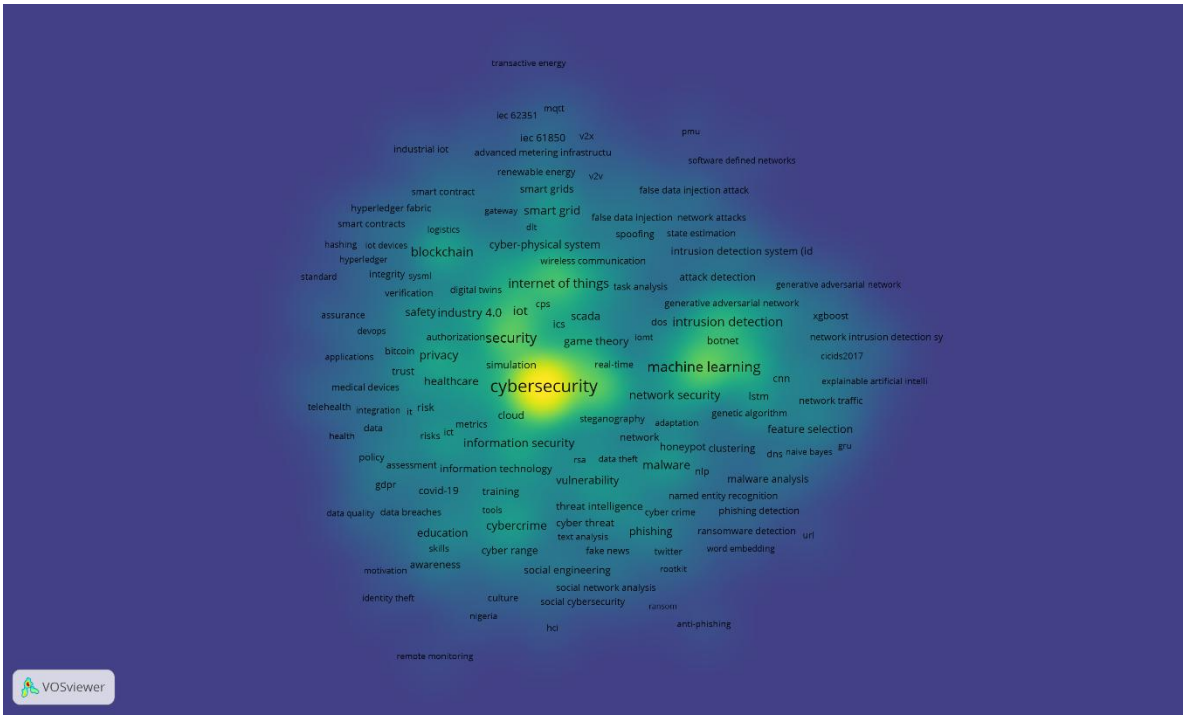
La ilustración anterior, permite evidenciar que para los años 2020 a 2023 los temas con mayor relevancia para ser investigados en la disciplina de la ciberseguridad son (Ver Anexo 5):

Tópico	Descripción
Cybersecurity Education	Hace referencia al proceso de enseñanza y aprendizaje que busca desarrollar conocimientos, habilidades y actitudes necesarias para proteger los sistemas informáticos y datos de amenazas cibernéticas (NICE, 2020).
Data models	Hace referencia a un modelo que describe la estructura de los datos relevantes para la seguridad de la información y los procesos de gestión de la seguridad de los sistemas informáticos (SienceDirect, 2018)

Risk management	Hace referencia al proceso de identificar, evaluar y gestionar los riesgos asociados a las amenazas cibernéticas en los sistemas informáticos y de información (Fischer, IMgrund, Janiesch, & Winkelmann, 2020)
Communication system security	Hace referencia al conjunto de medidas que se implementan para proteger las redes de comunicación y los datos que se transmiten por ellas (Rwat, Doku, & Garuba, 2021)
Information security	Hace referencia a la protección de la confidencialidad, integridad y disponibilidad de la información en los sistemas informáticos y de información
Cybersecurity assurance	Hace referencia a la verificación y validación de la efectividad de los controles de seguridad implementados en los sistemas de información para proteger los datos y los activos de la organización
Cybersecurity controls	Hace referencia a las medidas que se implementan para proteger los sistemas informáticos y de información contra las amenazas cibernéticas
Cybersecurity architecture	Hace referencia a la implementación de un conjunto de medidas y controles de seguridad en los sistemas de información de una organización para protegerlos contra posibles amenazas y vulnerabilidades
Cybersecurity threats	Hace referencia a las posibles amenazas que pueden afectar la seguridad de los sistemas informáticos y de información de una organización (Singer & Friedman, 2017)
Cybersecurity rules	Hace referencia a las políticas y procedimientos que se establecen para proteger los sistemas informáticos y de información de una organización contra posibles amenazas y vulnerabilidades (Singer & Friedman, 2017)
Automaten assessment	Hace referencia a la evaluación automatizada de la seguridad de los sistemas informáticos y de información de una organización
Cybersecurity posture	Hace referencia a la postura o posición de una organización en cuanto a su capacidad para proteger sus sistemas informáticos y de información contra posibles amenazas y vulnerabilidades (Singer & Friedman, 2017)
Standards	Hace referencia a las normas y mejores prácticas establecidas por organismos nacionales e internacionales para garantizar la seguridad de los sistemas informáticos y de información (ISO, 2022)
Computer Security	Hace referencia a la protección de los sistemas informáticos y de información contra posibles amenazas y ataques. La seguridad informática es un aspecto fundamental de la ciberseguridad, ya que protege los datos, sistemas y redes de una organización contra el acceso no autorizado, la modificación, el robo y la destrucción (Bosworth, kabay, & Whiney, 2014).

Base de datos documental **SCOPUS**
Total de documentos analizados: 17109

Ilustración 6: Tópicos de interés investigados y publicados en SCOPUS



Fuente. El Autor

La ilustración anterior, permite evidenciar que para los años 2020 a 2023 los temas con mayor relevancia para ser investigados en la disciplina de la ciberseguridad son:

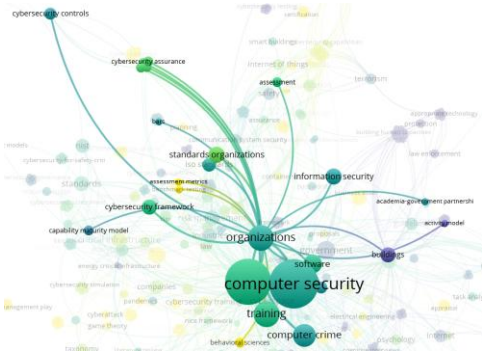
Tópico	Descripción
Machine learning	Jordan y Mitchell (2015) definen el aprendizaje automático como una rama de la inteligencia artificial que utiliza algoritmos y modelos para permitir a los sistemas informáticos aprender y mejorar su rendimiento sin programación explícita.
Intrusión detection	La detección de intrusiones es un proceso que busca identificar actividades malintencionadas o no autorizadas en una red o sistema, mediante la monitorización y análisis de eventos de red o sistema, según Dacier, Deswarte y Kaâniche (2000).
Safety industry 4.0	Según Ghazanchyan y Sundberg (2019), la industria de la seguridad 4.0 emplea tecnologías avanzadas como IoT, IA y robótica para mejorar la seguridad y eficiencia en ambientes industriales y empresariales.
Botnet	Una botnet es una red de dispositivos infectados con software malicioso, controlados por un atacante remoto para realizar acciones fraudulentas o dañinas (Singh & Singh, 2021).
Cybercrime	El ciberdelito se refiere a los delitos cometidos a través de dispositivos electrónicos y/o Internet, como el robo de datos, la extorsión y el acoso en línea (Jaishankar, 2020).
Blockchain	La tecnología de Blockchain es una base de datos descentralizada que permite el registro de transacciones de manera segura e inmutable

	mediante la utilización de algoritmos criptográficos y consenso distribuido (Swan, 2021).
Internet of things	El Internet de las cosas (IoT) se refiere a la interconexión de dispositivos y objetos cotidianos a través de internet, permitiendo la recopilación y transmisión de datos para su análisis y uso (Atzori, Iera & Morabito, 2017).
Malware	El malware es un software malicioso diseñado para dañar, alterar o robar información de un sistema o red, y puede incluir virus, gusanos, troyanos, spyware y ransomware (Kaspersky, 2021).
Cyber range	Cyber Range es un entorno controlado y simulado utilizado para entrenar y evaluar habilidades y respuestas de seguridad cibernética en tiempo real, con el objetivo de mejorar la capacidad de respuesta a incidentes cibernéticos (Tamboli, 2021).
Gdpr	La GDPR establece reglas para proteger los datos personales de ciudadanos de la UE y se aplica a empresas que procesan datos personales de ciudadanos de la UE, sin importar su ubicación geográfica (Kuner, et al., 2019).
Thret intelligence	Threat intelligence se refiere al análisis de información para identificar y predecir amenazas cibernéticas con el objetivo de mejorar la capacidad de una organización para detectar y responder a estas amenazas (Wright, et al., 2020).
Steganography	La esteganografía es la técnica de ocultar mensajes o archivos dentro de otros archivos, como imágenes o videos, para evitar su detección (Bhatt, 2020).
Network security	La seguridad de redes se refiere a la protección de la integridad y confidencialidad de los datos transmitidos a través de redes de computadoras, mediante el uso de herramientas y técnicas para prevenir y detectar posibles ataques cibernéticos (Li, et al., 2021).
Generative adversarial network	Las Redes Generativas Adversarias (GAN, por sus siglas en inglés) son un tipo de algoritmo de aprendizaje automático que consiste en dos redes neuronales compitiendo entre sí para generar datos realistas (Goodfellow et al., 2020).

El análisis de co-ocurencias realizado con la herramienta VOSviewer[11], las siguientes ilustraciones, presentan las apariciones conjuntas de los términos relacionados con los documentos analizados. Este tiene como propósito identificar cual es la estructura conceptual que en este momento la investigación en ciberseguridad viene abordando

[11] https://www.vosviewer.com/

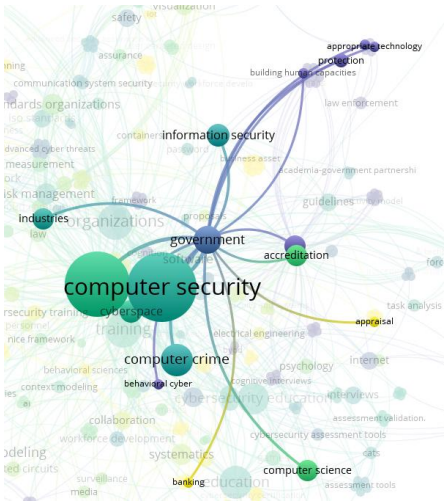
Ilustración 7: Co ocurrencias encontradas con el término "organizations"



Recuperado de: análisis a través de herramienta VOSviewer

La ilustración anterior, permite evidenciar como la investigación en Ciberseguridad gira en torno a las organizaciones y como ésta es crucial para proteger los sistemas de información, los datos contra el crimen computacional y los ataques cibernéticos. En este sentido, la investigación se asocia con el entrenamiento del talento humano, la necesidad de trabajar en modelos de madurez de capacidades, en la importancia de marcos de trabajo en ciberseguridad y en la articulación con la academia, el gobierno y las partes interesadas, entre otros.

Ilustración 8: Co ocurrencias encontradas con el término "goverment"

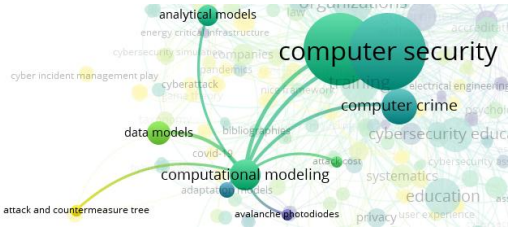


Recuperado de: análisis a través de herramienta VOSviewer

La ilustración anterior, permite evidenciar cómo la investigación en Ciberseguridad gira en torno al gobierno y cómo éste se articula con seguridad de la información, organizaciones de acreditación, con la necesidad de trabajar en relación con el crimen informático a partir de la apropiación de tecnologías se converge con la identificación de incidentes, la protección de los activos y la generación de estrategias teniendo como

base la construcción de capacidades del talento humano que puedan ser articuladas con la industria.

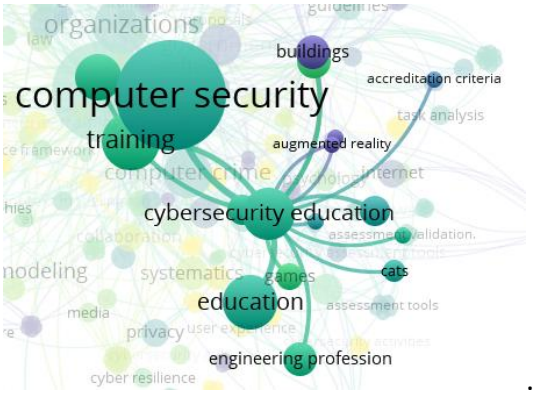
Ilustración 9: Co ocurrencias encontradas con el término "computational modeling"



Recuperado de: análisis a través de herramienta VOSviewer

La ilustración anterior presenta al modelado computacional, el crimen forense, los modelos de datos relacionado con el tópico de investigación de seguridad computación. Esto obedece al incremento de ataques cibernéticos que viene atravesando las organizaciones y las personas y a la necesidad de modelos computacionales que contribuyan en mejorar los tiempos y las técnicas de respuesta ante estas adversidades.

Ilustración 10: Co ocurrencias encontradas con el término "cybersecurity education"

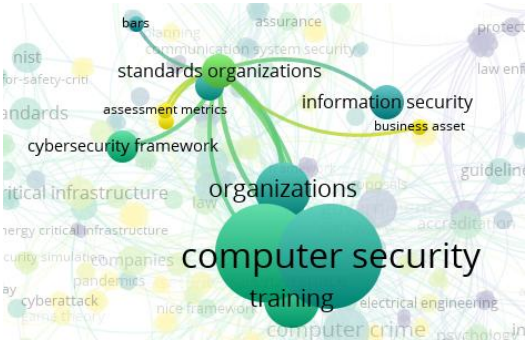


Recuperado de: análisis a través de herramienta VOSviewer

El documento de ACM 2023[12], el cual se encuentra en construcción evidencia la importancia de generar espacios de educación en Ciberseguridad. Aunque este tópico ya se ha venido abordando desde el documento de 2017, el talento humano[13] y la disciplina de la Ciberseguridad deben ser transversales respecto a la buena gestión de técnicas estratégicas y operativas que aporten en mejorar los procesos de tecnologías emergentes que hagan uso de infraestructuras tecnológicas y tecnologías emergentes.

[12] https://csed.acm.org/wp-content/uploads/2023/03/Version-Beta-v2.pdf
[13] https://www.scielo.org.mx/pdf/edsc/v10n24/2007-8064-edsc-10-24-e81727.pdf

Ilustración 11: Co ocurrencias encontradas con el término "Standar organizations"



Recuperado de: análisis a través de herramienta VOSviewer

Los estándares organizaciones en ciberseguridad debe estar trazados por tres factores fundamentales: Proceso bien definidos que contribuyan en el aseguramiento de un entorno digital, un talento humano entrenado y altamente capacitado para acompañar estos procesos y una infraestructura tecnológica que soporte su accionar. En este sentido los estándares organizaciones brindan pautas para garantizar que estos ejes trabajen de forma síncrona con aporten en la construcción de métricas y lineamientos en Ciberseguridad.

Contextualización de la línea de Investigación en Ciberseguridad en el ámbito Nacional e Internacional

Tendencias

Aunque la ciberseguridad y la concienciación sobre esta parecen estar mejorando, la amenaza y sofisticación de los ciberataques también están aumentando. (Brooks, 2022) destaca la importancia de abordar los riesgos de la ciberseguridad en la industria y el gobierno, y proporciona un análisis sobre las posibles implicaciones de las estadísticas y tendencias emergentes en ciberseguridad. Además, destaca la importancia de abordar los riesgos de la ciberseguridad en la industria y el gobierno, y proporciona recomendaciones para protegerse contra los ciberataques, incluyendo el uso de contraseñas fuertes, la monitorización de las puntuaciones de crédito y estados de cuenta bancarios, y la creación de una estrategia de gestión de riesgos corporativos y un marco de vulnerabilidad para proteger los activos digitales y los correos electrónicos confidenciales. En el documento, Brooks destaca tendencias y estadísticas de ciberseguridad para 2023, entre las cuales se encuentran:

- Mayor superficie de ataque y sofisticación de los ciberdelincuentes.
- Mayor interés en los usuarios y el Metaverso como nuevos vectores de explotación.
- Uso de herramientas de inteligencia artificial por parte de los piratas informáticos.
- Vulnerabilidades de la infraestructura crítica por amenazas de estado-nación.
- Código no parcheado y desactualizado y sistemas heredados.
- Escasez continua de personal de seguridad calificado.
- Aumento de los eventos cibernéticos dirigidos a los datos contables y financieros de las organizaciones.
- Falta de colaboración entre los equipos de contabilidad y finanzas y los equipos de ciberseguridad.
- Crecimiento exponencial de los datos colectivos de la humanidad y la necesidad de asegurarlos.
- Priorización de la ciberseguridad de arriba hacia abajo y de abajo hacia arriba en la industria y el gobierno.

(li & liu, 2021), destacan la importancia de proteger los datos de los ataques cibernéticos y explora varios métodos utilizados para prevenir el daño causado por estos ataques. En su documento, discuten los desafíos, debilidades y fortalezas de los métodos propuestos y se analizan diferentes tipos de nuevos ataques; entre ellos:

- Ataques a aplicaciones web como el punto más débil para atacar a una organización.
- El aumento de los ataques de grupos de personas que buscan obtener ganancias financieras.
- La infiltración de redes con un mínimo de conocimiento y habilidades.

- El aumento de los ataques de hacktivistas con motivos políticos.
- La falta de capacidad técnica para asignar actividades a individuos o grupos con un alto grado de confianza.
- La creciente complejidad de la ciberseguridad y la necesidad de tener una "perspectiva de seguridad" sobre cómo funciona la ciberseguridad.
- La importancia de la encriptación para proteger la información importante y privada.
- La necesidad de una estrategia integral de ciberseguridad que cubra todos los aspectos y no deje ninguno fuera.

En el artículo de investigación “The recent trends in cyber security: A review” (Kaur & Ramkumar, 2022), recopila varios artículos y estudios relacionados con la criptografía y la ciberseguridad. Cubriendo una amplia gama de temas, incluyendo tendencias recientes en ciberseguridad, tipos de ataques cibernéticos, técnicas avanzadas de encriptación y gestión de claves, vulnerabilidades y limitaciones de estas técnicas, y desafíos y amenazas en el campo de la ciberseguridad. El articulo proporciona una visión general de los avances y desafíos en la criptografía y la ciberseguridad, indicando que se han producido importantes avances en la tecnología de encriptación y la gestión de claves, incluyendo técnicas avanzadas de encriptación y autenticación, así como la adopción de estándares de seguridad más sólidos. Así mismo, se exponen en varios desafíos significativos en el campo de la ciberseguridad, como:

- La evolución constante de las amenazas y los ataques cibernéticos,
- La vulnerabilidad de los sistemas a los ataques de ingeniería social
- La necesidad de mantenerse al día con las últimas tendencias y tecnologías en el campo de la ciberseguridad.

Además (Kaur & Ramkumar, 2022) , indican que la aparición de la computación cuántica plantea nuevos desafíos para la criptografía y la seguridad de la información.

La comisión Económica para América Latina y el Caribe, pone a consideración para las agendas nacionales, que el alcance de políticas publicas deben estar alienadas con (CEPAL, 2022):

- El fortalecimiento de las políticas de privacidad y seguridad
- La generación de reglas de macrodatos y de inteligencia artificial, encriptación y anonimización
- La encriptación de las redes privadas
- La aplicación y monitoreos de seguridad
- Las brechas de datos
- La protección y monitoreo de ciberataques
- La respuesta a incidentes.
- Las reglas de resiliencia
- La protección de infraestructura crítica

Así mismo en sus objetivos plantea: *"Combatir la delincuencia en medios digitales mediante la formulación de políticas públicas y estrategias de ciberseguridad y de protección de infraestructuras críticas, el desarrollo o establecimiento de marcos normativos alineados con los instrumentos internacionales de derechos humanos y el fortalecimiento de capacidades y de sistemas seguros basado en las mejores prácticas, así como la coordinación local, regional e internacional entre equipos de respuesta a incidentes cibernéticos y entre los actores interesados." y "Promover la coherencia normativa digital a nivel regional, especialmente en materia de protección de datos, flujo de datos transfronterizo, ciberseguridad, comercio electrónico y digital y defensa de los derechos del consumidor en las plataformas en línea, así como la interoperabilidad de la firma y la identidad digitales en la región, de conformidad con el marco normativo y regulatorio interno de cada país.*"

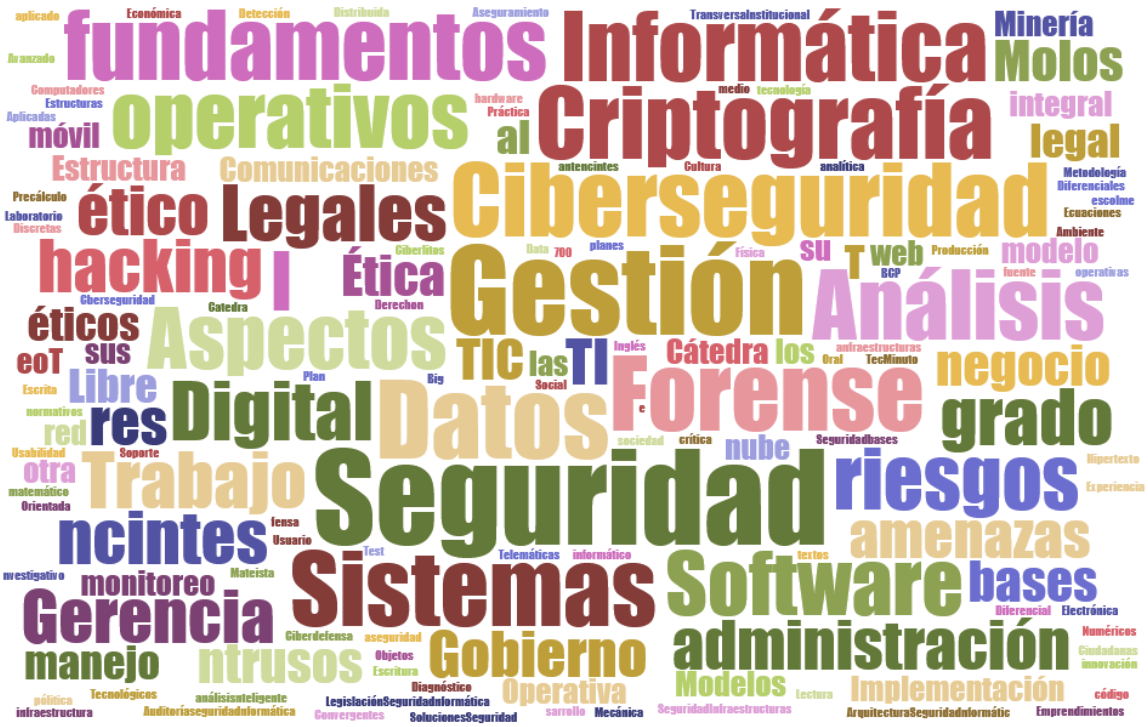
Ámbito Nacional

Colombia ha venido experimentando un aumento en la cantidad de incidentes de ciberseguridad en los últimos años[14], lo que ha llevado a un mayor interés en la protección de la información y la privacidad de los usuarios. Para abordar estas preocupaciones, Colombia ha implementado varias iniciativas para mejorar su postura en esta disciplina, incluyendo el establecimiento de leyes y regulaciones de ciberseguridad, la creación de equipos de respuesta a incidentes de seguridad como lo es el CSIRT Académico UNAD y la promoción de la educación y concienciación sobre la seguridad en internet. En ámbito académico, son mas de 40 instituciones de educación técnica y superior las que ofertan en su portafolio académico programas relacionados con la ciberseguridad (Ver anexo 3).

En el ejercicio de relacionar la Ciberseguridad con procesos de I+D+i, se toma como referente 30 instituciones de educación superior, las cuales a partir de su oferta académica y procesos investigación presentan una cercanía que pueden aportar al desarrollo de investigación en Ciberseguridad.

El siguiente análisis textual representado a través de una nube de palabras presenta cuales son los temas de aprendizaje abordados por la académica en Colombia respecto a las necesidades de Ciberseguridad.

[14] https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20Ciberseguridad%202022.pdf



La ilustración anterior presenta una co relación de la ciberseguridad con procesos forenses, procesos gerenciales, monitoreo, riesgos, gobierno, criptografía y aspectos éticos entre otros. Esto permite evidenciar que en Colombia se está trabajando en torno a necesidades de más operativas. Sin embargo, poco se evidencia como la academia en Colombia involucra en Ciberseguridad el uso de tecnologías emergentes o de desarrollo de capacidades.

Ámbito Internacional

Teniendo presente la importancia de ahondar en temas de investigación que se vienen realizando en el mundo de forma actual, este análisis internacional aborda las siguientes zonas geográficas:

- Asia
- Europa
- Norte América
- Sur América

Los criterios de búsqueda se relacionan con:

- Consulta académica y científica correspondiente a los últimos cuatro años
- Artículos científicos
- Currículos académicos relacionados con seguridad de la información, ciberseguridad y seguridad computacional
- Investigaciones realizadas y en proceso

Con base en lo anterior y realizando análisis a la información recolectada, se obtienen las temáticas que se aprecian en la siguiente tabla

Tabla 6: Temáticas de ciberseguridad que actualmente se vienen explorando en el mundo

Asia	Europa	Norte América	Latinoamérica
AI Servicio de Información	Algoritmos distribuidos	Seguridad de redes	Tecnología de la información, ética y normativa jurídica
Análisis de malware e investigación de ataques	Amenazas de ciberseguridad	Análisis de vulnerabilidades	Introducción al gerenciamiento innovador (entrepreneurship)
Análisis de vulnerabilidades	Amenazas persistentes	Protección de datos	Introducción a los paradigmas de programación
Análisis estático de contratos inteligentes	Arquitecturas de seguridad empresariales	Seguridad en la nube	Tecnología de la información
Aprendizaje automático y seguridad de IA	Arquitecturas seguras	Criptografía	Introducción a la criptología
Ataques de canal lateral y criptoanálisis	Auditoria de seguridad	Ciberseguridad móvil	Evolución de la tecnología militar hasta el enfoque "Network-Centric Warfare"
Autenticación y biometría	Big data	Seguridad de sistemas embebidos	Tecnología de redes
Basados cadena de bloques: Seguridad del sistema Android	Blockchain	Infraestructuras críticas	Malware
Basados en IA: Aprendizaje automático adversario	Ciberataque	Seguridad de sistemas distribuidos	Ciberataques masivos a sistemas de información
Basados en Sistemas de Seguridad: Seguridad del sistema Android	Cibercrimen	Seguridad de datos	Aspectos operativos de Ciberdefensa y Ciberseguridad
Base de datos de conocimiento compartible	Ciberdefensa	Seguridad de sistemas industriales	Principios y enfoques de diseño de software seguro
Bases de datos verificables y computación en la nube segura	Comunicaciones seguras	Privacidad de la información	Proyecto sobre principios y enfoques de diseño de software seguro
Cadena de bloques	Contratos inteligentes	Políticas de seguridad	Teoría organizacional y psicología organizacional
Clasificación del tráfico de Internet	Control de acceso	Seguridad en sistemas autónomos	Diseño y desarrollo de la "Data Exchange Layer" en ambientes de gobierno
Computación Segura	Criptografía	Seguridad de redes inalámbricas	Data Mining – Data warehousing Big Data
Configuración de red segura	Desarrollo seguro	Seguridad de la información en salud	Tecnología de redes
Control de acceso y autorización	Fintech	Seguridad en sistemas de control	Seguridad en redes de computadoras
Criptografía	Firma digital	Seguridad en vehículos autónomos	Talleres de Investigación Supervisada y/o Tutoriales en Aspectos Operativos de Ciberdefensa y Ciberseguridad
Criptografía aplicada: computación segura	Forense digital	Seguridad en la información biométrica	Introducción a la Seguridad Informática
Criptografía con funcionalidad avanzada	Gestión y Administración de la Ciberseguridad	Seguridad en redes sociales	Criptografía
Criptografía teórica y aplicada	Gobierno de la seguridad de TI	Amenazas cibernéticas	Gestión, Auditoría y Normas de Seguridad
Delitos cibernéticos	Hardware seguro	Protección contra ataques de phishing	Seguridad en Redes
Desarrollo de técnicas de protección y prevención de ataques	Infraestructuras criticas	Seguridad en el internet de las cosas (IoT)	Forensia Informática Aplicada
Detección avanzada de malware	Ingeniería de seguridad	Identificación y autenticación de usuarios	Criptografía Avanzada
Detección de ataques internos	Inteligencia artificial	Análisis de datos de seguridad	Criptografía Aplicada
Detección de spam en Twitter	Iot	Seguridad en sistemas operativos	Régimen Legal del Manejo de Datos
Detección de vulnerabilidades de seguridad del sistema basada en el análisis de programas de código fuente y binario	Libros de contabilidad distribuidos	Seguridad en sistemas de inteligencia artificial	Implementaciones de seguridad en distintos sistemas operativos
Detección de vulnerabilidades de software	Machine learning	Seguridad en sistemas de aprendizaje automático	Software Aplicativos
Diseño de Software	Malware	Seguridad en sistemas de blockchain	Seguridad en Redes Inalámbricas
El aprendizaje federado (FL)	Minería de Datos	Protección contra malware y virus	Seguridad de la Información en las Redes de Defensa
El mecanismo de privacidad diferencial (DP)	Principios de seguridad	Detección de intrusos	Introducción a la Ciberdefensa
Evaluación de amenazas cibernéticas	Privacidad	Seguridad en la nube híbrida	Infraestructuras críticas
Evaluación de riesgos en sistemas ciberfísicos	Privacidad de datos	Seguridad de aplicaciones web	Metodología de la investigación
Garantía de seguridad basada en IA	Privacidad de la informacion	Seguridad en sistemas SCADA	Identificación de Riesgos y Amenazas
Gestión de claves de seguridad	Protocolos seguros	Seguridad en la red 5G	Mecanismos de ciberdefensa
Informática de confianza	Redes y servicios seguros	Seguridad en sistemas de automatización industrial	Defensa en Sistemas Distribuidos
Ingeniería inversa binaria basada en el aprendizaje	Seguridad de la informacion	Seguridad en sistemas de gestión de identidad y acceso	Comando y control de la Ciberdefensa
Integridad de los datos del sensor	Seguridad en aplicaciones	Análisis de amenazas	Ciberdefensa aplicada
Internet de las cosas (iot) y seguridad de sistemas cibernéticos (CPS)	Seguridad en aplicaciones distribuidas	Seguridad en la cadena de suministro	
Investigación de Defensa Cibernética	Seguridad en comunicaciones	Seguridad en sistemas de defensa	
	Seguridad en la nube	Seguridad en sistemas de energía inteligente	
	Seguridad en redes	Seguridad en sistemas de transacciones financieras	
	Seguridad en sistemas	Seguridad en sistemas de IoT industrial	
	Seguridad en sistemas distribuidos	Seguridad en sistemas de realidad virtual y aumentada	
	Seguridad y privacidad de los datos	Protección de la privacidad en la nube	
	Sgsi		
	Sistemas de seguridad		

Investigación Forense Digital Iot Sociedad 5.0 Los esquemas de cifrado homomórfico (HE) Los esquemas de computación de múltiples partes (MPC) Los esquemas Symmetric Searchable Encryption (SSE) Phishing y el fraude Pointee integrity Política de Seguridad Cibernética Predicción y descubrimiento de incidentes de seguridad Privacidad Privacidad y seguridad móvil Producto de investigación: Investigación de seguridad en sistemas de almacenamiento en la nube Producto de investigación: Investigación de vulnerabilidades en dispositivos móviles y aplicaciones Productos y Sistemas Psico-ciberseguridad para Sistemas Redes de anonimato y técnicas de mejora de la privacidad Seguridad basada en lenguaje Seguridad cibernética Seguridad de hardware Seguridad de infraestructura y experimentación Seguridad de la cadena de bloques Seguridad de la información Seguridad de redes y protocolos Seguridad del sistema distribuido Seguridad del sistema Explanalbe Seguridad del sistema operativo Seguridad en dispositivos móviles y aplicaciones Seguridad en la nube Seguridad fintech Seguridad multimedia y análisis forense Seguridad para IA Seguridad web y privacidad Seguridad y análisis de software Seguridad y Privacidad Sistema Blockchain aplicado. Sistemas de aprendizaje automático confiables y confidenciales Sistemas de exploración de vulnerabilidades del kernel del sistema operativo Sistemas Redes Técnicas de mitigación de exploits en tiempo de ejecución Tecnologías de privacidad	Software seguro Tendencias en ciberseguridad Gestión de riesgos Analítica de datos Computación distribuida Computación ubicua Derecho informático Gestión de datos seguros Gestión incidentes Hacking ético Identificación Autenticación Gestión de acceso Informacion cuántica Protección de datos Seguridad física Esteganografía Estegoanálisis Verificación	Seguridad en la inteligencia de amenazas Seguridad en los sistemas de mensajería instantánea Seguridad en la red de sensores Seguridad en sistemas de geolocalización Seguridad en sistemas de drones Seguridad en sistemas de robótica Seguridad en sistemas de inteligencia de negocios Seguridad en sistemas de vehículos conectados Seguridad en sistemas de telemedicina Seguridad en sistemas de educación en línea Seguridad en sistemas de realidad mixta Seguridad en sistemas de computación en la nube Seguridad en sistemas de televisión inteligente Seguridad en sistemas de smart cities Seguridad en sistemas de automatización de hogares Seguridad en sistemas de criptomoneda Seguridad en sistemas de e-commerce Seguridad en sistemas de inteligencia artificial en la salud Seguridad en sistemas de vehículos autónomos aéreos Seguridad en sistemas de voz asistida Seguridad en sistemas de almacenamiento en la nube Seguridad en sistemas de computación cuántica Seguridad en sistemas de predicción de comportamiento del usuario Seguridad en sistemas de reconocimiento facial Seguridad en sistemas de tecnología vestible Seguridad en sistemas de redes de sensores inalámbricos Seguridad en sistemas de tecnología de la información en la agricultura Seguridad en sistemas de tecnología de la información en la energía renovable Seguridad en sistemas de tecnología de la información en el transporte Seguridad en sistemas de tecnología de la información en la industria alimentaria Seguridad en sistemas de tecnología de la información en la logística Seguridad en sistemas de tecnología de la información en la construcción Seguridad en sistemas de tecnología de la información en la moda y la belleza Seguridad en sistemas de tecnología de la información en el deporte Seguridad en sistemas de tecnología de la información en el arte y la cultura. Seguridad en sistemas de predicción de comportamiento del usuario	Introducción a la Seguridad Informática Criptografía Gestión Auditoría y Normas Seguridad en Redes Forensia Informática Aplicada Criptografía Avanzada Criptografía Aplicada Régimen Legal del Manejo de Datos Implementaciones de Seguridad en Distintos Sistemas Operativos Software Aplicativos Seguridad en Redes Inalámbricas Seguridad e la Información en las Redes de Defensa Introducción a la Ciberdefensa Metodologías de Tesis Infraestructuras críticas Mecanismos de ciberdefensa Identificación de Riesgos y Amenazas Defensa en Sistemas Distribuidos Comando y control de la ciberdefensa Ciberdefensa aplicada Trabajo Final Integrador Análisis de algoritmos Cómputo móvil Criptografía Inteligencia artificial Minería de datos Seguridad de información Seguridad de Redes Seguridad avanzada en redes Técnicas de seguridad en software Técnicas de seguridad en entornos informáticos Seguridad Informática e Implementación en la Empresa Seguridad informática en la empresa Seguridad de los sistemas de información Seguridad y protección de la información Criptografía Firewalls Hardward y Software Robustecimiento de sistemas Identificación de servicios Organización de la Seguridad de la Información Confianza, seguridad y sociedad de la información Tecnología y organización de la información La infraestructura para la construcción de confianza Marco normativo y regulatorio de la seguridad y del comercio electrónico Ciberseguridad, Criptografía y Delitos Telemáticos Seguridad de comunicaciones y criptografía Hacking, malware y DDOS

Teléfonos inteligentes digitales Teoría de la codificación y criptografía Teoría de la Computación Teoría de la criptografía Uso de modelos de falla y método bayesiano para la predicción de fallas en tiempo real y la gestión de la incertidumbre Verificación de seguridad funcional de los sistemas que implementan IA Visualización de seguridad cibernética. Visualización y modelado de datos para Procesos Vscape Vulnerabilidades		Seguridad en sistemas de reconocimiento facial Seguridad en sistemas de tecnología vestible Seguridad en sistemas de redes de sensores inalámbricos Seguridad en sistemas de tecnología de la información en la agricultura Seguridad en sistemas de tecnología de la información en la energía renovable Seguridad en sistemas de tecnología de la información en el transporte Seguridad en sistemas de tecnología de la información en la industria alimentaria Seguridad en sistemas de tecnología de la información en la logística Seguridad en sistemas de tecnología de la información en la construcción Seguridad en sistemas de tecnología de la información en la moda y la belleza Seguridad en sistemas de tecnología de la información en el deporte Seguridad en sistemas de tecnología de la información en el arte y la cultura.	Hardening y seguridad de la información Auditoría y detección de intrusos Delitos tipificados y fichas de delitos telemático Teoría de redes Protocolo TCP/IP Técnicas de seguimiento, exploración y enumeración Exploración del objetivo Tipos de ataques TCP/IP Debilidad de los protocolos TCP/I Ataques A Redes Inalámbricas Métodos De Penetración WIFI Introducción y conceptos previos a los métodos de penetración WIFI Parámetros de estudio estructural y topología de Redes Inalámbricas Equipos inalámbricos WIFI utilizar y realización de rastreos sobre posibles víctimas Fase de ataque a una red inalámbrica Técnicas y Herramientas de Protección de Redes para las Empresas Protección en nivel de red Ataques a redes e intrusiones Protección de sistemas Servidores big data y datos streaming Impacto tecnologías big data en protección de datos La Ciberseguridad desde el Ámbito Judicial Derechos y código deontológico del perito informático Evidencias digitales y judiciales Organismos internacionales en ciberseguridad Organismos nacionales relacionados con la ciberseguridad Aspectos legales y regulatorios en ciberseguridad La regulación en protección de datos Análisis y Auditoría Forense Metodología del cibercrimen Evaluación de la Situación Adquisición de Evidencias Análisis de Evidencias Informe de Investigación Auditoría del Sistema de Seguridad Desarrollo de un plan de políticas de seguridad informática Auditoría del sistema de seguridad y análisis de riesgos Norma ISO/IEC 27001 e implantación de un modelo SGSI Cumplimiento y gestión de la seguridad Gestión del riesgo Indicadores de riesgo tecnológico Infraestructuras Críticas Sistemas de prestación de servicios

			Líneas de acción estratégicas Los instrumentos de planificación Sistema nacional de protección de infraestructuras Exposición de las Pymes a los Ciberataques Vulnerabilidad de la PYMES Protección contra los ciberataques en las PYMES Métodos de seguridad para combatir ciberataques Mejora de la seguridad de la PYMES Preparación para la Investigación La investigación científica Tipos de investigación y diseños de investigación Métodos de investigación Técnicas de investigación Planteamiento del problema y elaboración del marco teórico Formulación de hipótesis y selección de la muestra Recolección de datos Análisis de datos Gestión de la seguridad Seguridad en sistemas operativos, software, aplicaciones online y bases de datos Aspectos legales y regulatorios Análisis de riesgos legales Criptografía y mecanismos de seguridad Delitos informáticos Seguridad en redes y análisis de vulnerabilidades Ciberseguridad y Análisis Forense Digital Auditoría de la seguridad

En el análisis realizado a la información que contiene la tabla anterior, se establece las palabras claves las cuales orientan la necesidad de las regiones en el contexto de la ciberseguridad. A continuación, se presentan las 50 palabras más relevantes por zona geográfica:

Asia	Europa	Norte América	Latino América
IA, Servicio de Información, Análisis de malware, Investigación de ataques, Análisis de vulnerabilidades, Contratos inteligentes, Aprendizaje automático, Seguridad de IA, Ataques de canal lateral, Criptoanálisis, Autenticación, Biometría, Cadena de bloques, Android, Bases de datos, Computación en la nube, Clasificación de tráfico, Configuración de red segura, Control de acceso, Autorización, Criptografía, Delitos cibernéticos, Prevención de ataques, Detección avanzada de malware, Detección de ataques internos, Detección de spam, Análisis de programas, Vulnerabilidades de software, Diseño de software, Aprendizaje federado, Privacidad diferencial, Evaluación de amenazas, Riesgos ciberfísicos, Seguridad basada en IA, Gestión de claves, Informática de confianza, Ingeniería inversa, Integridad de datos, IoT, Defensa cibernética, Forense digital, Sociedad 5.0, Cifrado homomórfico, Computación de múltiples partes, Búsqueda simétrica, Phishing, Fraude, Pointee integrity, Política de seguridad, Descubrimiento de incidentes, Privacidad, Seguridad móvil, Almacenamiento en la nube, Vulnerabilidades en dispositivos móviles, Productos y sistemas, Psico-ciberseguridad, Redes de anonimato, Seguridad basada en lenguaje, Seguridad de hardware, Infraestructura, Explanalbe, Sistema operativo, Seguridad web, Análisis de software, Privacidad en línea, Blockchain aplicado, Aprendizaje automático confiable, Exploración de vulnerabilidades, Mitigación de exploits, Tecnologías de privacidad, Teléfonos inteligentes, Codificación, Fallas en tiempo real, Verificación de seguridad, Visualización de seguridad, Modelado de datos, Vscape, Vulnerabilidades.	algorítmica, seguridad empresarial, seguridad de la información, ciberseguridad, amenazas persistentes, auditoría de seguridad, blockchain, ciberataque, cibercrimen, ciberdefensa, comunicaciones seguras, contratos inteligentes, control de acceso, criptografía, desarrollo seguro, fintech, firma digital, forense digital, gestión de la ciberseguridad, gobierno de la seguridad de TI, hardware seguro, infraestructuras críticas, ingeniería de seguridad, inteligencia artificial, IoT, libros de contabilidad distribuidos, machine learning, malware, minería de datos, principios de seguridad, privacidad, privacidad de datos, privacidad de la información, protocolos seguros, redes y servicios seguros, seguridad en aplicaciones, seguridad en aplicaciones distribuidas, seguridad en comunicaciones, seguridad en la nube, seguridad en redes, seguridad en sistemas, seguridad en sistemas distribuidos, seguridad y privacidad de los datos, SGSI, sistemas de seguridad, software seguro, tendencias en ciberseguridad, gestión de riesgos, analítica de datos, computación distribuida, computación ubicua, derecho informático, gestión de datos seguros, gestión de incidentes, hacking ético, identificación, autenticación, gestión de acceso, información cuántica, protección de datos, seguridad física, esteganografía, estegoanálisis, verificación algorítmica	Ciberseguridad, Protección de datos, Análisis de vulnerabilidades, Ataques informáticos, Amenazas de seguridad, Privacidad en línea, Criptografía, Seguridad en la nube, Autenticación, Seguridad en dispositivos móviles, Riesgos de seguridad, Gestión de riesgos, Auditoría de seguridad, Seguridad de la red, Prevención de intrusiones, Seguridad de los sistemas operativos, Gestión de incidentes de seguridad, Seguridad en el Internet de las cosas (IoT), Seguridad de redes inalámbricas, Seguridad en el comercio electrónico, Seguridad en la banca en línea, Seguridad en pagos móviles, Protección contra el malware, Seguridad de aplicaciones, Análisis de tráfico de red, Detección de amenazas, Seguridad en sistemas de control industrial, Seguridad en sistemas SCADA, Ciberinteligencia, Análisis de comportamiento de usuario, Gestión de identidad y acceso, Seguridad en sistemas de telecomunicaciones, Pruebas de penetración, Protección de la propiedad intelectual, Gestión de seguridad de la información, Seguridad en sistemas de salud, Seguridad en sistemas educativos, Seguridad en sistemas financieros, Seguridad en sistemas gubernamentales, Seguridad en sistemas militares, Seguridad en sistemas aeroespaciales, Seguridad en sistemas de transporte, Seguridad en sistemas de energía, Seguridad en sistemas de agua, Seguridad en sistemas de manufactura, Seguridad en sistemas de comercio, Seguridad en sistemas de entretenimiento, Seguridad en sistemas de medios de comunicación, Seguridad en sistemas de turismo, Seguridad en sistemas de servicios de consultoría.	Tecnología de la información, ética y normativa jurídica, gerenciamiento innovador, entrepreneurship, paradigmas de programación, criptología, tecnología militar, enfoque "Network-Centric Warfare", redes informáticas, malware, ciberataques masivos, ciberdefensa, seguridad de software, diseño de software seguro, teoría organizacional, psicología organizacional, Data Exchange Layer, gobierno electrónico, data mining, data warehousing, big data, seguridad en redes, investigación supervisada, tutoriales en ciberseguridad, criptografía, gestión de seguridad, auditoría de seguridad, normas de seguridad, forensia informática, régimen legal del manejo de datos, implementaciones de seguridad, sistemas operativos, software aplicativos, redes inalámbricas, infraestructuras críticas, identificación de riesgos, amenazas, mecanismos de defensa, sistemas distribuidos, comando y control, trabajo final integrador, análisis de algoritmos, cómputo móvil, inteligencia artificial, minería de datos, técnicas de seguridad en software y entornos informáticos, seguridad informática en la empresa, protección de sistemas de información, firewalls, robustecimiento de sistemas, organización de seguridad de la información, confianza, sociedad de la información, normativa de seguridad y comercio electrónico, delitos telemáticos, hacking, DDOS, hardening, auditoría y detección de intrusos, teoría de redes, protocolo TCP/IP, seguimiento, exploración y enumeración, debilidades de protocolos TCP/IP, ataques a redes inalámbricas, métodos de penetración WIFI, herramientas de protección de redes, servidores big data y datos streaming, ciberseguridad en el ámbito judicial, derechos y código deontológico del perito informático, evidencias digitales y judiciales, organismos internacionales de ciberseguridad.

Ilustración 13: Análisis de palabras usando herramientas de análisis textual para la zona geográfica asiática

Total: 193 palabras analizadas

Elaboración propia

Ilustración 14: Análisis de palabras usando herramientas de análisis textual para la zona geográfica Europea

Total: 155 palabras analizadas

Elaboración propia

Ilustración 15: Análisis de palabras usando herramientas de análisis textual para la zona geográfica de Norte América

Elaboración propia

Ilustración 16: Análisis de palabras usando herramientas de análisis textual para la zona geográfica Latinoamericana

Total: 211 palabras analizadas

Elaboración propia

Respecto a la visión organizacional, se consultan los planes estratégicos de organizaciones representativas en esta disciplina, obteniendo a partir del análisis de la información recolectada, las siguientes líneas de acción que se plantean para los siguientes cinco años.

Marco NICE	Política de ciberseguridad	Colaboración y cooperación	Ciberdefensa	Investigación y concientización
Desarrollo de capacidades Gestión de talentos Prácticas laborales Brechas de habilidades Promoción de carreras Aprendizaje transformador Diversidad y	Estrategia Nacional de Ciberseguridad Plan de acción Comité Directivo Proceso formal Evaluación y seguimiento Evaluación del panorama de riesgo	Cooperación interinstitucional Unificación de agencias Autoridad líder del proyecto Partes interesadas Empoderamiento de comunidades	Reducción de riesgos Resiliencia operacional Prevención de ciberataques Escudo único para la administración	Impulsar la investigación efectiva Concientización sobre riesgos cibernéticos Protección de infraestructura crítica Gobernanza y respuesta a incidentes de seguridad

capacitación	cibernético Evaluación del resultado de la estrategia Seguimiento del progreso de la implementación			

Las organizaciones en el orden mundial están alineadas con lo planteado por el Índice Global de Ciberseguridad[15]. En sus planes estratégicos para los siguientes años se plantea el desarrollar capacidades en términos legales, técnicos, estratégicos, organizaciones, de desarrollo de capacidades y de cooperación. En este sentido el CSIRT Académico UNAD soportado por la línea de investigación en Ciberseguridad establece sus objetivos en busca de desarrollo de capacidades que contribuyan en la construcción de políticas y reglamentas relacionados con ciberseguridad, en el desarrollo de capacidades técnicas y estratégicas articuladas con organizaciones internacionales, nacionales y sectoriales y en el desarrollo de campañas de concienciación de formación y educación en Ciberseguridad.

[15] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/

Objetivos de la línea de investigación

Objetivo General

Desarrollar estrategias efectivas y sostenibles que contribuyan en la construcción del conocimiento de la disciplina de la Ciberseguridad a partir de la ejecución de proyectos de I+D+i articulados a los grupos y semilleros de investigación mediante la investigación formativa

Objetivos Específicos

- Elaborar documentos exhaustivos relacionados con tendencias y avances en ciberseguridad, con el fin de identificar áreas de investigación relevantes y desarrollar nuevos enfoques que contribuyan a la construcción del conocimiento en esta disciplina.
- Analizar datos recopilados en los procesos de I+D+i y de experimentación para identificar patrones, tendencias, y desarrollo de modelos predictivos que puedan ayudar a prevenir y detectar amenazas futuras con el fin de llevar a cabo validaciones para la generación de diferentes soluciones para la Ciberseguridad.
- Desarrollar productos y servicios basados en los resultados de I+D+i, con el fin de brindar soluciones prácticas y efectivas en la disciplina de la Ciberseguridad teniendo presente necesidades específicas de las partes interesadas con el fin de contribuir en el desarrollo regional.
- Generar espacios para el desarrollo de capacidades de ciberseguridad a partir del fortalecimiento del talento humano y la integración de los procesos de I+D+i que se generan desde las escuelas de la UNAD y las partes interesadas para la difusión o divulgación de nuevo conocimiento.

Línea de investigación: **Ciberseguridad**

Temas de investigación	Descripción	Tópicos
Ciberseguridad estratégica	Desarrollo de técnicas de análisis de riesgos y amenazas, incluyendo el análisis de vulnerabilidades y el análisis de incidentes de seguridad para comprender mejor las amenazas y los riesgos en el ámbito cibernético.	• Sistemas De Gestión de Seguridad de la Información • Peritaje e informática forense • Derecho digital • Vigilancia tecnológica en Ciberseguridad • Métricas en Ciberseguridad
Ciberseguridad Operativa	Investigación de técnicas para fortalecer la seguridad de los sistemas informáticos y de redes, incluyendo el uso de criptografía y tecnologías de autenticación avanzada.	• Aseguramiento en sistemas operativos (Escritorio, server, móvil) • Firmas digitales • Aseguramiento de dispositivos digitales de comunicación • Herramientas FOSS para Ciberseguridad
Ciberseguridad Operativa	Desarrollo de tecnologías de protección de datos y privacidad, incluyendo la encriptación y el control de acceso a los datos.	• Seguridad en aplicaciones (Escritorio, web, móvil) • Desarrollo de software seguro • Seguridad en la nube • Sistemas de monitores • Sistemas de respuesta y contención • Aseguramiento basado en biometría
Desarrollo de capacidades	Investigación de técnicas de gestión de riesgos y de seguridad, incluyendo el desarrollo de políticas y protocolos de seguridad para garantizar la integridad de los datos y la privacidad de los usuarios.	• Fortalecimiento de la seguridad de los activos de información • Gestión y tratamiento de los datos
Desarrollo de capacidades	Desarrollo de técnicas avanzadas de detección y respuesta ante amenazas cibernéticas, incluyendo el uso de inteligencia artificial y aprendizaje automático para detectar patrones y comportamientos sospechosos en tiempo real.	• Metodologías de análisis de riesgo • Metodologías de pruebas de penetración • Desarrollo de técnicas de threat hunting
Desarrollo de capacidades	Estudio de la dimensión humana de la ciberseguridad, incluyendo la educación y concientización sobre ciberseguridad, la psicología de los usuarios y la identificación de los factores humanos que contribuyen a la exposición a las amenazas cibernéticas.	• Cyber crimen • Educación y cultura en Ciberseguridad • Riego Psicosocial enfocado en Ciberseguridad • RI5 • Ingeniería social • Seguridad en identidad digital
Desarrollo de capacidades - operativa - estratégica	Estudio de las amenazas (zero day) y los riesgos asociados con las tecnologías emergentes, como el Internet de las cosas (IoT), la inteligencia artificial (IA) y la tecnología blockchain.	• Criptografía • Análisis de malware • Inteligencia artificial aplicada a Ciberseguridad • Blockchain aplicado a Ciberseguridad • Desarrollo de HW y SW aplicado a Ciberseguridad • Tecnologías emergentes • Internet (IoT, IoP, IoX) aplicado a la Ciberseguridad • Infraestructura crítica • Aseguramiento para implementación digital en la industria • Ciberseguridad cuántica

Transdisciplinariedad de la línea de investigación en Ciberseguridad

(Sanchez, 2022)indica que "*lejos de querer convertir en un absoluto la transdisciplinariedad, considero que la universidad del SXXI debe iniciar un acercamiento más decidido y juicioso a cualquier concepto, metodología, idea, etc., que permita avanzar y dejar atrás las miradas unidisciplinarias que funcionaron en su correspondiente momento histórico, pero que ahora resultan inconvenientes para la generación de nuevo conocimiento. La universidad necesita avanzar orientando su quehacer en función de nuevos paradigmas y enfoques que busquen reducir el espacio de incertidumbre de estos tiempos y de los que habitamos en estos tiempos como agentes generadores del cambio Dado que ACM plantea a la Ciberseguridad como una Disciplina del conocimiento y que está repercute*".

Lo anterior soporta la importancia de la generación del nuevo conocimiento en Ciberseguridad visto no solamente desde esta disciplina; sino desde la construcción de un conocimiento con un enfoque holístico y que pueda integrarse con diversos saberes humanos. En este sentido la transdisciplinariedad de la línea de investigación en Ciberseguridad aporta en la construcción del conocimiento en diversas áreas de la investigación, tal como se ve en la siguiente ilustración:

Ilustración 17: Transdisciplinariedad de la línea de investigación con la Ciberseguridad

Elaboración propia

La ilustración anterior muestra la interrelación que presenta la disciplinad e la ciberseguridad con algunas disciplinas del conocimiento. En este sentido cada uno de los subtemas puede tener como fin:

Tecnología: La investigación y el desarrollo de tecnologías de ciberseguridad son fundamentales para mejorar la seguridad de los sistemas informáticos. Al diseñar algoritmos de encriptación y herramientas de análisis de vulnerabilidades, se pueden detectar y prevenir posibles ataques cibernéticos, lo que garantiza la seguridad de la información y la protección de los sistemas informáticos.

Derecho digital, moral y la ética: El marco legal y ético en ciberseguridad es importante para garantizar el cumplimiento de las leyes y las normas de ciberseguridad. La investigación en esta disciplina del conocimiento y la ética en el uso y tratamiento de la información obtenida en investigaciones de ciberseguridad son cruciales para asegurar que la ciberseguridad se aborde de manera responsable.

Psicología: El comportamiento humano respecto a la ciberseguridad es un factor clave a considerar en la protección de los sistemas informáticos. Al comprender cómo los usuarios interactúan con los sistemas, se pueden identificar patrones de comportamiento y desarrollar medidas de seguridad adecuadas para prevenir ataques o incidentes.

Cooperación y alianzas (comunicaciones): La comunicación en situaciones de crisis de ciberseguridad es crucial para una respuesta efectiva y rápida respuesta. Al analizar la comunicación entre equipos de respuesta a incidentes de ciberseguridad y desarrollar herramientas de comunicación en situaciones de crisis, se puede garantizar una respuesta adecuada y oportuna para minimizar los efectos de los ciberataques.

Negocios: Los riesgos empresariales en ciberseguridad son un factor crítico en la protección de los sistemas informáticos. Al analizar los riesgos empresariales asociados con la ciberseguridad y desarrollar planes de contingencia para empresas en caso de incidentes de ciberseguridad, se puede garantizar la continuidad del negocio y minimizar las pérdidas económicas.

Ingeniería: La infraestructura de ciberseguridad es fundamental para proteger los sistemas informáticos. Al diseñar redes seguras y analizar vulnerabilidades en sistemas industriales o infraestructuras críticas, se puede garantizar la seguridad de los sistemas y la protección de la información.

Medicina: La seguridad en sistemas de salud es un tema crítico, ya que la información médica es extremadamente sensible. Al analizar la seguridad de los sistemas de información en salud y desarrollar medidas de seguridad para proteger la información médica, se puede garantizar la privacidad y confidencialidad de los pacientes.

Educación: La formación en ciberseguridad es esencial para crear una cultura respecto a la buena gestión de la información. Al diseñar programas educativos en ciberseguridad e

identificar necesidades de formación en ciberseguridad para diferentes sectores de la sociedad, se puede fomentar una cibercultura y mejorar la seguridad de los entornos digitales.

Transformación social: La ciberseguridad no puede abordarse únicamente desde una perspectiva tecnológica, sino que también es necesario comprender la naturaleza social y psicológica de las amenazas cibernéticas. La transdisciplinariedad de la ciberseguridad con la transformación social implica el diálogo entre diferentes disciplinas para abordar los desafíos de manera integral y colaborativa.

Vigilancia tecnológica: La ciberseguridad y la vigilancia tecnológica son dos disciplinas que están estrechamente relacionadas, ya que ambas se enfocan en la protección de los activos digitales. Aunque son disciplinas distintas, la transdisciplinariedad entre ellas es fundamental para lograr una gestión efectiva de los riesgos tecnológicos. La ciberseguridad se enfoca en la protección de los sistemas, redes y dispositivos de las amenazas cibernéticas, como virus, malware, phishing y otros ataques. Por otro lado, la vigilancia tecnológica se enfoca en una permanente identificación, seguimiento y análisis de la información relevante para el negocio, con el fin de tomar decisiones informadas y anticiparse a los riesgos y oportunidades tecnológicas.

Metas previstas

La línea de investigación en Ciberseguridad se propone como metas previstas los productos relacionados con

Tabla 7: Productos derivados de la línea de investigación, según Acuerdo 005 de 2016

Producto	Resultado
Generación de nuevo conocimiento	Libros o capítulo de libro Artículo s en revistas especializadas Productos tecnológicos patentados o en proceso de concesión de patente
Desarrollo tecnológico e innovación	Productos tecnológicos certificados o validados Productos empresariales Regulaciones Normas Reglamentos Legislaciones Consultorías científico-tecnológicas Informes técnicos finales
Apropiación social y de circulación del conocimiento	Participación ciudadana Intercambio y transferencia del conocimiento Comunicación del conocimiento Circulación del conocimiento especializado
Formación del recurso humano	Tesis de doctorado Trabajos de grado de maestría Trabajos de pregrado Proyectos de I+D+i con formación Apoyo a programas en formación
Desarrollo de capacidades en ciberseguridad	Desarrollo de Software o Hardware enfocado en ciberseguridad Informes técnicos Informes estadísticos Políticas, procesos y procedimientos Implementación de infraestructura lógica enfocada en ciberseguridad

Recuperado de:
https://investigacion.unad.edu.co/images/investigacion/ACUERDO_005_2016_04_19_LINEAS_DE_INVESTIGACIN_1.pdf

*Para dar cumplimiento a las metas propuestas por la línea de investigación, se tendrá presente el plan de trabajo, una vez aprobada por el comité de investigación de la ECBTI

Alianzas interinstitucionales

En el ejercicio de generar espacios de cooperación y alianzas interinstitucionales que promuevan la generación, difusión y divulgación de nuevo conocimiento, la línea de investigación en Ciberseguridad se propone realizar alianzas internas y externas que permitan dar cumplimiento a su objetivo general teniendo presente las partes interesadas que se relacionan en la siguiente tabla:

Contexto	Descripción	Parte interesada
Político y legal	El contexto político y legal influye en la línea de investigación, ya que las leyes y regulaciones varían entre países y regiones y pueden impactar en el desarrollo de los proyectos de I+D+i.	Min de Educación MinTIC Superintendencia de industria y comercio
Económico y Financiero	Con el fin de identificar las organizaciones que deben o pueden asignar los recursos adecuados para el desarrollo de proyectos de I+D+i	Clientes y proveedores Partes interesadas Organizaciones gubernamentales y no gubernamentales
Cultural y Social	El contexto cultural influye en las actitudes y valores de los investigadores y de sus partes interesadas respecto al cumplimento ético de sus acciones	Aspirantes Estudiantes Egresados Proveedores Comunidades que la Universidad impacta Equipos de respuesta a incidentes informáticos Reguladores y autoridades gubernamentales Instituciones de educación Superior Redes y comunidades de Investigación en Ciberseguridad (REDCIC, Sociedad Colombiana de Computación)
Tecnológico	Es importante conocer y entender la tecnología utilizada por la Universidad, para poder Desarrollar proyectos de I+D+i.	Proveedores (EC-Council, CISCO, Oracle Academy) GPIT ECBTI VIEM Otras escuelas Comunidades públicas y privadas de ciberseguridad

Bibliografía

Bosworth, kabay, & Whiney. (2014). Retrieved from Computer Security Handbook, Set, 6th Edition: https://www.wiley.com/en-us/Computer+Security+Handbook%2C+Set%2C+6th+Edition-p-9781118127063

Brooks, C. (2022). *Cybersecurity Trends & Statistics For 2023; What You Need To Know.* Retrieved from https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=2b64fa5619db

CEPAL. (2022). *Tecnologías digitales para un nuevo futuro.* Retrieved from https://repositorio.cepal.org/bitstream/handle/11362/46816/1/S2000961_es.pdf

Fischer, IMgrund, Janiesch, & Winkelmann. (2020). *SienceDirect.* Retrieved from Strategy archetypes for digital transformation: Defining meta objectives using business process management: https://doi.org/10.1016/j.im.2019.103262

ISO. (2022). *ISO/IEC 27001:2013.* Retrieved from Information technology — Security techniques — Information security management systems — Requirements: https://www.iso.org/standard/54534.html

ITU. (2022). *Programa de Ciberseguridad del UIT-D ndice de Ciberseguridad Global – GCIv5.* Retrieved from ITU: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/513560_2S.pdf

Kaur, & Ramkumar. (2022). Retrieved from The recent trends in cyber security: A review: https://www.sciencedirect.com/science/article/pii/S1319157821000203

li, & liu. (2021). *ElSevier.* Retrieved from A comprehensive review study of cyber-attacks and cyber security;: https://pdf.sciencedirectassets.com/311225/1-s2.0-S2352484720X00072/1-s2.0-S2352484721007289/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEDkaCXVzLWVhc3QtMSJIMEYCIQD59Aec12nHEIqTA0W0ZdheEHqbszd5zIUvgIkOM7g7%2BAIhAJNcl2%2BUTSMbyFkzrKvwzbdyM6VMD447CbcBiT%2

NICE. (2020). *Nist.* Retrieved from National Initiative for cybersecurity education: https://www.nist.gov/system/files/documents/2020/10/26/2012_NICE-strategic-plan_withcover.pdf

Peñuela. (2005). *Scielo.* Retrieved from La transdisciplinariedad. Más allá de los conceptos, la dialéctica: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-00632005000300003

Rwat, Doku, & Garuba. (2021). *IEEE.* Retrieved from Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security: https://ieeexplore.ieee.org/document/8673585

Sanabria, & Ospina. (2020). *SCielo.* Retrieved from Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199

Sanchez. (2022). *La Importancia de la Transdisciplina en el Desarrollo de los Proyectos de Investigación-Acción.* Retrieved from Universidad Polito de Colombia: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/11799/La%20Importancia%20de%20la%20Transdisciplina%20en%20el%20Desarrollo%20de%20los%20Proyectos%20de%20Investigaci%C3%B3n-Acci%C3%B3n%20Educativa%20del%20Programa%20de%20Fotograf%C3%ADa%20p

SienceDirect. (2018). *ELSEVIER.* Retrieved from Future Generation Computer Systems: https://www.sciencedirect.com/science/article/abs/pii/S0167923605001144?via%3Dihub

Singer, & Friedman. (2017). *Oxford.* Retrieved from Cybersecurity and Cyberwar: https://global.oup.com/academic/product/cybersecurity-and-cyberwar-9780199918119?cc=co&lang=en&#

Sonicawall. (2023). Retrieved from CHARTING CYBERCRIME'S: https://www.sonicwall.com/medialibrary/en/white-paper/2023-cyber-threat-report.pdf

UNAD. (2019). *Acuerdo 039.* Retrieved from https://sgeneral.unad.edu.co/images/documentos/consejoSuperior/acuerdos/2019/COSU_ACUE_039_20190312.pdf

Anexo 1.

Cadena	Línea de Investigación	Temáticas	SI	NO
Sistemas	Ingeniería del Software	Técnicas y metodologías de análisis y diseño		X
		Sistemas inteligentes		X
		Desarrollo de soluciones de software de calidad		X
		Tecnología para la educación		X
	Gestión de sistemas	Gestión del conocimiento		X
		Auditoria de sistemas	X	
		Cibernética organizacional	X	
		Administración de tecnología	X	
ETR	Infraestructura tecnológica y seguridad en redes	Gestión de redes de telecomunicaciones		X
		Arquitectura, protocolos y plataformas	X	
		Aplicaciones adaptativas en redes de comunicaciones heterogéneas		X
		Computación móvil		X
	Automatización y herramientas lógicas	Acondicionamiento de señales		X
		Metrología		X
		Instrumentación vial		X
		Instrumentación aplicada		X
		Automatización de procesos		X
		Robótica		X
ETR Actualizada	Electrónica, automatización y robótica	Instrumentación electrónica	No aplica actualmente	
		Laboratorio (personal y remoto)		
		Manufactura avanzada		
		Automatización y control		
		Sistemas dinámicos		
		Microelectrónica y nanoelectrónica		
		Semiconductores		
		Robótica		
		Pensamiento deseñales y de imágenes		
		Diseño electrónico		
		Interface humano-maquina		
	Infraestructura tecnológica y transformación digital inteligente	IoT y su evolución		
		Comunicaciones inalámbricas		
		Comunicaciones optoelectrónicas		
		Redes de Sensores		
		Realidad aumentada y extendida		
		Gestión de redes y servicios telemáticos		
		Tecnologías y sistemas especiales		
		Arquitectura, productos y plataforma		
		Aplicaciones TIC para la industria 5.0		
		Inteligencia artificial		
		Ciencia de datos		
		Big data		
		Computación en la nube		
		Supercomputación		
		Blockchain		
		Seguridad en redes		
		Redes cuánticas		
	Energías limpias y desarrollo sostenible	Vehículos de nuevas energías (NEVs)		
		Eficiencia energética		
		Smart-grids		
		Micro redes		
		Electrónica de potencia		
		Sistemas de potencia		
		Generación y almacenamiento de energía		
		Energías renovables		
		Infraestructura TIC sostenible		

Anexo 2.

Tabla 8: Relación de programas y cursos que impacta la línea de investigación en Ciberseguridad

Programa	¿Impacta?	Curso que se relaciona con Ciberseguridad
Tecnología en Calidad Alimentaria	No	
Tecnología en Logística Industrial	No	
Tecnología en Producción de Audio	No	
Diseño industrial	No	
Ingeniería de Alimentos	No	
Ingeniería industrial	No	
Especialización en Gerencia de Procesos Logísticos den Redes de Valor	No	
Maestría en Biotecnología Alimentaria	No	
Maestría en Gerencia de Proyectos	No	
Maestría en Logística y Redes de Valor	No	
Tecnología en Desarrollo de Software	Si	INTRODUCCIÓN AL DESARROLLO DE SOFTWARE ALGORITMOS Y PROGRAMACIÓN PROGRAMACIÓN AVANZADA ANÁLISIS DE REQUISITOS INTERACCIÓN HUMANO COMPUTADOR DESARROLLO DE APLICACIONES PARA LA WEB MODELADO Y ADMINISTRACIÓN DE BASES DE DATOS DESARROLLO DE APLICACIONES PARA MÓVIL DOCUMENTATION AND TECHNIQUES OF SOFTWARE TEST GOBIERNO DE DATOS DESARROLLO LOW CODE METODOLOGÍAS ÁGILES INTRODUCCIÓN A LOS METADATOS FRAMEWORK PARA EL DESARROLLO WEB TECNOLOGÍAS ETL FRAMEWORK PARA EL DESARROLLO APLICACIONES MÓVILES Desarrollo de Software Seguro (E - M - 3)
Tecnología en Gestión de Redes Inalámbricas	Si	Software Aplicado para la gestión de Redes Inalámbricas (O - M - 3) FUNDAMENTOS DE REDES (O - M - 3) ALGORITMOS Y PROGRAMACIÓN (O - M - 3) COMUNICACIONES INALÁMBRICAS LAN INALÁMBRICA Y CABLEADA ANTENAS Y PROPOGACIÓN MANTENIMIENTO DE REDES INALÁMBRICAS REDES TELEMÁTICAS INALÁMBRICAS: WLAN WIMAX (E - M - 3) ACCESOS A LA WAN (E - M - 3) iot – CONECTANDO LAS COSAS (E - M - 3) TECNOLOGÍA Y SERVICIOS DE LOCALIZACIÓN (E - M - 3) COMUNICACIONES MÓVILES (E - M - 3) PRINCIPIOS DE ENRUTAMIENTO (E - M - 3)
Tecnología en Automatización Electrónica Industrial	Si	INTRODUCCIÓN A LA AUTOMATIZACIÓN INDUSTRIAL ALGORITMOS Y PROGRAMACIÓN COMUNICACIONES INDUSTRIALES AUTOMATIZACIÓN INDUSTRIAL ROBÓTICA INDUSTRIAL AUTÓMATAS PROGRAMABLES COMUNICACIONES INDUSTRIALES AVANZADAS iot – CONECTANDO LAS COSAS
Ingeniería multimedia	Si	Fundamentos de informática y redes fundamentos de programación programación programación web bases de datos multimedia programación para videojuegos seguridad informática
Ingeniería de Sistemas	Si	Introducción a la Ingeniería de Sistemas Fundamentos de programación Arquitectura de Computadores

		Programación Análisis y Especificación de Requerimientos Sistemas Operativos Diseño de Bases de Datos Diseño de Software Estructura de Datos Redes y Comunicaciones Bases de Datos Verificación y Validación de Software Administración de Bases de Datos Calidad de Software Gestión de TI Information Security (*) Emprendimiento de Base Tecnológica Análisis de Datos Servicios en la nube Interacción humano computador Evaluación de experiencia de usuario Introducción a los Metadatos Big Data Diseño centrado en el usuario Diseño Accesible Tecnologías ETL Computación Distribuida Planificación, Program. Y control de proyectos BPM con TI (Gestión de procesos Tecnológicos con T.I) Bases de datos Distribuidas Internet de las cosas
Ingeniería de Telecomunicaciones	Si	Introducción a la Ingeniería de Telecomunicaciones Algoritmos Software para Ingeniería Sistemas de comunicaciones Tratamiento Digital de Señales Antenas y Propagación Fundamentos de Redes (CCNA_1) Conmutación Principios de Enrutamiento (CCNA_2) LAN Inalámbrica y Cableada (MOD 3- CISCO) Accesos a la WAN (MOD 4-CISCO) Sistemas Avanzados de Transmisión I Sistemas Avanzados de Transmisión II Comunicaciones Industriales Avanzadas Microondas Ingeniería de Servicios telemáticos Aplicaciones Telemáticas Sistemas Telemáticos para la Gestión de la Información Gestión de Redes Telemáticas
Ingeniería electrónica	Si	Introducción a la ingeniería electrónica fundamentos de programación lenguajes interpretados señales y sistemas sistemas dinámicos teoría del control sistemas automáticos industriales iot ingeniería de datos applied artificial intelligence comunicaciones industriales instrumentación virtual modern and intelligent control diseño industrial avanzado
Especialización en Redes de Nueva Generación	Si	Modelo de Arquitectura en NGN Diseño en Redes de Acceso de Nueva Generación Diseño de Redes de Transporte en NGN Protocolos de Control y Señalización en NGN Planificación y Diseño de IMS

		Seguridad en NGN Vo IP Aplicado a NGN Normatividad en Telecomunicaciones Servicios en NGN Gestión de Redes NGA Servicios en NGN qos en Redes NGN
Especialización en Seguridad Informática	Si	Estrategia y gobierno corporativo fundamentos y modelos de seguridad informática fundamentos de intrusión y testing estándares, normatividad y regulación de la seguridad informática trabajo de grado i administración y gestión del riesgo análisis forense infraestructuras seguras trabajo de grado ii planeación y control de proyectos de seguridad informática algoritmos y modelos criptográficos infraestructuras críticas ciberseguridad e iot aplicaciones y servicios seguros
Maestría en Diseño de Experiencia de Usuario	Si	Arquitectura de la Información y Prototipado Accesibilidad en Información Digital
Maestría en Gestión de Tecnología de Información	Si	Arquitectura de TI y de la solución Gestión de infraestructura de TI Gobierno y Gestión de servicios de TI Gestión de seguridad en TI Tendencias disruptivas
Maestría en Ciberseguridad	Si	Intrusión y Testing Estándares, Normatividad y Regulación de la Ciberseguridad Operaciones de Ciberseguridad Criptografía Moderna Seminario de Investigación Aplicada I Aprendizaje Automático Aplicado a Ciberseguridad Administración del Riesgo de Ciberseguridad Seminario de Investigación Aplicada I Seminario de Investigación Aplicada II Cybersecurity Incident Response Management Seguridad en la Nube Digital forensics Seguridad en el Software Blockchain Ciber-Resiliencia Organizacional Derecho Digital

Anexo 3. Ámbito Nacional

Núm.	Nombre IES	Programa	Pensum	Temas Investigación
1	CORPORACION UNIVERSIDAD PILOTO DE COLOMBIA	MAESTRÍA EN SEGURIDAD INFORMÁTICA Y DE LAS COMUNICACIONES	Gobierno TIC BCP planes de continuidad de negocio Gestión de riesgos y continuidad Seguridad en redes de comunicación Arquitectura de seguridad Detección de intrusos y analítica de datos Pruebas de penetración a infraestructuras Seguridad en bases de datos Diseño de software seguro Seguridad en sistemas operativos y software li Manejo de incidentes informática forense Criptografía Derecho informático Electiva profundización I Electiva profundización II Seminario de tecnología y sociedad Seminario de investigación I Proyecto de profundización	No relacionan temáticas de investigación en ciberseguridad en los grupos actuales
2	CORPORACION UNIVERSIDAD PILOTO DE COLOMBIA	ESPECIALIZACION EN SEGURIDAD INFORMATICA	Introducción a la seguridad Criptografía Gestión de la seguridad Seguridad en aplicaciones Investigación II Investigación I Seguridad operativa Detección de intrusos Informática forense Electiva	No relacionan temáticas de investigación en ciberseguridad en los grupos actuales
3	CORPORACION UNIVERSITARIA AMERICANA	ESPECIALIZACION EN SEGURIDAD INFORMATICA	Fundamentos de Comunicaciones y Seguridad. Aspectos Legales y Éticos. Análisis de Riesgos y Test de Penetración. Criptografía. Electiva I. Seminario de Investigación I. Seguridad en Infraestructuras Telemáticas. Seguridad en el Desarrollo de Aplicaciones. Sistemas de Gestión de Seguridad de la Información. Gestión de Incidentes y Computación Forense. Electiva II . Seminario de investigación II.	No relacionan temáticas de investigación en ciberseguridad en los grupos actuales
4	CORPORACION UNIVERSITARIA MINUTO DE DIOS -UNIMINUTO-	ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA	Seguridad Informática Gestión de Seguridad de la Información Sistemas de Detección de Intrusos Ingeniería Social Criptografía Análisis Forense Electiva Investigación	No relacionan temáticas de investigación en ciberseguridad en los grupos actuales
5	FUNDACION CENTRO DE INVESTIGACION DOCENCIA Y CONSULTORIA ADMINISTRATIVA-F-CIDCA-	TECNOLOGIA EN SEGURIDAD INFORMATICA	No aplica	En liquidación

6	FUNDACIÓN POLITÉCNICO MINUTO DE DIOS - TEC MD	TÉCNICO PROFESIONAL EN SERVICIOS DE SEGURIDAD INFORMATICA	Inglés Manejo de información y datos Administración de sistemas operativos Análisis y diseño de sistemas Cátedra TecMinuto Producción de textos e Hipertexto Estructura de datos Diagnóstico de la seguridad de la información Programación y desarrollo de software Emprendimiento Monitoreo de la seguridad de la información Soporte de software Gestión de redes de comunicación de datos Práctica profesional Diseño del modelo de seguridad Implementación del modelo de seguridad de la información Aseguramiento del modelo de seguridad de la información Administración de hardware y software de seguridad Implementación de bases de datos Electiva	No registra Investigación en el campo de la Cibserguridad
7	FUNDACIÓN UNIVERSITARIA COMPENSAR	ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA	Aplicación de Métodos Criptográficos Modelos y Estándares de Seguridad Informática Regulación y Legislación en Seguridad Informática Transversal Institucional Electiva I Hacking Ético Análisis Forense y Delitos Informáticos Cyberseguridad y Cyberdefensa Electiva II Seminario de Grado	No registra Investigación en el campo de la Cibserguridad

8	FUNDACION UNIVERSITARIA INTERNACIONAL DE LA RIOJA - UNIR	ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA	Hacking ético Informática Forense y Respuesta ante incidentes Desarrollo seguro de software y Auditoría Seguridad en redes y análisis inteligente de amenazas Gobierno de la ciberseguridad y análisis de riesgos Seguridad en Sistemas, aplicaciones y el Big Data Ciberdelitos y regulación de la ciberseguridad Electiva	*Análisis y reingeniería de malware y Seguridad del Código. Técnicas de análisis y reingeniería de malware aplicadas al análisis de malware para poder comprender el funcionamiento del código malicioso (troyanos, virus, rootkits, etc.), evaluar los daños causados y valorar las intenciones y capacidades del atacante de una manera sistemática y metodológica *Arquitecturas seguras y seguridad de los protocolos de red: mecanismos de control de acceso, seguridad en IoT y ciudades inteligentes, ciberseguridad y protección de infraestructuras críticas, computación en la nube y redes P2P seguras, seguridad en dispositivos móviles, blockchain, hacking ético. *Desarrollo seguro de software y aplicaciones: Desarrollo seguro del ciclo de vida de software y aplicaciones. Servicios web de seguridad, seguridad de aplicaciones web y herramientas de prueba de seguridad, análisis estático y dinámico. Seguridad de red, lan, wan, wifi, etc. Monitoreo de seguridad, patrones de ataques, honeynets, y auditoría segura. Blockchain y sistemas de control de acceso: gobierno de la seguridad, diseño de arquitecturas seguras, evaluaciones de seguridad y blockchain.
9	FUNDACION UNIVERSITARIA PARA EL DESARROLLO HUMANO - UNINPAHU	ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA	Gestión de Seguridad Informática Criptografía Riesgos y Soluciones en Seguridad Informática Electiva I Metodología de la Investigación en Seguridad I Seguridad Operativa, Estructura y Software Auditoría y Seguridad Informática Sistemas de Penetración y Defensa Electiva II Metodología de la Investigación en Seguridad II	No registra Investigación en el campo de la Cibserguridad

10	FUNDACION UNIVERSITARIA SAN MATEO - SAN MATEO EDUCACION SUPERIOR	ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA	Catedra Mateista y manejo de herramientas TIC Aspectos éticos. Legales y normativos de la seguridad informática Seguridad en aplicaciones y sistemas operativos Gestión de riesgos de la información Principios de Criptografía Arquitectura en Seguridad Informática Seguridad Informática II Ciberseguridad Gesiutón, estratégica de la seguridad informática Informática forense y delitos informáticos Gestión de incidentes de seguridad de la información Auditoría en seguridad informática	No registra Investigación en el campo de la Cibserguridad
11	FUNDACION UNIVERSITARIA TECNOLOGICO COMFENALCO - CARTAGENA	TECNOLOGÍA EN GESTIÓN DE REDES DE COMPUTADORES Y SEGURIDAD INFORMÁTICA	Introducción a las Redes Algoritmos y Programación Precálculo Comunicación Oral y Escrita Proyecto de Vida Ambiente y Desarrollo Cultura y Deporte Redes de Computadores Programación Orientada a Objetos Cálculo Diferencial Física Mecánica y Laboratorio Fundamentos de Seguridad Informática Estructuras de Datos Aplicadas Electiva Libre Sociohumanística I Cálculo Integral Estadística Inglés II Análisis de Vulnerabilidades Desarrollo de Software I Bases de Datos Electrónica Digital y de las Comunicaciones Seguridad en Redes y Servicios Cálculo de Varias variables Visualización de Datos II Minería de Datos II Computación Distribuida Ecuaciones Diferenciales Metodología de la Investigación Emprendimientos Tecnológicos Electiva IIIElectiva V Gerencia de Proyectos TI Opción de Grado Diseño de Usabilidad y Experiencia de Usuario Infraestructura TI Ingeniería Económica Electiva IV Computación en la Nube Métodos Numéricos Matemáticas Discretas Inglés VI Inglés VII Computación Móvil Investigación de Operaciones Desarrollo Web Avanzado Visualización de Datos I Minería de Datos I Inglés V Electiva Libre Sociohumanística III Desarrollo de Software II Seminario Investigativo Innovación y Emprendimiento Electiva de Profundización I Seguridad en Sistemas Operativos de Red Electiva Libre Sociohumanística II Ingeniería de Software Competencias Ciudadanas Redes de Servicios Convergentes Electiva de Profundización IIInglés IInglés III Inglés IV	EthicalHacking Internet de las Cosas CiberSeguridad Deep Web Servicios basados en localización WiFiEscalable

12	INSTITUCION UNIVERSITARIA ESCOLME	TECNOLOGIA EN REDES Y SEGURIDAD INFORMATICA	Derecho informático Fundamentos de administración Fundamentos de investigación Lengua extranjera i Algoritmos i Cátedra escolme Matemáticas operativas Pensamiento matemático Escritura Lectura crítica Algoritmos ii Fundamentos de seguridad informatica Introduccion al calculo Lengua extranjera ii Redes de datos i Sistemas operativos Algoritmos ii Fundamentos de seguridad informatica Introduccion al calculo Lengua extranjera ii Redes de datos i Sistemas operativos Bases de datos y seguridad Emprendimiento i Programacion de dispositivos moviles Arquitectura de los sistemas operativos Electiva i informatica Lengua extranjera iv Configuracion de redes y servicios Hacking etico aplicado Seguridad e implementacion de redes inalambricas y computacion movil Constitucion politica Emprendimiento ii Principios de criptografia Seguridad en internet Estadistica descriptiva Etica Trabajo de grado – tecnologia Electiva ii informatica Prospectiva tecnologica Seguridad y monitoreo	Analizar el uso y beneficios de los ciberseguros para empresas dando las mejores opciones para mejorar su seguridad informática Implementación de una Infraestructura de Red y Seguridad perimetral en la empresa TYM Autopartes por medio de software libre Conjunto de buenas prácticas que ayuden a aumentar los niveles de seguridad informática en las empresas colombianas

13	INSTITUTO TECNOLOGICO METROPOLITANO	MAESTRIA EN SEGURIDAD INFORMÁTICA	Fundamentos de seguridad y Gestión de Riesgos Seguridad en redes y en Sistemas Operativos Aspectos legales de Incidentes de Seguridad Seminario I Sistemas de detección y prevención de Intrusos Análisis Forense en sistemas de procesamiento Electiva 1 Seminario II Seguridad en aplicaciones y código fuente Conformación de equipos de respuesta a incidentes de seguridad Electiva 2 Seminario III Gestión de Vulnerabilidades Electiva 3 Seminario 4 – proyecto de grado Electiva 1 – Plan de continuidad de negocio y gestión de crisis Electiva 1 – Criptografía Electiva 2 – Análisis de Malware Electiva 2 – Hacking Ético y Pentesting Electiva 2 – Auditoría de la seguridad Electiva 3 – Análisis Forense en dispositivos móviles Electiva 3 – Seguridad en la nube híbrida, contenedores y servicios Electiva 3 – Seguridad en IoT	No registra Investigación en el campo de la Cibserguridad
14	UNIVERSIDAD AUTONOMA DE OCCIDENTE	ESPECIALIZACION EN SEGURIDAD INFORMATICA	Introduccion al hacking etico ciclo del hacking etico Ataques a aplicaciones web y redes inalambricas Conceptos basicos del algebra Espacio y medida Familia de funciones en una variable real y de valor real Aspectos eticos y legales de los datos e información Proteccion legal del conocimiento y comercio electronico Introduccion a la criptografia y tipos de cifrado Algoritmos de cifrado Aplicaciones de redes y equipos Introduccion a la seguridad de datos Analisis de vulnerabilidades Auditoria y desarrollo seguro Políticas y aspectos legales: seguridad de datos Seguridad en sistemas operativos Seguridad en el almacenamiento de datos Introduccion a la informatica forense Evidencia digital La ciencia Forense	No registra Investigación en el campo de la Cibserguridad

15	UNIVERSIDAD DE INVESTIGACION Y DESARROLLO - UDI	ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA	Seguridad y gestión de riesgos Criptografía Modelos y estándares de seguridad Protocolos de seguridad forense Comunicación y seguridad en redes Seminario de trabajo de grado i Arquitectura de seguridad e ingeniería Evaluación de seguridad y pruebas de control Marco legal y ético de la seguridad informática Informática forense Taller optativo Seminario de trabajo de grado ii	Aplicación Software Para Estimar Los Costos De Vulnerabilidad En Claves De Seguridad E Indicadores Del Nivel De Protección Para La Auditoria De Diversos Sistemas Informáticos Con El Software Intel Paralell Studio
16	UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD	ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA	Estrategia y gobierno corporativo Administración y gestión del riesgo Fundamentos de intrusión y testing Infraestructuras seguras estándares, normatividad y regulación de la seguridad informática Electivos Electiva i Electiva ii Trabajo de grado i Trabajo de grado ii Trabajo de grado iii Planeación y control de proyectos de seguridad informática Algoritmos y modelos criptográficos Infraestructuras críticas Ciberseguridad e iot Aplicaciones y servicios seguros	Auditoria de sistemas
17	UNIVERSIDAD PONTIFICIA BOLIVARIANA	ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA	Seguridad Informática y la Evaluación del Riesgo de TI Criptografía y sus aplicaciones Evidencia Digital e Investigaciones Forenses Digitales Seguridad Ofensiva y Defensiva Régimen Jurídico en Seguridad de la Información Liderazgo y Gerencia Estratégica de la Seguridad de la Información	Modelo de medidas efectivas de seguridad de la información para la protección de datos Modelo estructural de los observatorios de ciberseguridad: Perspectiva desde la dinámica de sistemas Estudio de Viabilidad para la Creación de un Observatorio Nacional de Ciberseguridad de Colombia.
18	CORPORACION UNIVERSITARIA IBEROAMERICANA	ESPECIALIZACION EN CIBERSEGURIDAD	Electiva Integral Desarrollo Sostenible Fundamentos de Ciberseguridad Competencias y Procesos Investigativos Análisis de Vulnerabilidades y Pruebas De Penetración Arquitecturas de Ciberseguridad Gestión de Riesgos en Ciberseguridad Electiva Profesional Opción De Grado Ciberseguridad en Entornos TIC Software Seguro Respuesta a Incidentes de Ciberseguridad	No registra Investigación en el campo de la Cibserguridad

19	DIRECCION NACIONAL DE ESCUELAS	MAESTRÍA EN CIBERSEGURIDAD E INFORMÁTICA FORENSE	Normalización Análisis y gestión de riesgos Fundamentos de las ciencias computacionales Fundamentos de criptografía Identificación de la evidencia digital Ética profesional Investigación I Electiva I Legislación en ciberseguridad Sistemas de gestión de seguridad de información Infraestructuras críticas Técnicas avanzadas de protección de la información Recolección y preservación de la evidencia digital Investigación II Electiva II Procedimiento judicial en las TIC Gerencia y administración de los CERT, CSIRT y manejo incidentes Técnicas de explotación de vulnerabilidades Seguridad de la información en la arquitectura TI Análisis de la evidencia digital Trabajo de campo Electiva III Audiencia Gestión y administración de proyectos de ciberseguridad Comercio electrónico legal Ciberlavado de activos Diseño de estrategias nacionales e internacionales de ciberseguridad Gobierno de TI Prospectiva de la ciberseguridad Análisis en el ciberespacio Técnicas avanzadas de ataques a redes y sistemas de información Auditoría de seguridad Redacción de informes periciales Trabajo de grado	No registra Investigación en el campo de la Cibserguridad

20	ESCUELA SUPERIOR DE GUERRA GENERAL RAFAEL REYES PRIETO	MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA	Contexto en Ciberseguridad y Ciberdefensa Gestión de la Ciberseguridad Seguridad y Defensa en el Ciberespacio Gobernanza de la Ciberdefensa de Investigación Prospectiva en Ciberseguridad y Ciberdefensa Anticipación de Amenazas Cibernéticas Gestión de Riesgos Cibernéticos Electiva 1 Resilencia Cibernética y Continuidad en el Negocio Juegos de Guerra Cibernética Regulaciones en Ciberseguridad y Ciberdefensa Proyecto de Investigación Innovación en Ciberseguridad y Ciberdefensa Electiva 2 Forense Digital Amenazas Cibernéticas Contemporáneas Ciberdiplomacia y Cooperación en el Ciberespacio Trabajo de Investigación	Modelo estructural para el análisis y la construcción de políticas de seguridad y defensa. Evaluación de riesgo de Ataque Terrorista a Infraestructuras Críticas en Colombia a partir de la Comisión Europea
21	FUNDACION UNIVERSITARIA MARIA CANO	ESPECIALIZACIÓN EN CIBERSEGURIDAD	Ciberseguridad. Gestión de riesgos. Inteligencia de amenazas. Detección de intrucciones. Seminario de investigación I. Aspectos legales de ciberseguridad Controles de protección en ciberseguridad Gestión de incidentes y ciberdefensa Continuidad de negocio Electiva. Seminario de investigación II	No registra Investigación en el campo de la Cibserguridad
22	UNIVERSIDAD AUTONOMA DE BUCARAMANGA-UNAB	ESPECIALIZACIÓN EN CIBERSEGURIDAD ORGANIZACIONAL	Electiva i Fundamentos en ciberseguridad Liderazgo para el cambio Seminario i Solucion creativa de problemas Tecnologias de informacion Amenazas informaticas Electiva ii Gestion de seguridad de la informacion Marco regulatorio en ciberseguridad Seminario ii Tendencias en ciberseguridad	No registra Investigación en el campo de la Cibserguridad

23	UNIVERSIDAD CATOLICA DE MANIZALES	ESPECIALIZACIÓN EN CIBERSEGURIDAD	Ethical hacking Desarrollo para el pentesting Seguridad en transmisión de datos Investigación I Identidad UCM Computo forense y cibercrimen Gestión de incidentes de ciberseguridad Electivo Investigación II Responsabilidad social y normatividad	No registra Investigación en el campo de la Cibserguridad
24	UNIVERSIDAD DE SAN BUENAVENTURA	ESPECIALIZACIÓN EN CIBERSEGURIDAD	Seminario de Investigación Fundamentos de Seguridad de la Información y Ciberseguridad Gestión del riesgo cibernético Detección y respuesta de ciberataques Seguridad en aplicaciones Optativa I Humanística Proyecto de Ciberseguridad Gestión del programa de ciberseguridad Controles para la información en reposo y en tránsito Gestión de inteligencia de amenazas Optativa II	No registra Investigación en el campo de la Cibserguridad
25	TECNOLOGICO DE ANTIOQUIA	ESPECIALIZACION EN SEGURIDAD DE LA INFORMACION	Fundamentos de seguridad de la información Mecanismos de protección criptográficos Seguridad en aplicaciones y bases de datos Seguridad en redes y sistemas operativos Gobernabilidad TI Ciencia forense digital Aspectos jurídicos delitos informáticos Gestión de riesgo Seguridad en dispositivos móviles Gerencia de proyectos	criptografía, algoritmia, y mecanismos de seguridad, seguridad de la información en redes, seguridad en aplicaciones de internet y WEB, seguridad y protección de sistemas operativos, seguridad en bases de datos, estándares y protocolos de seguridad, ciencia forense digital, aspectos legales de la seguridad de la información, entre otros.
26	UNIVERSIDAD CATOLICA DE COLOMBIA	ESPECIALIZACION EN SEGURIDAD DE LA INFORMACIÓN	Gerencia de proyectos Normas y estandares para la gestion de la seguridad de la informacion Gestion de riesgos de la seguridad de la informacion Vulnerabilidades, seguridad en redes y sistemas operativos Electiva I Informatica forense y gestion de incidentes de seguridad Etica aplicada Seminario de trabajo de grado Electiva II	Diseño de una arquitectura de seguridad de TI para cloud computing Seguridad de jax-rs frente a ataques por inyección de código

27	UNIVERSIDAD COOPERATIVA DE COLOMBIA	ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN	Contexto de la seguridad de la informacion Criptografia Seguridad en las aplicaciones Gestion de riesgos de la informacion Definicion de modelos de seguridad Gestion estrategica de la seguridad Informatica forense Aspectos legales de la seguridad de la informacion	No registra Investigación en el campo de la Cibserguridad
28	UNIVERSIDAD DE LOS ANDES	MAESTRÍA EN SEGURIDAD DE LA INFORMACIÓN	Ingeniería Criptográfica y su aplicación en TI Defensa y ciberseguridad en la red Seguridad en el Host Arquitectura de Infraestructura Modelos de Resiliencia Operacional y su Aplicación a Seguridad en TI, Continuidad y Servicios en TI Gerencia de CSIRTs y manejo de incidentes Programación Segura **Gerencia de Proyectos en Seguridad de la Información Computación Forense: Delitos informáticos, Aspectos Legales y Evidencia Digital Criptografía moderna en aplicaciones Ciberseguridad Ofensiva Herramientas de Seguridad y sus fundamentos Seguridad y Privacidad de sistemas IIoT e IoT Información, Seguridad y Privacidad Habilidades gerenciales en TI Formación de Directivos de TI Gobierno de TI Gestión de servicios de TI TI para Sector público Electiva en otra maestría de Sistemas y Computación Electiva en otra maestría Proyecto	Ciberseguridad. Plataformas emergentes Privacidad Educación ciudadana
29	UNIVERSIDAD DISTRITAL-FRANCISCO JOSE DE CALDAS	MAESTRÍA EN GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN	Módulo i introducciónalaseguridad de lainformación Módulo il. Legislación en seguridad de lainformación Módulo iii. Ethicalhacking Módulo iv. Normaiso 27001seguridad de lainformación Módulo v. Criptografía Módulo vi. Informáticaforense	No registra Investigación en el campo de la Cibserguridad

30	UNIVERSIDAD SERGIO ARBOLEDA	ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN E INFORMÁTICA	Ética Profesional Derecho Informático Aspectos Generales de Seguridad Modelos de Gestión de la Seguridad Criptografía Seguridad en Redes Seguridad en Aplicaciones Seguridad en Base de Datos Informática Forense Gestión de Incidentes Análisis de Malware Electiva Seminario Internacional	No registra Investigación en el campo de la Cibserguridad