Resultados “Informe I+D en Ciberseguridad”

siempre en directa relación al Eje 5 de la actual política nacional de ciberseguridad 2023-2028.

El 5 de junio, el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación presentó los resultados de este trabajo, el cual consistió en un análisis de los investigadores con afiliación chilena en el área de ciberseguridad durante los últimos 10 años.

El estudio se dividió en tres partes: Revisión del estado del arte en las áreas de investigación en seguridad y privacidad en las que los autores afiliados a instituciones chilenas han contribuido. Con el respaldo de un panel de investigadores, se han propuesto cuatro áreas prioritarias para la investigación en los próximos 5 a 10 años.

Durante el análisis de las necesidades y apoyos requeridos, los expertos consultados resaltaron la falta de especialización en ciberseguridad, tanto a nivel técnico como de usuarios finales. También resaltaron la falta de conciencia al respecto. Por esta razón, el área Educación toma mayor importancia pues permite promover la conciencia en ciberseguridad, fomentar el desarrollo de herramientas y procesos locales de manera más efectiva y eficiente permitiendo integrar a las personas de manera intuitiva, sin la necesidad de estudiar manuales extensos y por supuesto, promover la educación como una competencia transversal en la educación en los diferentes niveles de educación.

Resultados:

ESTADO DEL ARTE

Para comenzar, el estudio identificó áreas prioritarias de investigación en diversos países de Europa, India y México.

Tanto India como México se realizó un análisis sistemático de la literatura en investigación en ciberseguridad. Los resultados arrojaron:

Sobre India…

- Se realiza un estudio sistemático que examinó **989 publicaciones** provenientes de la fuente de datos Scopus.
- El número de **publicaciones en ciberseguridad aumentó significativamente de 1 en 1999 a 280 en 2020,** mostrando una tendencia al alza, con más del 70%

de estas publicaciones realizadas en los últimos tres años (2018, 2019 y 2020) y ocupando el cuarto lugar a nivel internacional en número de publicaciones en este ámbito.

- Destaca la importancia de la colaboración internacional en la investigación en ciberseguridad con países líderes en la temática tales como Estados Unidos, el Reino Unido, Canadá, Israel y otros actores importantes en el ámbito de la ciberseguridad.
- Las tendencias específicas en ciberseguridad, se describieron siguiendo una evolución temporal en tres fases:
  Incubación: Se enfocó principalmente en temas relacionados con datos. Criptografía también estuvo en el período de incubación.

  Desarrollo: Hubo un cambio hacia temas como la red inteligente y la integración de aprendizaje automático y computación en la nube en ciberseguridad.

  Madurez: Las áreas de enfoque se ampliaron para incluir tecnologías relacionadas con la inteligencia artificial y el Internet de las cosas (IoT), con foco en detección de intrusiones y malware.

En cuanto a México…

- Las investigaciones en ciberseguridad se centran en temas relacionados con el ciberespacio, seguridad cibernética, Tecnologías de la Información y las Comunicaciones (TIC) y protección de datos.
- Este estudio se basó en el periodo 2015–2020 -18 trabajos específicamente de las fuentes Sciencedirect, Redalyc, and Dialnet.
- Existe una conexión entre la ciberseguridad y temas más amplios como la seguridad del Estado y los movimientos sociales en el ciberespacio.
- El análisis sugiere la necesidad de considerar la ciberseguridad como un tema serio y prioritario en los planes estratégicos gubernamentales de México, donde las universidades deberían jugar un papel clave en la generación y divulgación de estudios multidisciplinarios relacionados con la ciberseguridad.
- Este análisis destaca la importancia de abordar la ciberseguridad desde una perspectiva multidisciplinaria y fomentar la colaboración entre instituciones educativas y de investigación para abordar los desafíos en este campo en México.
- Los principales Temas de Investigación son: Seguridad Cibernética, TIC y Protección de Datos, Seguridad de la Información, Ciberespacio y Seguridad del Estado.

Por otra parte, el documento “Analysis of the European R&D priorities in cybersecurity: Strategic priorities in cybersecurity for a safer Europe” publicado en diciembre de 2018 identificó las amenazas de ciberseguridad para la sociedad europea y determinó las siguientes áreas investigación: Inteligencia Artificial (IA), tecnologías cuánticas, la complejidad de la interconexión que puede llevar a la falla en cascada de múltiples, ciberdelincuencia, investigación y desarrollo de predicción de malware/ataques mediante análisis de datos y predicción automática y privacidad versus "big data".

Sin embargo, este documento publicado por la misma agencia en 2022 “Research and Innovation Brief; Annual Report on Cybersecurity Research and Innovation Needs and Priorities” actualizó la lista de los desafíos de investigación en los que se debe tener foco:

- **Inteligencia Artificial en ambientes productivos:** Diseño de enfoques para la monitorización de sistemas a gran escala y posiblemente interconectados; Exploración de algoritmos de ciberseguridad biomiméticos; Incorporación del concepto de seguridad por diseño (evaluación de la seguridad de los mecanismos de protección frente a un marco estandarizado considerando diversos intentos maliciosos); Preservación de la privacidad y confidencialidad del flujo de información; Inclusión de la conciencia contextual en el aprendizaje automático para aumentarla resiliencia. Como podemos notar este foco aborda de manera conjunta los focos del reporte del 2018 de IA y privacidad vs big data.
- **Tecnologías emergentes:** la redefinición de los límites de la interacción humano-computadora y los riesgos cibernéticos concomitantes asociados a esto; Ciberseguridad en el contexto de las nuevas generaciones de comunicaciones móviles y métodos de recopilación o procesamiento de datos (evolución de 5G a 6G).
- **Criptografía:** Esquemas de clave pública cuánticamente resilientes o seguros y eficientes; Implementaciones eficientes de esquemas de clave simétrica con un mayor nivel de seguridad; Estándares para nuevos algoritmos y protocolos cuánticamente resilientes o seguros; Planificación y preparación para la transición a la era poscuántica de sistemas criptográficos; Seguridad asistida por hardware, en particular en tecnología de CPU, soporte transparente de aplicaciones y el uso combinado de tecnologías de Entorno de Ejecución Confiable (TEE) y Cifrado Homomórfico (HE); entre otros.
- **Ciberbioseguridad:** Los riesgos en evolución y el panorama de amenazas en la I+D en biotecnología; Marco de gestión de riesgos en el campo de la microbiología de la salud pública (por ejemplo, secuenciación de ADN moderna); Categorías de vulnerabilidades de ciberbioseguridad (es decir, distinguir las más tradicionales de las que están fuera de las metodologías existentes); Identificación de los procesos y rutinas en los campos de las ciencias de la vida que requieren interfaces y dependencia de la automatización.

En cuanto a Chile, el estudio se centró en los focos prioritarios de investigación en ciberseguridad declarados por el Libro “Construyendo la Ciberseguridad en Chile”, entre ellos se destacan: Ataques de ciberseguridad a Inteligencia Artificial: ataques a modelos de Machine Learning o modelos grandes de lenguaje; Optimización de capacidades de detección/mitigación de intrusos y malware; Criptografía; Interoperabilidad; Identidad digital con biometría; Fake News y Desinformación en línea; Resiliencia en infraestructura Crítica/IoT; Investigación Forense Digital; Ciudades Inteligentes y resilentes con subcomunidades por segmento de mercado; regulaciones, legislación; Ciberseguridad por diseño y Privacidad por diseño.

Capacidades de I+D de laboratorios/Centros en países de referencia

Basados en la RENIC, se hizo una comparación de infografías entre el año 2017 y 2022 sobre las materias en las que investiga la red desde su creación. Dado que la segunda infografía es para el último cuartil del 2022, podemos comentar que:

- A inicios de 2023 la investigación en ciberseguridad en España se realizaba principalmente en 4 Centros tecnológicos, 27 Universidades y 7 Centros de Investigación.
- A inicios de 2023 se identifican también 50 equipos de investigación ubicados en 19 localizaciones geográficas de España, concentrando la mayor cantidad en Madrid, Barcelona, Pontevedra y León.
- El 22% de los equipos eran pequeños (menor o igual a 5 participantes), 44% de tamaño entre 6 a 10 personas, 20% entre 11 a 15% y el 14% restante con equipos con más de 15 integrantes.
- En la media se visualizan 8 investigadoras e investigadores por equipo. De un total de 470 investigadoras e investigadores en España, solo el 25% son mujeres. Comparando con el escenario en 2017 vemos en general una contracción de la RENIC; menos investigadoras e investigadores, así como menos Universidades (de 94 a 27) y centros tecnológicos (de 9 a 4).
- Por otro lado, vemos un aumento de los centros de investigación en ciberseguridad de 1 en 2017 a 7 a fines de 2022. Por tanto, es posible que a medida que aumenta la madurez de la red, exista una mayor especialización en temáticas más profundas, lo cual se refleja en más centros especializados de investigación.
- Principales áreas de investigación. En 2022, dado el propio avance de la transformación digital aumenta la demanda de investigación en ciberseguridad en seguridad de redes así como en seguridad de internet de las cosas (IoT) y cloud computing. RENIC presentó mayor investigación en los siguientes temas:
  1) exfiltración de datos, protocolos criptográficos para preservar privacidad, privacidad en IoT y criptografía y 2) no disponibilidad de servicios,

seguridad/privacidad mediante el diseño, autenticación criptográfica, control de acceso y autenticación; además detección de anomalías lo cual a la vez se interconecta con la necesidad de resolver desafíos de investigación en análisis de datos a gran escala.

REDES DE COLABORACIÓN

Una segunda parte de esta investigación consistió en una revisión bibliométrica para caracterizar la investigación desarrollada por la comunidad científica de Chile en ciberseguridad los últimos 10 años. La revisión considera artículos publicados en revistas, conferencias, capítulos de libros y revisiones en inglés o español obtenidos de la Base de Datos Científica Scopus, periodo 2012-2023.

Para comenzar, se entregó una visión general respecto del corpus de documentos a analizar, así como de las autoras y los autores responsables de la publicación de los resultados de estas investigaciones.

Segundo, realizamos un mapeo de la ciencia durante los últimos 10 años con el objetivo de levantar los tópicos de investigación cubiertos por las investigadoras y los investigadores, así como sus redes de colaboración. Tercero, describimos como dividimos el periodo en 5 subperiodos de manera de poder analizar la presencia y evolución de los tópicos durante los últimos 10 años en 5 subsecciones. En paralelo, identificamos las redes de colaboración existentes a nivel nacional, como a nivel internacional.

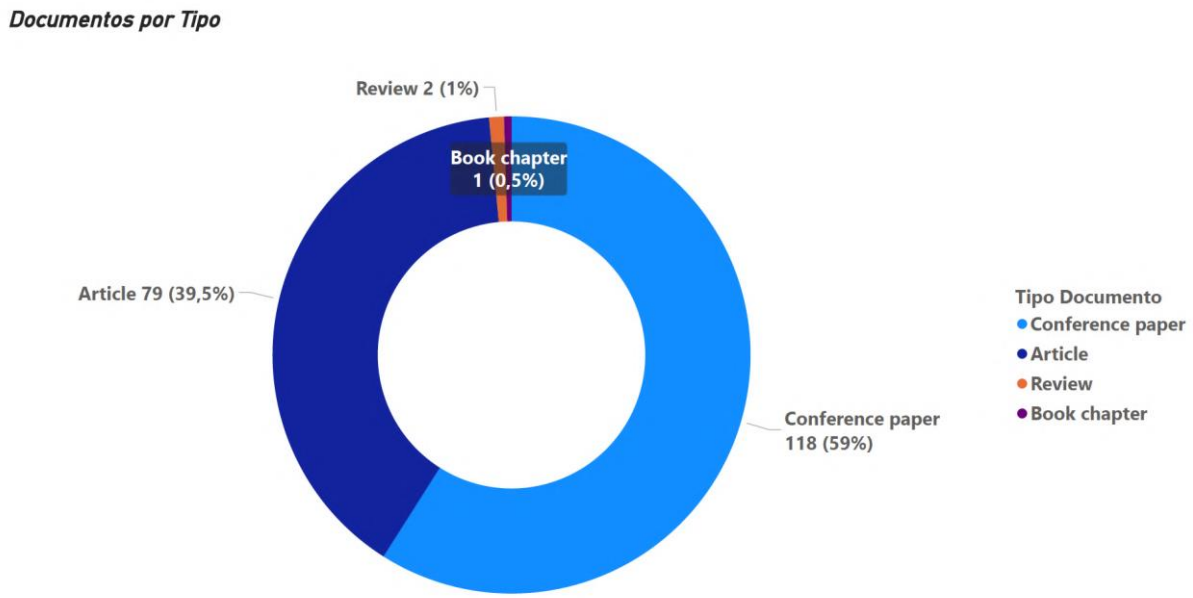
1. Visión general

De manera de permitir la reproducibilidad de este reporte, el siguiente Cuadro muestra explícitamente la consulta realizada a la Base de Datos Scopus en Octubre 2023.

La consulta arrojó un resultado de 1550 documentos donde al menos un autor tenía afiliación chilena al momento de la publicación.

Ejecutada la etapa de “screening”, se ejecuta la etapa de clasificación. En esta etapa, se intenta, si es posible, clasificar los artículos en las áreas del sistema de clasificación de computación ACM (ver Anexo: Taxonomía ACM): (1) Criptografía, (2) Seguridad en el Almacenamiento y en bases de datos, (3) Métodos formales y teoría de la seguridad, (4)Aspectos humanos y sociales respecto de la seguridad y privacidad, (5) Mitigación y detección de intrusos y malware, (6) Seguridad de la red, (7) Seguridad en el Hardware, (8) Servicios de Seguridad, (9) Seguridad de Software y Aplicaciones, y (10) Seguridad de los Sistemas. Esto con el fin de seguir una taxonomía formal, reconocida y aceptada por la comunidad científica.

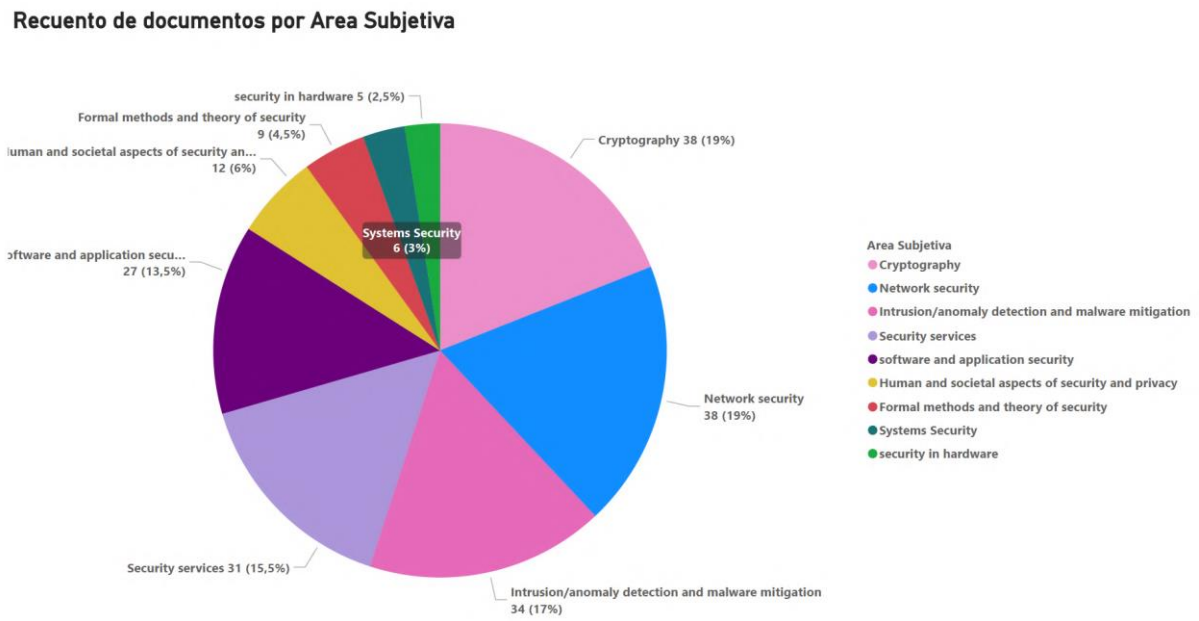
Vemos además que dada la base de datos científica seleccionada, los artículos a revisar se dividen en Artículos de revistas (aproximadamente un 40%) y Artículos de conferencias (casi un 60%).



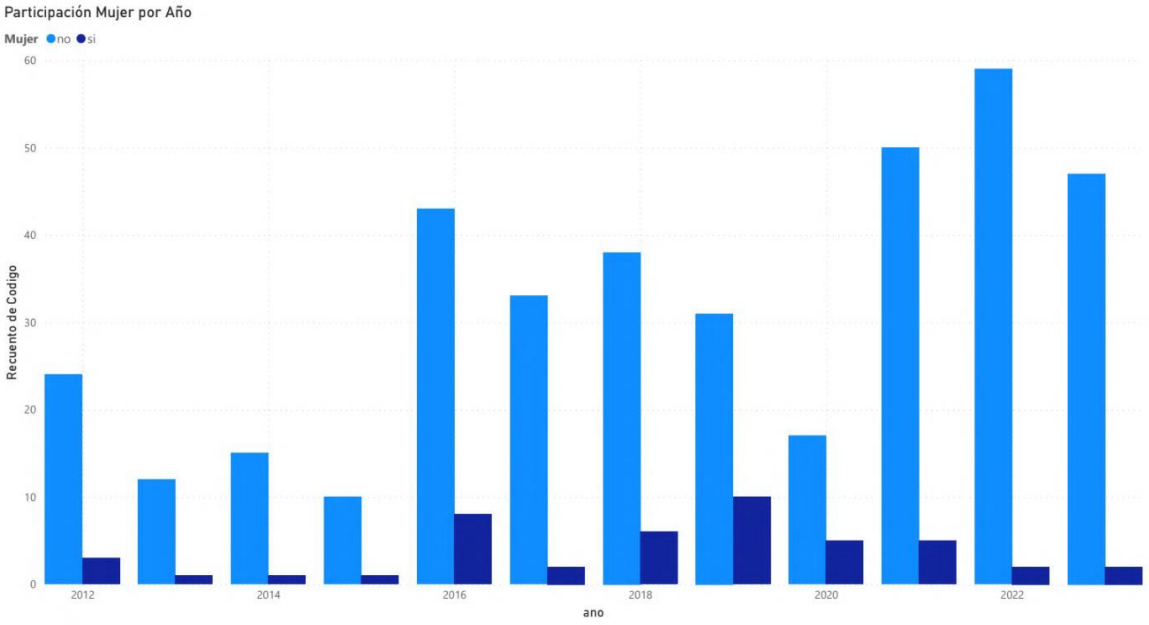
Documentos por tipo

Figura 3.3 vemos una distribución respecto al área principal en que se clasificaron los documentos, donde podemos ver que en los últimos 10 años las autoras y los autores con afiliación chilena han investigado principalmente en Criptografía, seguridad en redes, detección y mitigación de intrusos y malware, en servicios de seguridad y seguridad a nivel de aplicación y software.

Donde vemos una falta de artículos es en el área Seguridad en el almacenamiento y base de datos, así como de seguridad en Hardware. Ahora bien, es posible dada la naturaleza de esta última categoría que los requerimientos para realizar patentes genere un efecto que las investigadoras y los investigadores tiendan a no querer o no poder publicar sus resultados en conferencias y revistas (y por tanto la base de datos científica Scopus no la indexe).

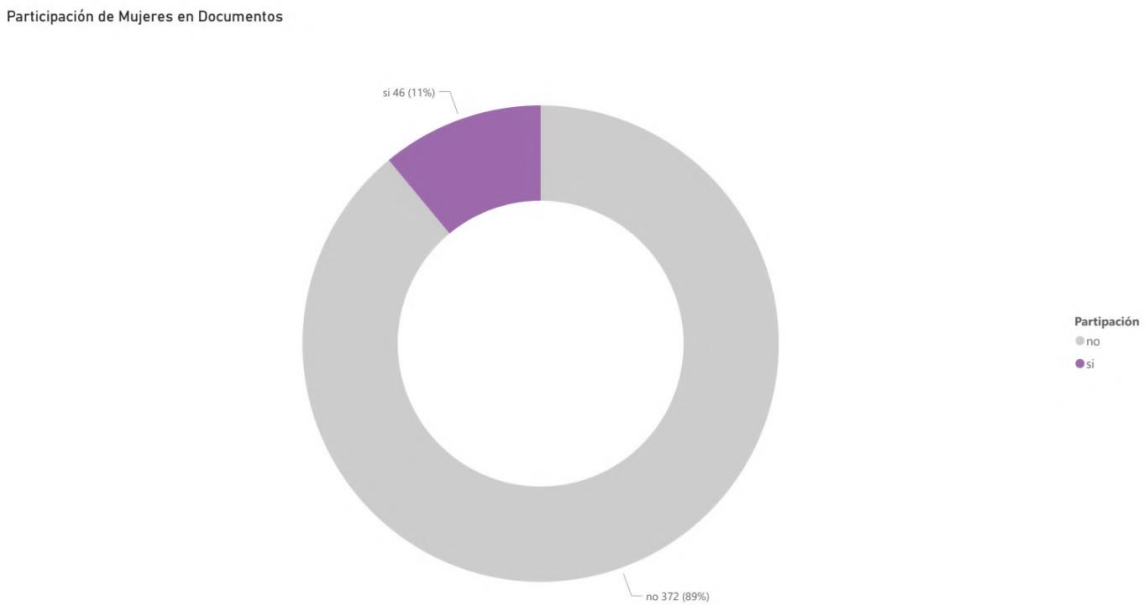


En la Figura 3.4 podemos ver la cantidad de autoras vs autores en el tiempo, sin importar si son mujeres u hombres o si tienen o no afiliación chilena al momento de la publicación u hoy (finnoviembre 2023).



Participación de mujeres por año

De las autoras y los autores considerados, el 11% son mujeres.



El objetivo es realizar un análisis de redes de investigación en ciberseguridad, donde se indiquen las principales colaboraciones entre investigadoras y/o investigadores y temas abordados. Para facilitar la comprensión, hemos dividido el periodo bajo estudio en cinco iniciando desde el año 2023 en reversa, el cual considera dos subperiodos de 2 años y un último subperiodos de 4 años. El siguiente Cuadro muestra la cantidad de documentos y autoras y autores que comprende cada subperiodo acorde a esta división.

Rango	#Documentos	#Autoras/Autores
2012–2015	40	115
2016–2017	39	112
2018–2019	38	113
2020–2021	31	84
2022–2023	52	168

Cuadro 3.3: Número de artículos y autoras/autores por subperiodo considerado.

Generados los grafos para cada uno de los subperiodos, el estado del arte de investigación en ciberseguridad en Chile se describe en los cinco periodos anteriormente indicados utilizando primero los grafos de tópicos de investigación, donde se busca contar la evolución desde la mirada de las grandes áreas de la ACM pero

utilizando los tópicos que emergen de manera natural de los artículos seleccionados. En cada uno de estos periodos se ha escogido un grupo representante de artículos por tópico o área de investigación que permita luego discutir respecto de la comunidad alrededor de estos tópicos en el grafo de colaboración entre investigadoras o investigadores.

2012-2015

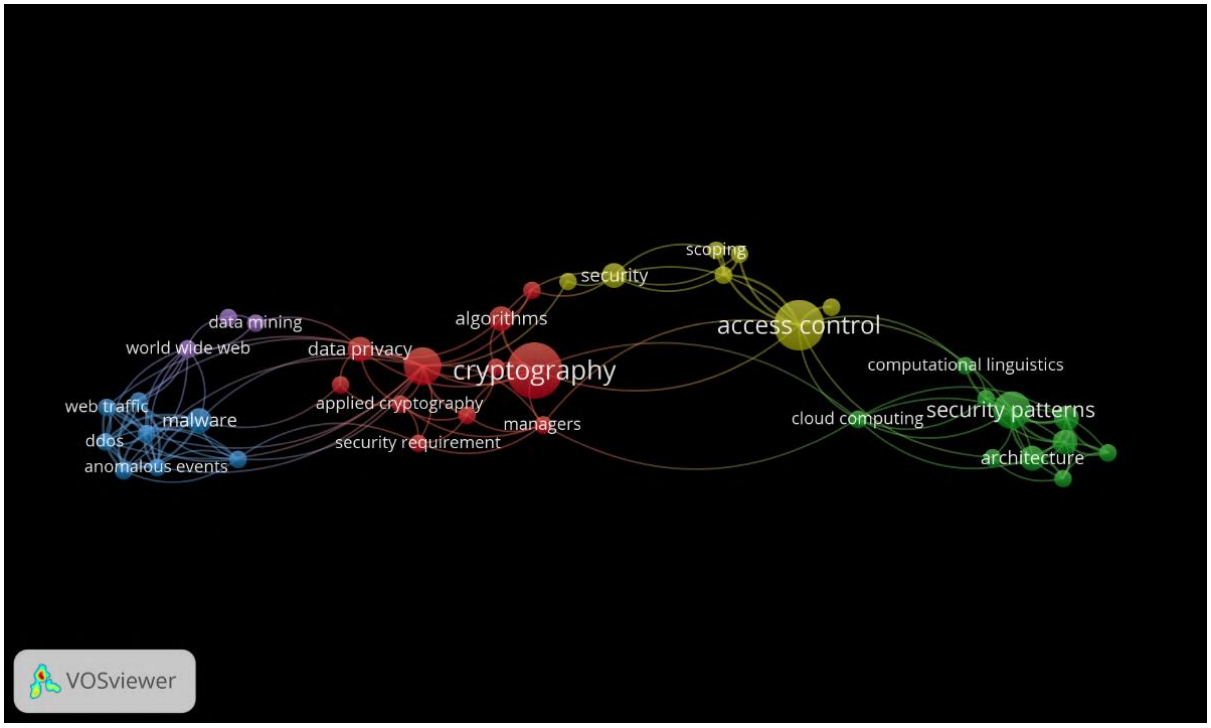


Figura 3.6

Iniciando desde el grupo verde de más a la derecha podemos ver que uno de los tópicos relevantes de investigación en este periodo fue la ingeniería de software en ciberseguridad o seguridad de software y aplicaciones acorde a la nomenclatura de la ACM, la cual busca integrar prácticas de diseño seguro desde las etapas iniciales del ciclo de vida del desarrollo de software, con el objetivo de idealmente prevenir vulnerabilidades y fortalecer con sus decisiones de diseño, la resistencia de los sistemas frente a posibles amenazas actuales o futuras.

El grupo azul de la Figura 3.6 representa los trabajos realizados por diversos autoras/autores en el ámbito de seguridad en redes y la comunidad de detección y mitigación de intrusos y malware.

La Figura 3.7 vemos que las comunidades mayormente representadas son aquellas relacionadas a los servicios de seguridad, detección y mitigación de intrusos y malware, criptografía y por último, en este periodo particular, la superposición del área de investigación de seguridad de software y aplicaciones con el área de métodos formales y teoría de seguridad. En particular la comunidad de detección y mitigación de intrusos

y malware es numerosa respecto de las otras comunidades y altamente conectada, a diferencia por ejemplo de la comunidad de criptografía que se ve numerosa pero con subgrupos disconexos. La comunidad servicios de seguridad en general se ve también conectada donde existe un subgrupo menos conectado que en particular trabaja en biometría usando Inteligencia Artificial.

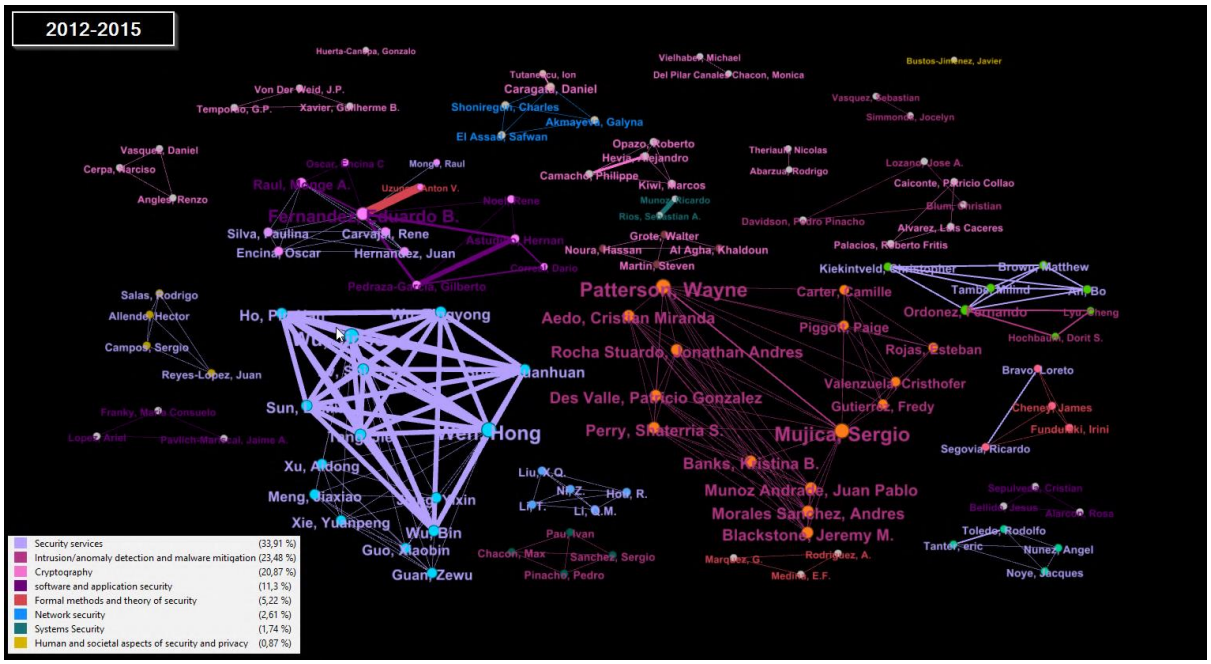


Figura 3.7: Autoras/Autores responsables de las investigaciones consideradas en este estudio publicadas durante periodo 2012–2015.

Periodo 2016–2017

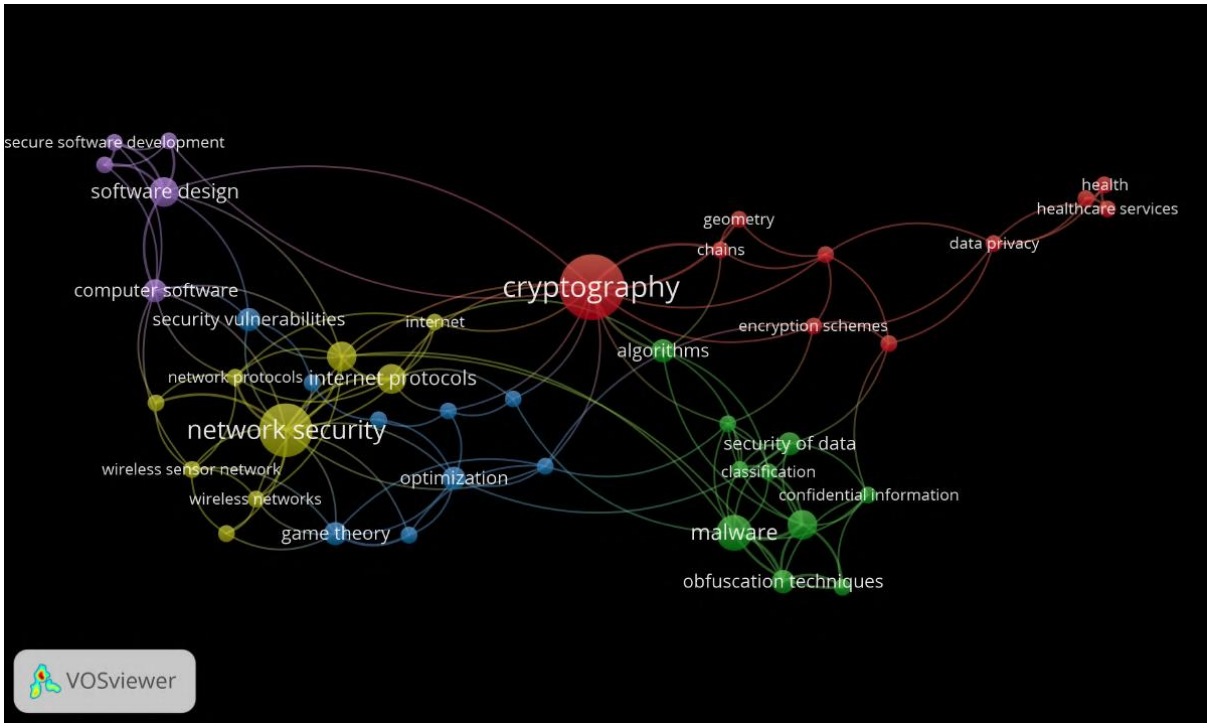


Figura 3.8: Principales tópicos en los que investigadoras o investigadores realizan investigación en

Nuevamente importante en este periodo, es la comunidad de criptografía que aparece en el centro de la Figura 3.8.

En esta misma comunidad, pintada de rojo, podemos ver la privacidad de datos como tópico relevante de investigación conectada también a la salud y específicamente a servicios de salud, mostrando como estas comunidades, la de criptografía para asegurar la privacidad y para así entregar mejores servicios de seguridad como la autenticación en este ámbito, durante este periodo presentan una alta conexión.

En este periodo, en amarillo en la Figura 3.8 aparece fuertemente la comunidad de seguridad de redes, la cual pareciera ser una especialización de la comunidad azul de la Figura 3.6 que aunque se encuentra presente el 2012–2015, pocas publicaciones se centraban directamente en esta temática. En particular, en este periodo vemos contribuciones diversas.

Por su naturaleza esta comunidad alberga también las comunidades de seguridad de redes inalámbricas y también de detección y mitigación de intrusos y malware que estaba explícitamente presente el periodo 2012–2015.

La Figura 3.9 muestra en lila el grupo de investigadoras e investigadores en biometría en el área ACM de servicios de seguridad, las y los autoras/autores de las comunidades de seguridad de redes y criptografía que toman casi el 50% de las publicaciones de este periodo y que se ve como estando pintados del color de un área, tienen colaboraciones pintadas en la otra. Investigadoras e investigadores de la comunidad de seguridad en

software y aplicaciones en general se mantiene; varios de ellos aparecen también como parte del área de investigación ACM, métodos formales y teoría de la seguridad.

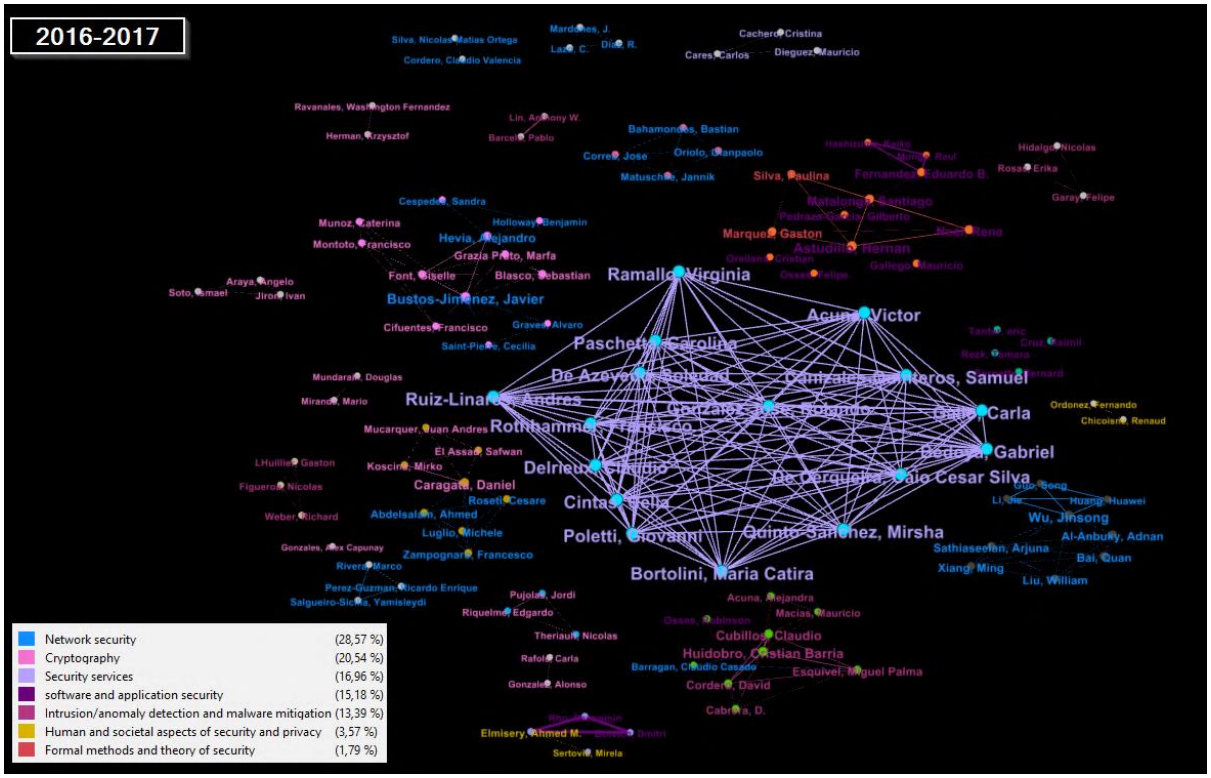


Figura 3.9: Autoras/Autores responsables de las investigaciones consideradas en este estudio publicadas durante periodo 2016–2017.

2018-2019

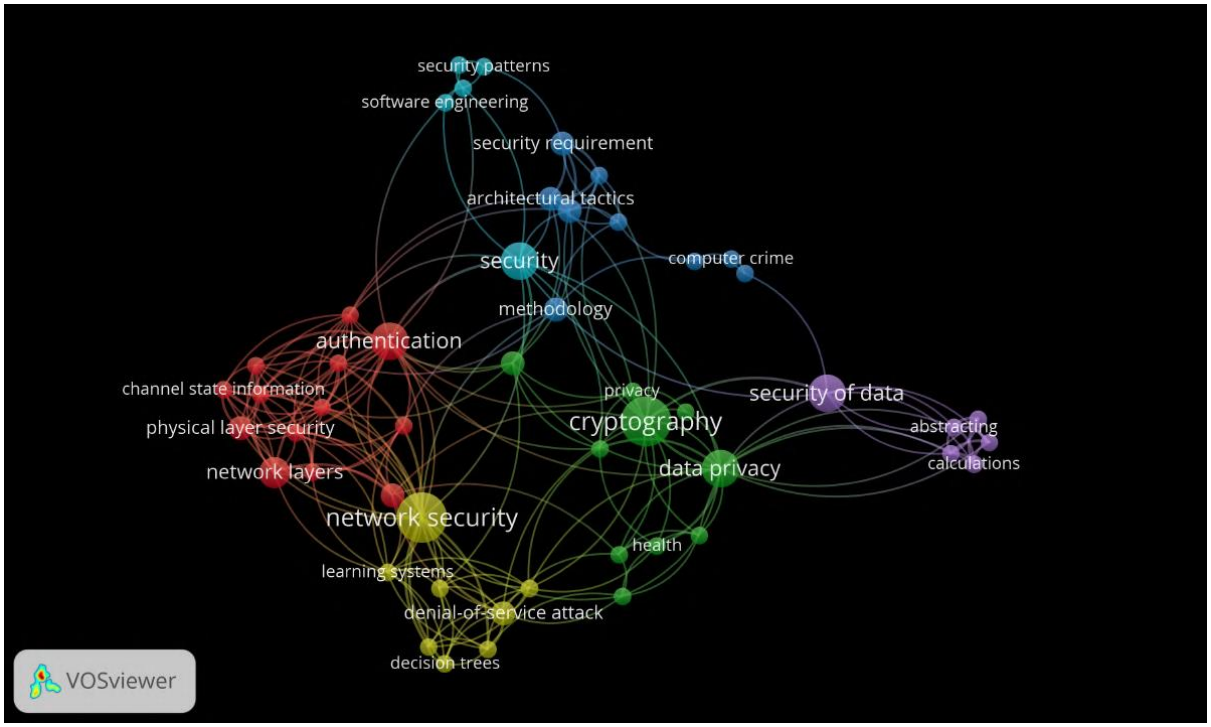


Figura 3.10: Principales tópicos en los que investigadoras e investigadores realizan investigación en periodo 2018–2019.

En la Figura 3.10, en celeste se identifica los tópicos de investigación de las comunidades de seguridad de software y aplicaciones y de métodos formales y teoría de la seguridad.

En la Figura 3.10 podemos ver como tópico relevante la autenticación, el cual es parte del área de investigación servicios de seguridad identificada por la ACM. En Figura 3.10 en parte en rojo, pero principalmente en amarillo, vemos los tópicos de investigación de seguridad en redes hacia los tópicos de investigación del área de detección y mitigación de intrusos y malware.

En Figura 3.10 puede verse en verde la comunidad de criptografía como tópico relevante de investigación durante el periodo 2018–2019 conectado con otros tópicos tales como la privacidad y áreas de aplicación específicas como la salud.

La Figura 3.11 muestra que las comunidades más relevantes en cuanto a cantidad de artículos publicados son un 35% en seguridad en redes y detección y mitigación de intrusos y malware. Luego la comunidad de criptografía con un 21,24% la que se ha mantenido estable en “tamaño” durante los últimos tres periodos. Ahora bien, comunidades como la de seguridad en software y aplicaciones, la de servicios de seguridad, la de aspectos humanos y de sociedad respecto de la privacidad y seguridad, así como la de métodos formales y teoría de seguridad, que representan aproximadamente un 45%, son las que permiten traducir y transferir la investigación al desarrollo de proyectos y productos en la industria, mediante cambios en las

metodologías, generación de nuevas herramientas para usar en los desarrollos, entre otros.

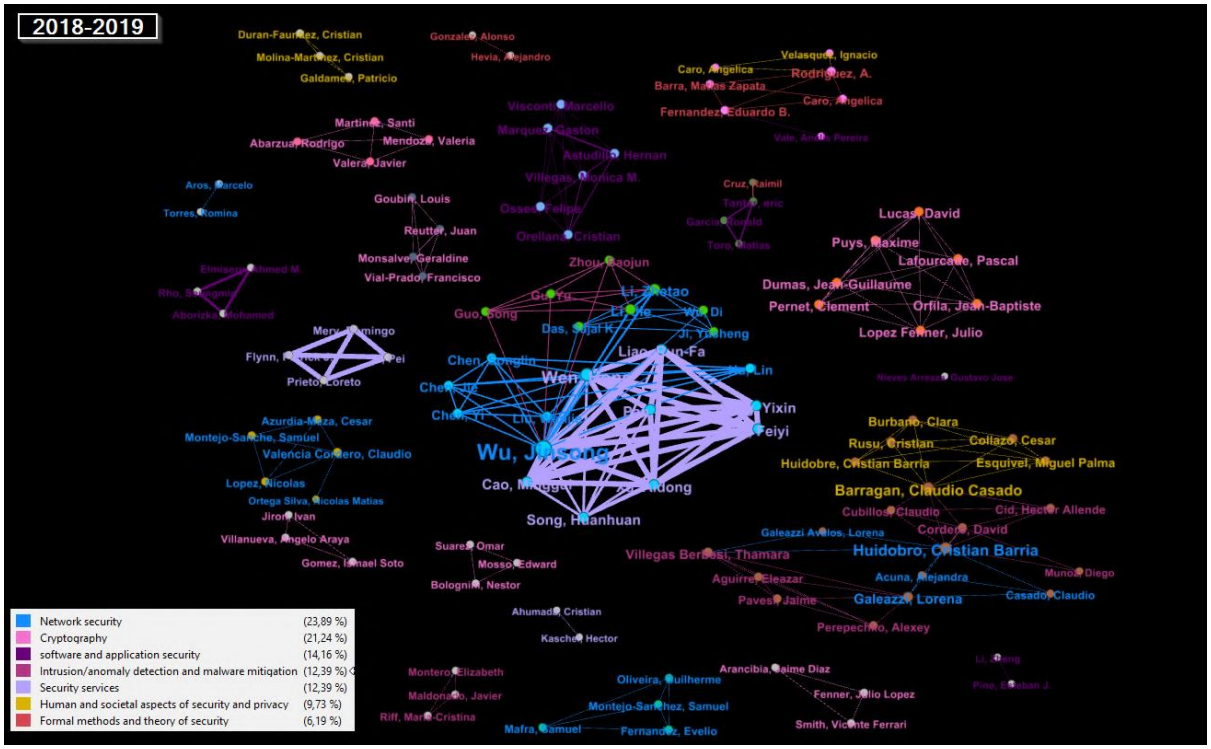


Figura 3.11: Autoras/Autores responsables de las investigaciones consideradas en este estudio publicadas durante periodo 2018–2019.

2020-2021

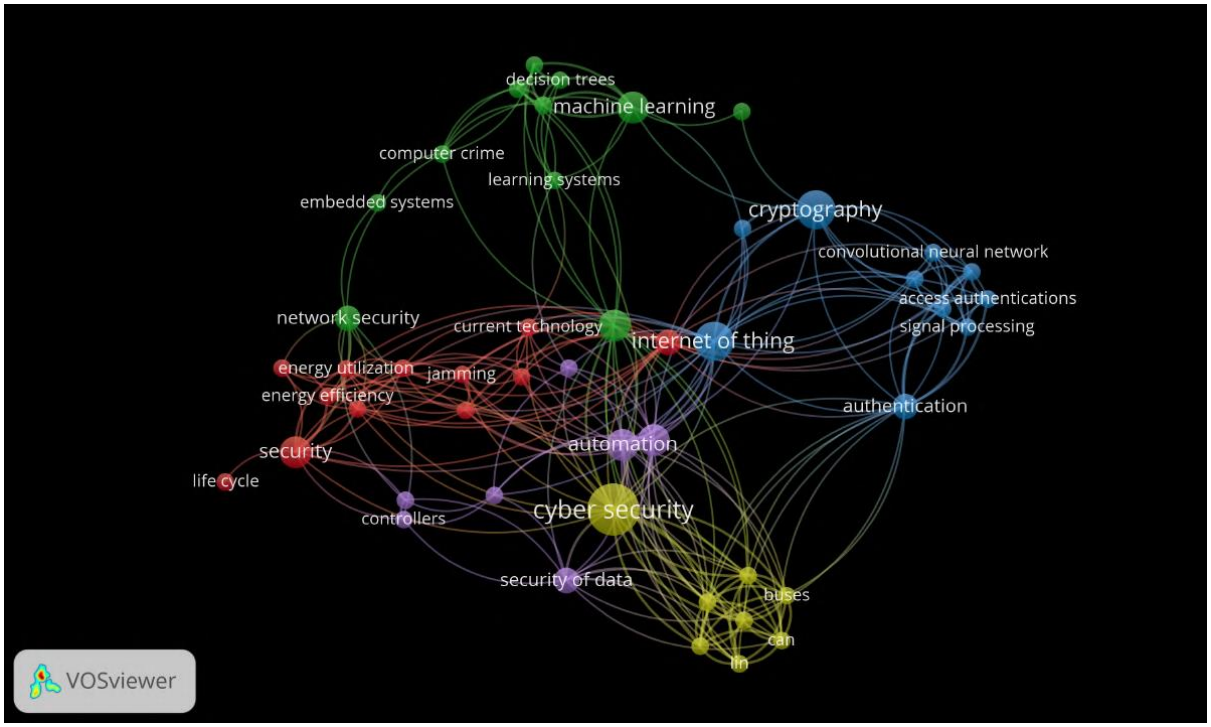


Figura 3.12: Principales tópicos en los que investigadoras e investigadores realizan investigación en periodo 2020–2021.

Aunque aún un tópico de investigación activo, las investigaciones en criptografía comienzan a disminuir frente a otras comunidades durante este periodo. Figura 3.12 muestra a esta comunidad en azul la cual aborda desde la mejora de componentes criptográficos fundamentales hasta la aplicación de principios cuánticos y la preservación de la privacidad en entornos de aprendizaje automático.

Otros tópicos relevantes de investigación siguen siendo la seguridad en redes que aparece en los tópicos en rojo como “jamming” dadas las investigaciones realizadas durante este periodo.

Respecto del área ACM detección y mitigación de intrusos y malware, a pesar de que la Figura 3.12 no muestra explícitamente estos tópicos, sí muestra el tópico ‘machine learning’ que es una rama de la Inteligencia Artificial, “learning systems” como investigación aplicada de lo aprendido en pruebas de conceptos de sistemas para apoyar la toma de decisión o incluso métodos específicos como “decision trees”.

Otros tópicos de investigación en este periodo son ciberseguridad en general, seguridad de datos, autenticación y acceso, además de internet de las cosas. Todos estos relacionados a desarrollar sistemas o software que incluya los resultados de investigación de manera aplicada.

En cuanto a la colaboración de autoras/autores mostrado es posible apreciar que existen más equipos con evidencia de más de una colaboración dado el grosor de ciertas aristas. También es posible a diferencia de periodos anteriores visualizar dentro de este ecosistema presencia de publicaciones en otras áreas identificadas por la taxonomía ACM, tales como seguridad en Hardware y seguridad en sistemas.

2022-2023

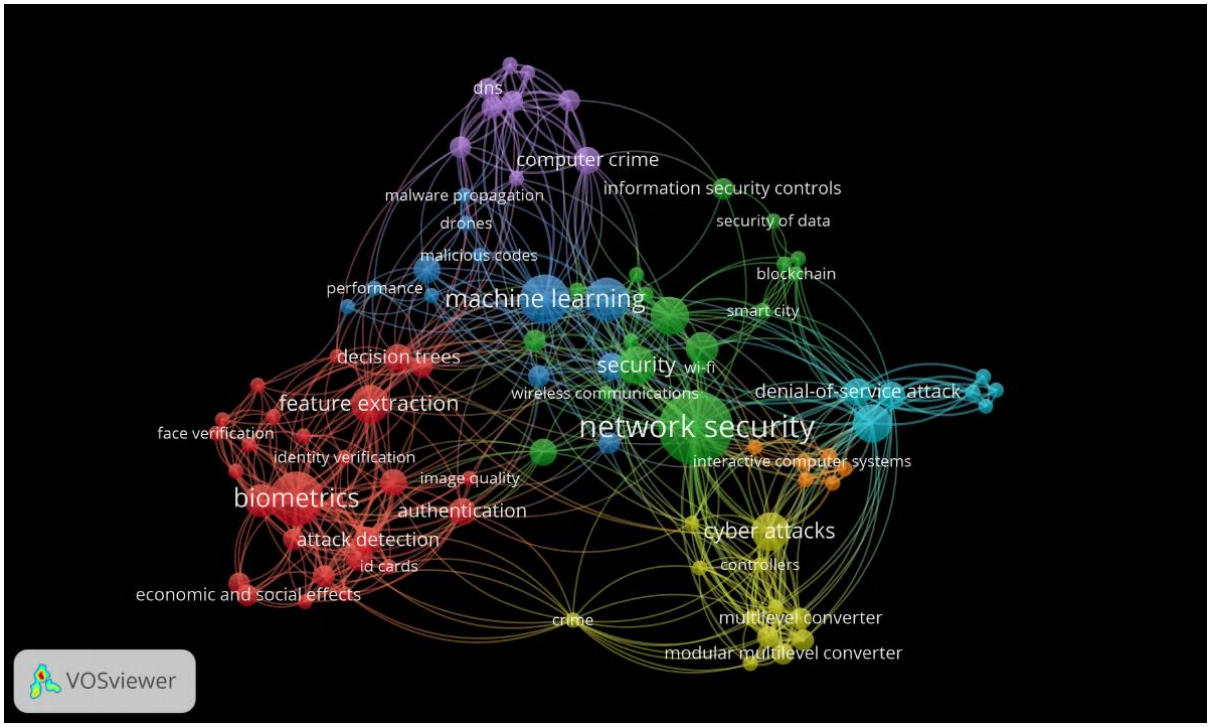


Figura 3.14: Principales tópicos en los que investigadoras e investigadores realizan investigación en periodo 2022–2023.

Durante el periodo 2022–2023, tal como puede apreciarse en la Figura 3.14, la criptografía deja de aparecer como un tópico explícito en el grafo de tópicos de investigación. Esto, no porque desaparezca sino porque respecto de otras investigaciones en ciberseguridad en Chile, es menos frecuente durante este periodo.

Una comunidad importante durante periodo 2022–2023, es la de investigadoras e investigadores chilenas y chilenos en autenticación biométrica y detección de fraudes, la cual es visible en rojo en la Figura 3.14. Vista desde las áreas de investigación de la ACM, se clasifica en servicios de seguridad.

A diferencia de la comunidad de criptografía, en este periodo la comunidad en verde en la Figura 3.14 en seguridad en redes ha crecido, con aportes que se centran desde la comunidad en detección y mitigación de intrusiones y malware hasta la protección de

sistemas ciberfísicos y redes inalámbricas. Importante destacar en la Figura como el tópico machine learning es relevante tanto para esta área como para la de biometría.

Áreas de investigación tales como seguridad en software y aplicaciones experimentan una contracción en este periodo. Existen diversas comunidades de investigación que muestran por el grosor de las aristas que unen a esta/os autoras/autores una alta actividad conjunta en temáticas tanto como seguridad en redes, detección y mitigación de intrusos y malware como en el área de servicios de seguridad.

ÁREAS PRIORITARIAS DE INVESTIGACIÓN

El día martes 12 de diciembre de 2023 el MinCiencia realizó un panel para discutir los resultados del estudio de la "Caracterización de las capacidades de I+D en ciberseguridad en Chile". En esta actividad, se procedió a identificar áreas prioritarias de investigación en Chile para los próximos 5–10 años tomando los siguientes elementos como referencia:

- Capacidades actuales de investigadoras e investigadores con afiliación chilena.
- Prioridades estratégicas en ciberseguridad por una Europa más segura
- Lineamientos del Modelo de Madurez de Capacidades de Oxford

Este capítulo es dividido en tres secciones. La primera, enfocada en cómo alcanzamos el nivel establecido dado el nivel de colaboración actual. La segunda, mirando desde hoy al mediano plazo, qué comunidades han emergido estos últimos 10 años de estudios que deberían seguir potenciándose para poder eventualmente generar comunidades maduras de I+D en el País. Y tercero, en base a las conclusiones y sugerencias del panel dirigido por la autora del estudio, cuáles deben ser los focos en los que debemos trabajar para estar preparados a amenazas actuales y futuras.

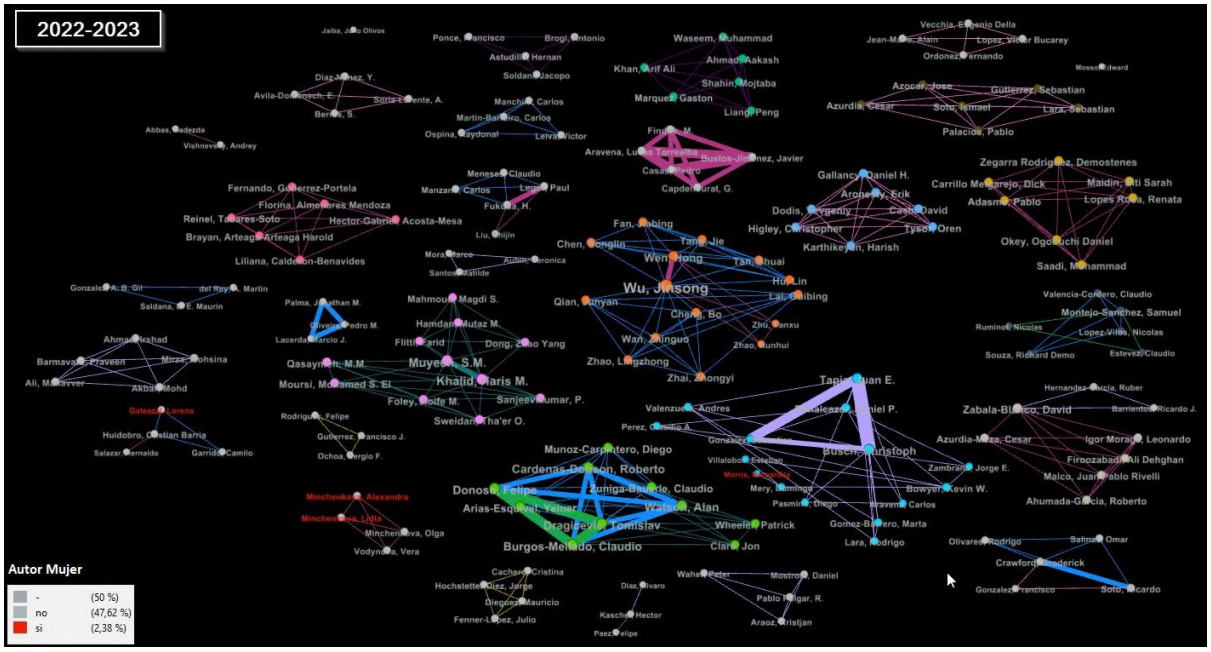


Figura 4.2: Mujeres con afiliación chilena responsables de la producción científica en ciberseguridad en Chile coloreadas en rojo.

Como primer tema, el tema género es un tema preocupante en investigación en ciberseguridad, pues muestra que del 50% de autores y autoras con afiliación chilena, solo el 2.38% son mujeres.

La Figura 4.3 muestra los principales países con los que se colabora en las publicaciones, lo cual puede ser utilizado como estado base para poder fortalecer la colaboración internacional que se requiere para tener el factor D3.4 un nivel de madurez establecido en el corto plazo.

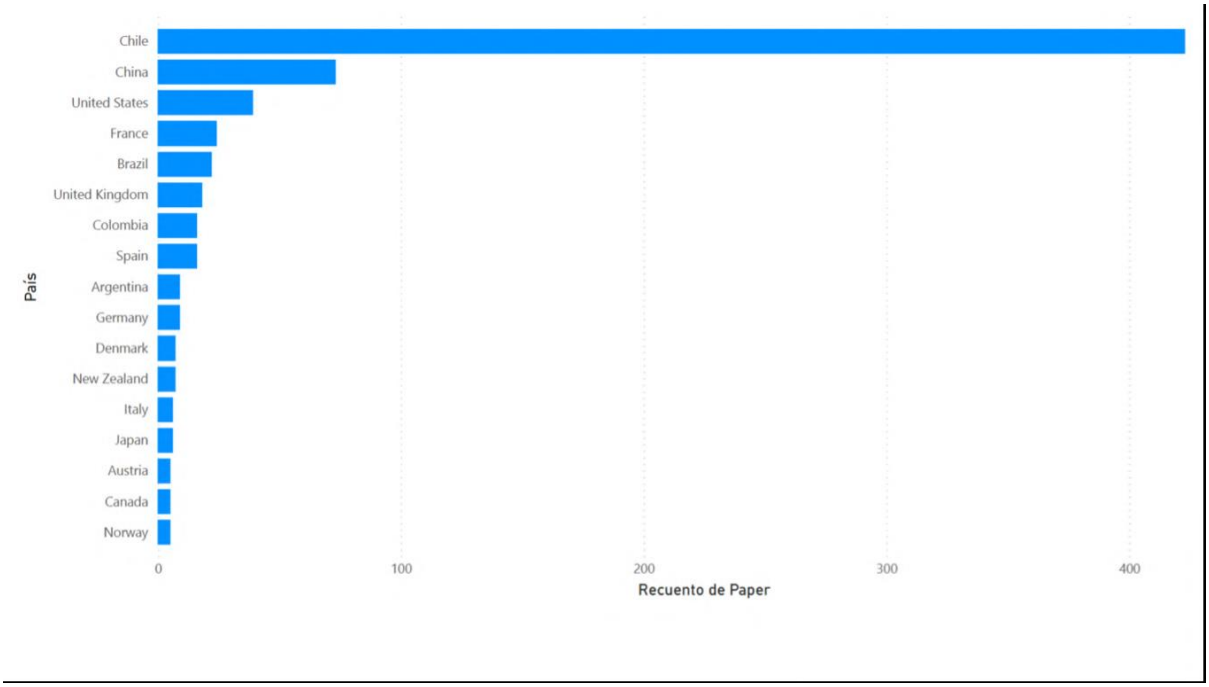


Figura 4.3: Los países con los que Chile compartió autoría para artículos publicados en el periodo 2012–2023.

Tal como se ve en la Figura 4.4 las mayores capacidades de investigación durante los últimos 10 años se ven en criptografía, en seguridad en redes utilizando inteligencia artificial para la detección de intrusos o malware y en métodos formales para el desarrollo seguro de software y aplicaciones. Esto se condice con lo que se aprecia en la Figura 4.5 que muestra por cada área de la ACM, el foco que ha dado la comunidad científica en generar conocimiento durante los cinco periodos del estudio. Por ejemplo, la comunidad de criptografía vemos que se mantiene presente durante toda la evolución de la investigación en ciberseguridad en Chile, donde respecto del total que se publica en los diferentes periodos, vemos que desde 2020 se ha ido contrayendo respecto de otras comunidades, por ejemplo la de intrusión y mitigación de intrusos y malware, la cual muestra el mayor crecimiento el periodo 2020–2021, dado en general el uso importante de Inteligencia Artificial en esta área. Por otro lado, alineado a que Chile posea las capacidades para desarrollar productos y servicios, vemos el área de servicios de seguridad con un gran potencial dado los resultados de diversos investigadores e investigadoras con foco en temas de autenticación y biometría usando Inteligencia Artificial. Respecto del desarrollo de software y en general soluciones ciberfísicas seguras, áreas de la ACM importantes son por un lado, la seguridad de software y aplicaciones en conjunto con la de métodos formales y teoría de la seguridad que permiten apoyar las etapas de diseño y desarrollo, en conjunto con el área seguridad en redes para apoyar con conocimiento su despliegue seguro, así como el área de Aspectos humanos y de sociedad en seguridad y privacidad para el adecuado alineamiento de las soluciones con las personas usuarias. En general, las áreas más descendidas o con menos resultados declarados son seguridad en hardware y seguridad de sistemas a

excepción en este último de investigaciones relacionadas a ataques de denegación distribuido de servicios.+

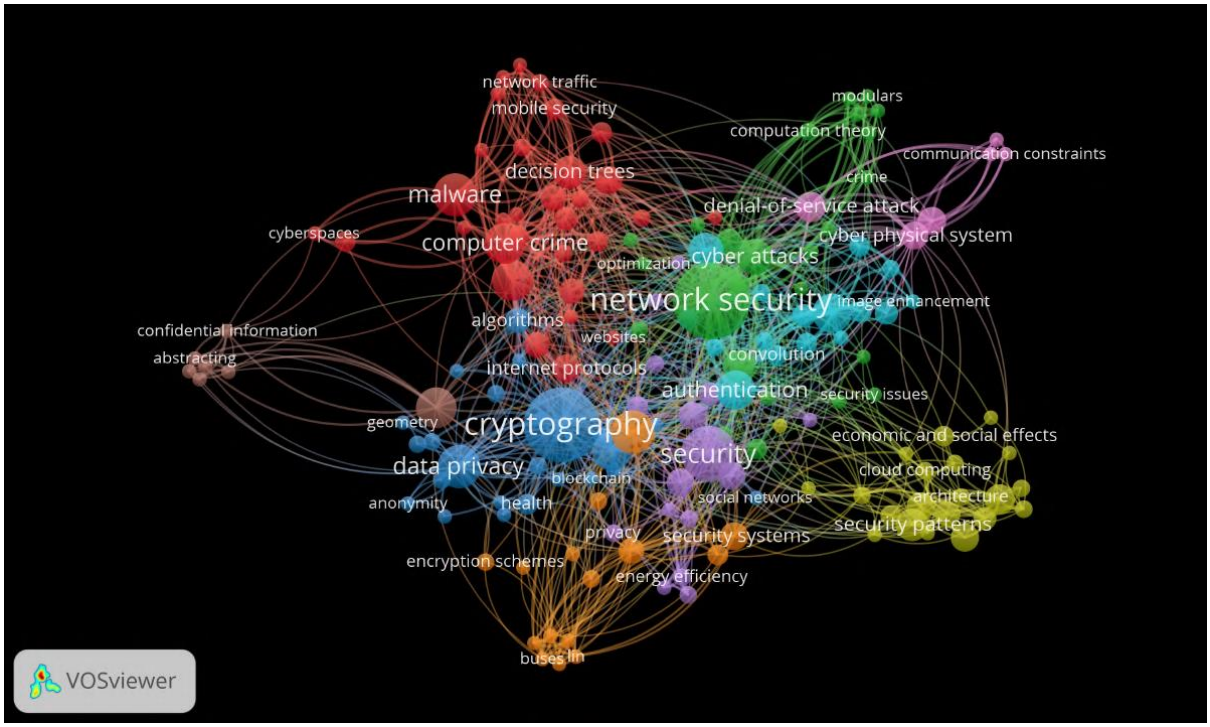


Figura 4.4: Principales tópicos en los que investigadores en publicaron resultados durante periodo 2012–2023

Durante el panel se plantearon las principales conclusiones respecto de la investigación y se delinearon áreas necesarias de investigación reconocidas por la Agenda Europea de investigación y desarrollo en ciberseguridad de España. A continuación se introducen las cuatro áreas prioritarias.

La primera área fue Criptografía postcuántica. La posibilidad de que las computadoras cuánticas superen las actuales medidas de seguridad criptográfica plantea una amenaza existencial, socavando la seguridad en transacciones digitales, comercio electrónico y gobierno electrónico. Los investigadores e investigadoras deben enfocarse en técnicas para resistir ataques mediante la computación cuántica, conocida como criptografía poscuántica o Criptografía Cuánticamente Segura (QSC).

La segunda área de priorización es el desarrollo seguro de sistemas ciberfísicos, de manera de mitigar desde su diseño hasta su despliegue amenazas y vulnerabilidades tanto de componentes de software como físicos mediante decisiones de diseño de desarrollo de sistemas ciberfísicos seguros por defecto. En esta área de investigación prioritaria es necesario considerar: Seguridad en hardware, Servicios de seguridad (Control de acceso, autenticación, autorización, gestión de derechos digitales, pseudonimato, anonimato e inrastreabilidad, no repudio además de protocolos de

preservación de la privacidad y seguridad en todas las capas del modelo OSI (no solo a nivel de aplicación); Métodos Formales y Teoría de la Seguridad y Diseño de Sistemas Ciberfísicos Seguros y Seguridad de base de datos y almacenamiento de Sistemas Ciberfísicos Seguros.

Una tercera arista es la Sinergia bidireccional entre IA y ciberseguridad. La inteligencia artificial (IA) desempeña un papel crucial en la ciberseguridad. Existe una comunidad activa de investigación en desarrollo de métodos y herramientas para detectar intrusos, malware y ataques en general mediante Inteligencia Artificial tanto a sistemas físicos, como ciberfísicos como sólo de software. Lamentablemente, en la otra dirección, existe casi nulos resultados publicados en la ciberseguridad para los sistemas de IA que aborden amenazas de envenenamiento de datos de entrenamiento, robo y/o envenenamiento de modelos, manipulación de la cadena de suministro, de las entradas, salidas, entre otros.

Como último punto se aborda la Educación. Esta área se centra en el desarrollo de estrategias innovadoras para promover la conciencia y comprensión de la ciberseguridad, así como en la investigación de aspectos humanos y sociales relacionados. Los investigadores deben trabajar en:

- Crear herramientas interactivas y educativas que ayuden a las organizaciones y usuarios a comprender la importancia de la ciberseguridad.
- Investigación en Aspectos Humanos y Sociales:
- Diseñar campañas de concientización que sean efectivas y adaptables a diversos públicos, destacando los riesgos y mejores prácticas de seguridad.
- Investigar y mejorar la usabilidad de las soluciones de seguridad, asegurándose de que sean accesibles y comprensibles para usuarios con diversos niveles de conocimiento técnico.
- Enfoque Interdisciplinario para abordar los desafíos humanos y sociales, garantizando que las soluciones sean efectivas, respeten la privacidad y sean adoptadas de manera generalizada.