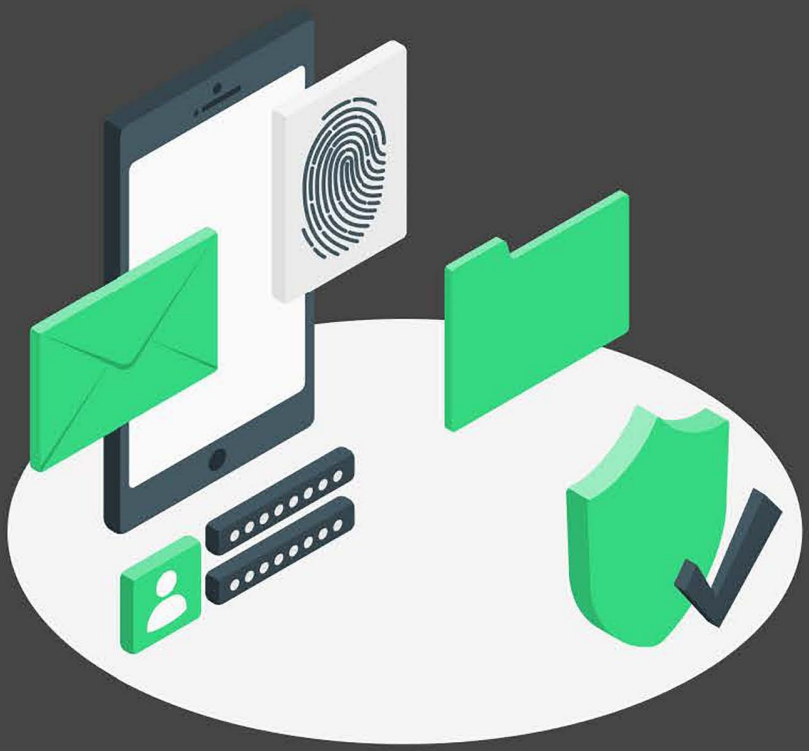
Ministerio de Ciencia, Tecnología, Conocimiento e Innovación

Gobierno de Chile

MinCiencia

Informe **I + D** en Ciberseguridad

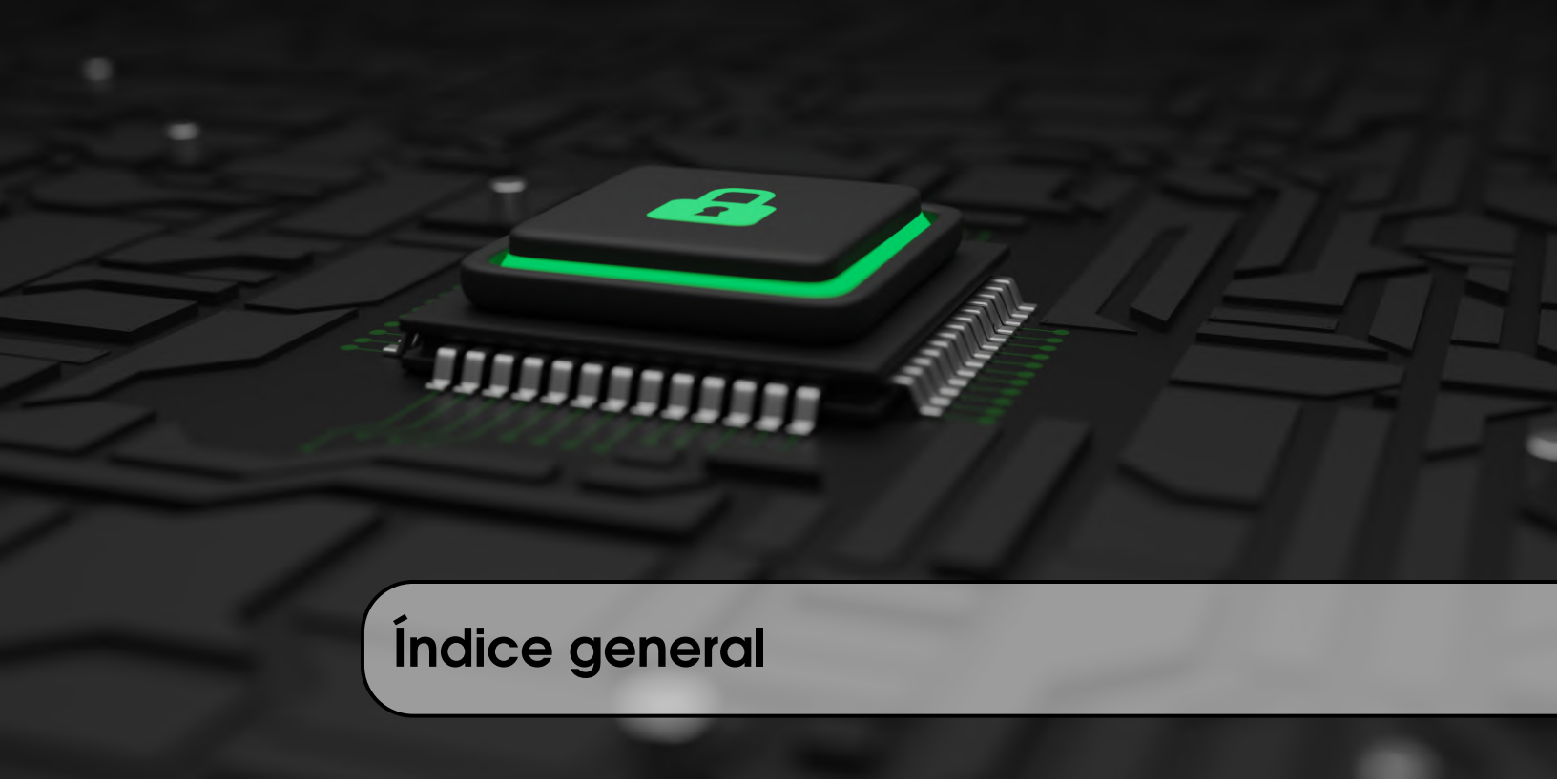


Este documento ha sido preparado para el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación (CTCI) en el marco de los compromisos adquiridos en la mesa interministerial de ciberseguridad en el marco de la creación de la política nacional de ciberseguridad 2023–2024 en colaboración con CSIRT.

Autora: Romina Torres Torres.
Colaboradores del Informe: Fabiola Herrera Leiva, Bruno Reyes Sánchez, Ana García Gutiérrez y Claudio Canales Pavez.
Equipo editor MinCiencia: Carla Carrera Galdames, Catalina Terra Rosas y Daniela Vera Puga.
Equipo editor CSIRT: Cristian Bravo Lillo y Eduardo Riveros Roca.

Fecha de publicación: Enero de 2024.

Imágenes de inicio de capítulos diseñadas por Freepik `https://www.freepik.es`.



Índice general

1. Introducción

El “Modelo de Madurez de Capacidades de Ciberseguridad para Naciones” (CMM, por sus siglas en inglés: “Cybersecurity Capability Maturity Model for Nations”) es un marco desarrollado para evaluar la madurez de las capacidades de ciberseguridad de una nación. En particular, el “Factor D3.4: Investigación e Innovación en Ciberseguridad” se refiere a la **capacidad de una nación para llevar a cabo investigaciones avanzadas y promover la innovación en el campo de la ciberseguridad**. Acorde a la Agencia de la unión Europea para Ciberseguridad, “Un investigador o investigadora en Ciberseguridad es aquel o aquella que investiga en materias de ciberseguridad e incorpora estos resultados en soluciones de ciberseguridad”.

En el capítulo de Investigación Avanzada en Ciberseguridad del Libro “Construyendo la Ciberseguridad en Chile” [1], se presentaron entre otras, dos iniciativas prioritarias: *Centro Nacional de Investigación en Ciberseguridad* y *Centro de Escalamiento y nuevos negocios en torno a los resultados de Investigación en Ciberseguridad*. Investigación y desarrollo de base científico tecnológica es lo que el país necesita para aumentar su nivel de madurez en I+D en ciberseguridad, lo cual se alinea con el eje “fomento a la industria y la investigación científica” de la Política Nacional de Ciberseguridad 2023-2028 de Chile. Ambos programas tributan a los pilares de capacidades de investigación y capacidades de innovación, desarrollo tecnológico aplicado y negocios. El primero busca tener equipos de investigadoras e investigadores de diferentes niveles (tanto actuales, nuevos o nuevas, o aquellos o aquellas que se reconvierten de áreas afines, como de otras disciplinas de aplicación) colaborando para abordar desafíos y amenazas prioritarias para el país, que permita generar capacidades en esta materia en diferentes verticales. El segundo programa, busca reunir investigadoras e investigadores con las necesidades de la Industria en torno a proyectos colaborativos nacionales y/o internacionales de manera de incubar y escalar desarrollos de base científico tecnológico al mercado nacional y eventualmente internacional; esto con el fin de facilitar el desarrollo de la industria de productos y servicios de base científico tecnológica en el área de ciberseguridad en Chile que ayude a posicionar al país en innovación, en la investigación aplicada y

en el desarrollo tecnológica en ciberseguridad.

Por lo tanto, en este trabajo de caracterización de la I+D en ciberseguridad en Chile nos concentramos en levantar el estado base de investigación en ciberseguridad en Chile, ya sea realizada por investigadoras o investigadores alrededor de comunidades nacionales o internacionales que se desempeñen en laboratorios, Instituciones de Educación Superior, centros de investigación en ciberseguridad públicos y/o privados, ya sean especializados, afines o al menos con actividad científica que lo demande de manera transversal.

Los objetivos de este informe son levantar 1) el estado actual en investigación y potencial desarrollo en ciberseguridad del país por medio de un estudio bibliométrico que nos permita visualizar los principales tópicos de investigación así como su evolución los últimos 10 años; 2) las redes de investigación en ciberseguridad alrededor de estos tópicos, así como sus colaboración internacionales a partir de las publicaciones conjuntas; y 3) identificar al menos tres áreas relevantes en I+D que deban priorizarse y fomentarse desde la política pública, a partir del resultado de los dos puntos anteriores como de la opinión de investigadoras e investigadores del área citados a un panel exclusivo para ello.

Este documento se organiza como sigue. El capítulo 2 revisa trabajos similares que han identificado áreas prioritarias de investigación en diferentes países. El capítulo 3 presenta el método bibliométrico aplicado para caracterizar la investigación desarrollada por la comunidad científica de Chile en ciberseguridad los últimos 10 años. La revisión considera artículos (artículos publicados en revistas, conferencias, capítulos de libros y revisiones) en idioma inglés o español obtenidos de la Base de Datos Científica Scopus, periodo 2012-2023. En el Capítulo 4 partimos de la base que todas las áreas de investigación en seguridad y privacidad son necesarias, pero que en el caso que deban priorizarse, se presentan cuatro áreas prioritarias. El capítulo 5 delinea las principales conclusiones y sugiere trabajo futuro para seguir profundizando en el levantamiento de las capacidades I+D en ciberseguridad de Chile.

2. Estado del Arte

2.1 Estudios sistemáticos de literatura científica que muestran la investigación en ciberseguridad de un País

Tanto India como México han realizado un análisis sistemático de la literatura en investigación en ciberseguridad.

En el caso de India [2], se realiza un estudio sistemático que examinó 989 publicaciones provenientes de la fuente de datos Scopus. La identificación del país de origen se basó en las afiliaciones enumeradas en las publicaciones en lugar de la nacionalidad del autor. Acorde al mismo estudio, 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. Importante mencionar que las investigadoras y los investigadores de India publican sus hallazgos de investigación tanto en forma de artículos de conferencia como artículos de revista. Sin embargo, es importante destacar que seis de las principales revistas/conferencias donde se han publicado los resultados, fueron excluidas de la cobertura de Scopus. Los tres autores más productivos provienen de Amrita Vishwa Vidyapeetham, la institución india más productiva en ciberseguridad, que también cuenta con centros de excelencia en este campo. También 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.

Por otro lado, las investigaciones en ciberseguridad en México [3] 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 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. Se cree que los esfuerzos colaborativos interinstitucionales pueden fortalecer la investigación en este campo. 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: Seguridad Cibernética, TIC y Protección de Datos, Seguridad de la Información, Ciberespacio y Seguridad del Estado.

2.2 Principales focos prioritarios de investigación en ciberseguridad declarados en Europa

El documento *"Analysis of the European R&D priorities in cybersecurity: Strategic priorities in cybersecurity for a safer Europe"* [4] publicado en Diciembre del 2018 identificó las amenazas de ciberseguridad para la sociedad europea y determinó las prioridades en la investigación que debían ser conducidas para mitigarlas antes de que se materialicen:

- **Inteligencia Artificial (IA)**: el diseño deficiente de sistemas de IA puede causar un comportamiento inseguro y perjudicial, por lo que diversos desafíos deben ser abordados.
  - Validez: Cómo garantizar que un sistema que cumple con sus requisitos formales no tenga comportamientos y consecuencias no deseados como efectos secundarios negativos;
  - Seguridad: Cómo prevenir la manipulación intencional o no intencional por parte de partes no autorizadas tales como manipulaciones para obtener recompensas o beneficios;
  - Control: Cómo permitir un control humano significativo sobre un sistema de IA después de que comienza a operar;
  - Trazabilidad: Cómo poder rastrear cómo el sistema de IA ha tomado una cierta decisión.

  Acorde a este documento, todos estos problemas pueden abordarse de manera más efectiva a través de una IA robusta y explicativa, que tiene como objetivo producir modelos más explicables de manera que los humanos puedan entender el razonamiento, confiar en los resultados y prever cómo se comportará la IA en el futuro. La investigación debería centrarse en el desarrollo de técnicas de IA que produzcan modelos más explicables sin comprometer la precisión de las predicciones (comúnmente denominada en la investigación como Inteligencia Artificial Explicable). Otra área que requiere investigación es en aplicaciones donde el aprendizaje automático es no supervisado y hay interacción con personas, donde los estudios han mostrado sesgos y resultados injustos imponiendo el desafío sobre cómo construir una IA inclusiva y no discriminatoria. Por último, la falta de robustez de la IA en ambientes productivos, demanda actualmente investigación en cómo la IA generativa y adversarial permite aumentar la robustez del modelo resultante antes muestras anteriormente no vistas.
- **Tecnologías cuánticas**: donde la incertidumbre es una característica clave, pueden utilizarse

tanto en ataques contra los métodos de protección criptográfica actuales como en el desarrollo de nuevos modelos computacionales para una mayor aceleración del cambio. El trabajo de las investigadoras y de los investigadores debería centrarse en técnicas para resistir ataques utilizando la computación cuántica, conocida como criptografía poscuántica o Criptografía Cuánticamente Segura (QSC). Esta área de investigación se centra en desarrollar métodos de cifrado que sigan siendo seguros incluso en un entorno en el que la computación cuántica puede amenazar las técnicas de cifrado convencionales. Técnicas que aprovechan efectos cuánticos en la Distribución Cuántica de Claves (QKD). Estas técnicas se basan en los principios de la mecánica cuántica y se utilizan para la generación de claves de cifrado seguras mediante la explotación de propiedades cuánticas, lo que las hace resistentes a ciertos tipos de ataques.

- **La complejidad de la interconexión que puede llevar a la falla en cascada de múltiples sistemas a lo largo de la cadena de suministro**. Se requiere investigación en desarrollo de nuevos enfoques para evaluar el impacto de dependencias e interdependencias y la definición de interfaces seguras e interoperables entre diferentes infraestructuras críticas para prevenir efectos en cascada.
- **Ciberdelincuencia**: desarrollo de enfoques novedosos para proporcionar a las organizaciones la conciencia situacional adecuada en relación con las amenazas de ciberseguridad, lo que les permite detectar y responder de manera rápida y efectiva a ataques cibernéticos sofisticados, así como desarrollo de técnicas novedosas para recopilar información forense.
- **Investigación y desarrollo de predicción de malware/ataques mediante análisis de datos y predicción automática**. Esto requerirá la creación de conjuntos de datos muy grandes y actualizados de malware etiquetado para entrenar al predictor automático.
- **Privacidad versus "big data"**: se requieren nuevos modelos y métodos de privacidad para la anonimización, nuevas herramientas de análisis en las que se aplique el principio de minimización de datos, ademas de un nuevo modelo de mecanismos de protección siguiendo los requisitos de privacidad por diseño y por defecto.

Un nuevo documento publicado por la misma agencia en 2022 *"Research and Innovation Brief; Annual Report on Cybersecurity Research and Innovation Needs and Priorities"* [5] actualiza 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 aumentar la 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); Compiladores que produzcan código eficiente y seguro para cálculos de múltiples partes y código protegido por HE; Estandarización de esquemas de HE y protocolos de cálculo de múltiples partes; Aceleración de hardware de protocolos de cálculo de múltiples partes y esquemas de HE; Nuevas suposiciones y resultados imposibles derivados de matemáticas, física o limitaciones de hardware, como base para la criptografía futura; Implementaciones seguras de sistemas criptográficos que resistan ataques de canales laterales.

- **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.

2.3 Principales focos prioritarios de investigación en ciberseguridad declarados por el Libro "Construyendo la Ciberseguridad en Chile"

El capítulo de investigación avanzada en ciberseguridad del Libro "Construyendo la Ciberseguridad en Chile" [1] presentó como propuestas las siguientes comunidades de investigación:

- 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 (e.g. Smart Health),
- regulaciones,
- legislación,
- Ciberseguridad por diseño,
- Privacidad por diseño.

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

La Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC) es una asociación sectorial que agrupa a centros de investigación y otros agentes del ecosistema investigador en ciberseguridad de España que nace en 2015 para abordar los desafíos propios de un ecosistema emergente, no articulado, dinámico y distribuido en diversas líneas de investigación como puede apreciarse en la Figura 2.1.

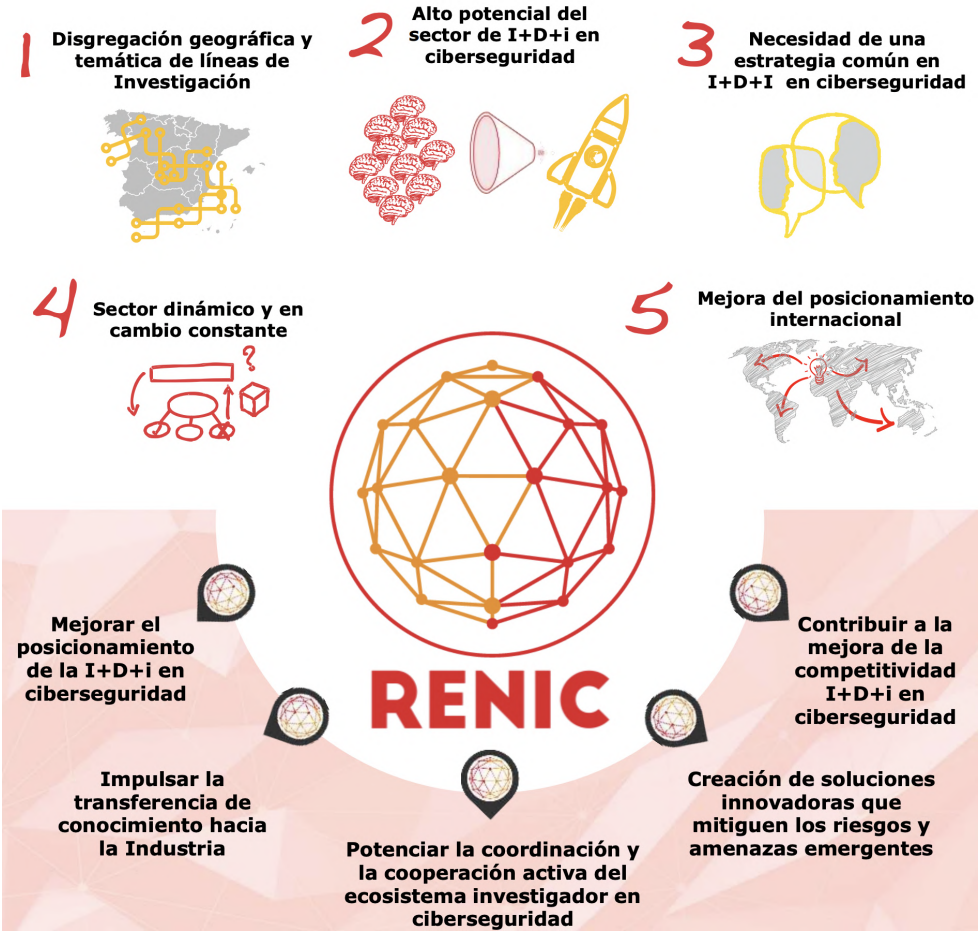


Figura 2.1: Propuesta RENIC de España ante los desafíos de la I+D+i en ciberseguridad. Fuente: RENIC `https://www.renic.es/sites/default/files/Infografia_RENIC.pdf`

Su objetivo principal es fomentar la I+D+i en el sector de la ciberseguridad, potenciando la colaboración, la transferencia y la excelencia de sus miembros. RENIC busca posicionar la I+D+i nacional en ciberseguridad a nivel europeo e internacional, participar en la definición de las políticas de investigación, mejorar la conexión con la industria, representar los intereses del colectivo, promover la difusión y el desarrollo de profesionales en ciberseguridad, facilitar la financiación y realizar otras actividades necesarias para alcanzar sus fines. Cubre el ciclo completo de la innovación haciendose cargo de identificar retos en ciberseguridad a resolver por el ecosistema permitiendo incubar ideas así como también de crear nodos de especialización en I+D+i en ciberseguridad potenciando la sinergia de los socios así como la colaboración con la Industria para la transferencia de conocimiento.

La RENIC libera regularmente infografías respecto de ella. En este trabajo comparamos las infografías liberadas en 2017 [1] y en 2022 [2] a fin de comparar las materias en las que investiga la red desde su creación. Dado que la segunda infografía es para el último cuartil del 2022,

[1] Infografía 2017: `https://www.incibe.es/sites/default/files/paginas/red-excelencia/estudios-caracterizacion/201701_catalogo_infografia.pdf`

[2] Infografía 2022: `https://www.renic.es/sites/default/files/RENIC_Infografia2022_ES.pdf`

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, pero también a que cada socio para unirse y mantenerse debe demostrar y acreditar la excelencia investigadora en ciberseguridad, lo cual al inicio pudo tener menos requisitos que en la actualidad. c

Áreas de investigación	2017	2022
Sistemas fiables y actualizables	64 %	-
privacidad	50 %	-
procesado de datos	46 %	-
infraestructura crítica	45 %	
evaluación de sistemas y ciberriesgos	41 %	
ataque y defensa ante amenazas	37 %	
gestión de la identidad	35 %	
criptografía	28 %	28 %
fomento y concienciación de la seguridad	22 %	
seguridad de redes	21 %	44 %
cloud computing	17 %	28 %
Internet de las cosas	15 %	44 %
análisis de datos a gran escala		30 %
autenticación criptografíca		34 %
protocolos criptográficos preservar privacidad		32 %
detección de anomalías		30 %
elaboración de mecanimos de respuesta ante ataques		24 %
control de acceso y autenticación		34 %
privacidad en iot		30 %
seguridad/privacidad mediante el diseño		26 %

Cuadro 2.1: Temáticas de investigación de la RENIC - Comparación 2017 con 2022.

El Cuadro 2.1 muestra que en 2017 uno de los principales foco de investigación era concienciación de la seguridad así como investigación en cómo evaluar los sistemas y ciberriesgos. Otros temas relevantes fueron investigar en cómo lograr sistemas fiables y actualizables, así como investigación en ciberseguridad en infraestructura crítica, lo cual demanda investigación específica en temáticas de cómo asegurar la confidencialidad e integridad de los datos tanto en reposo, durante su procesamiento, como en tránsito en grandes sistemas distribuidos, así como se asegura su propia disponibilidad. Por este motivo o por la demanda en general del mercado, la RENIC investiga en 2017 respecto de 1) seguridad de redes, seguridad en cloud computing y seguridad en internet de las cosas; 2) privacidad

de datos, procesado de datos, y criptogragía; y 3) ataque y defensa ante amenazas así como la gestión de la identidad para reducir probablemente los accesos no autorizados que pueden traducirse en ataques de diferente tipo.

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. Dada la proliferación de ataques exitosos a sistemas y grandes infraestructuras resultantes en 1) exfiltración de datos: RENIC presenta mayor investigación en temáticas de protocolos criptográficos para preservar privacidad, privacidad en IoT y criptografía y 2) no disponibilidad de servicios: RENIC presenta mayor actividad de investigación en 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.

3. Redes de Colaboración

El primer artículo con al menos un autor con afiliación chilena que aparece como resultado a la búsqueda realizada es Demonstrating possession of a discrete logarithm without revealing it de los autores Chaum D.; Evertse J.-H.; van de Graaf J.; Peralta R. Año 1987 clasificado en Criptografía, específicamente en Mathematical foundations of cryptography, donde el autor chileno ***René Peralta*** *estaba afiliado al momento de la publicación a la Facultad de Matemáticas de la Universidad Católica de Chile.*

En este trabajo utilizamos la bibliometría para evaluar la investigación desarrollada por la comunidad científica de Chile en ciberseguridad. Para ello realizamos una revisión de la literatura respecto de la pregunta en qué temáticas de la ciberseguridad investigan las investigadoras y los investigadores con afiliación en Chile. Los materiales o conjunto de datos utilizados en este estudio son artículos publicados en revistas, conferencias, capítulos de libros y revisiones en idioma inglés o español obtenidos de la Base de Datos Científica Scopus, periodo 2012–2023.

En este capítulo primero entregamos 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.

Limitaciones o Trabajo Futuro: en este estudio hemos seleccionado Scopus en vez de Web of Science (WoS), debido a que Scopus ofrece una lista más amplia de fuentes, cubre un mayor número de revistas de menor impacto, especialmente de países no anglosajones, tiene un mayor índice de citas por artículo que WoS, lo que puede indicar una mayor visibilidad de las publicaciones. Ahora bien, Scopus no incluye todos los artículos indexados por WoS, dado que posee diferentes criterios de selección y cobertura de las revistas científicas, pero según un estudio de 2019, Scopus cubría el 93 % de las revistas de WoS, pero solo el 79 % de los artículos de WoS (probablemente porque

Scopus ofrece una cobertura temporal más reciente que WoS). **Como trabajo futuro se recomienda utilizar ambas bases de datos e incluso otras como scielo para obtener una visión más completa y precisa de la producción científica**.

3.1 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.

Nomenclatura palabra-clave,número (donde el número será el número de ocurrencia en todos los artículos

(KEY(security AND privacy) OR KEY(cybersecurity) OR KEY(social AND engineering AND attacks) OR KEY(spoofing AND attacks) OR KEY(phishing) OR KEY(computer AND crime) OR KEY(identity AND theft) OR KEY(malware) OR KEY(spyware AND crime) OR KEY(computer AND forensics) OR KEY(surveillance AND mechanisms AND cybersecurity) OR KEY(forensics AND investigation AND techniques) OR KEY(forensic AND ((evidence AND collection) OR storage OR analysis)) OR KEY(network AND forensics) OR KEY(system AND forensics) OR KEY(forensics AND data AND recovery) OR KEY(cyberwarfare) OR KEY(hci AND user AND models AND cybersecurity) OR KEY(hci AND (design OR evaluation OR methods) AND cybersecurity) OR KEY(user AND studies AND cybersecurity) OR KEY(usability AND testing AND cybersecurity) OR KEY(heuristic AND evaluations AND cybersecurity) OR KEY(walkthrough AND evaluations AND cybersecurity) OR KEY(laboratory AND experiments AND cybersecurity) OR KEY(field AND studies AND cybersecurity) OR KEY(interaction AND design AND process AND methods) OR KEY(user AND centered AND design AND cybersecurity) OR KEY(activity AND centered AND design AND cybersecurity) OR KEY(smartphones AND cybersecurity) OR KEY(mobile AND devices AND cybersecurity) OR KEY(cryptography) OR KEY(cryptanalysis) OR KEY(information-theoretic AND techniques AND cybersecurity) OR KEY("key.AND management) OR KEY(public AND "key") OR KEY(asymmetric) OR KEY(digital AND signatures) OR KEY(public AND "key.AND encryption) OR KEY(symmetric AND cryptography) OR KEY(hash AND function) OR KEY(stream AND ciphers) OR KEY(block AND ciphers) OR KEY(encryption) OR KEY(message AND authentication AND codes) OR KEY(database AND security) OR KEY(storage AND security) OR KEY(data AND anonymization) OR KEY(data AND sanitization) OR KEY(database AND activity AND monitoring) OR KEY(information AND accountability) OR KEY(usage AND control) OR KEY(management AND encrypted AND data) OR KEY(querying AND of AND encrypted AND data) OR KEY(formal AND security AND methods) OR KEY(theory AND of AND security) OR KEY(formal AND security AND models) OR KEY(logic AND verification AND cybersecurity) OR KEY(security AND requirements) OR KEY(trust AND framework) OR KEY(human-centric AND cyber AND security) OR KEY(human-centric AND cybersecurity) OR KEY(human AND aspects AND of AND security AND privacy) OR KEY(societal AND aspects AND of AND security AND privacy) OR KEY(economics AND of AND security) OR KEY(economics AND of AND privacy) OR KEY(privacy AND protection) OR KEY(social AND aspects AND of AND security) OR KEY(social AND aspects AND of AND privacy) OR KEY(usability AND in AND security) OR KEY(usability AND in AND privacy) OR KEY(anomaly AND detection) OR KEY(intrusion AND detection AND cybersecurity) OR KEY(malware AND detection) OR KEY(intrusion AND mitigation) OR KEY(intrusion AND detection AND systems) OR KEY(malware AND its AND mitigation) OR KEY(social AND engineering AND attacks) OR KEY(phishing) OR KEY(spoofing AND attacks) OR KEY(network AND security) OR KEY(denial-of-service AND attacks) OR KEY(firewalls) OR KEY(mobile AND security) OR KEY(wireless AND security) OR KEY(security AND protocols) OR KEY(web AND protocol AND security) OR KEY(security AND in AND hardware) OR KEY(hardware AND security) OR KEY(embedded AND systems AND security) OR KEY(spoofing AND attacks) OR KEY(hardware AND attacks) OR KEY(malicious AND design AND modifications) OR KEY(side-channel AND analysis AND cybersecurity) OR KEY(side-channel AND countermeasures AND cybersecurity) OR KEY(hardware AND reverse AND engineering) OR KEY(hardware AND security AND implementation) OR KEY(hardware-based AND security AND protocols) OR KEY(tamper-proof) OR KEY(tamper-resistant AND designs) OR KEY(security AND services) OR KEY(access AND control) OR KEY(authentication) OR KEY(biometrics) OR KEY(visual AND passwords) OR KEY(graphical AND passwords) OR KEY(multi-factor AND authentication) OR KEY(authorization) OR KEY(digital AND rights AND management AND cybersecurity) OR KEY(privacy-preserving AND protocols) OR KEY(pseudonymity) OR KEY(anonymity) OR KEY(untraceability) OR KEY(software AND security) OR KEY(application AND security) OR KEY(domain-specific AND security AND architectures) OR KEY(domain-specific AND privacy AND architectures) OR KEY(social AND network AND security) OR KEY(social AND network AND privacy) OR KEY(software AND reverse AND engineering) OR KEY(software AND security AND engineering) OR KEY(web AND application AND security) OR KEY(systems AND security) OR KEY(browser AND security) OR KEY(denial-of-service AND attacks) OR KEY(distributed AND systems AND security) OR KEY(file AND system AND security) OR KEY(firewalls) OR KEY(information AND flow AND control) OR KEY(operating AND systems AND security) OR KEY(mobile AND platform AND security) OR KEY(trusted AND computing) OR KEY(virtualization AND security) OR KEY(vulnerability AND management AND cybersecurity) OR KEY(penetration AND testing) OR KEY(vulnerability AND scanners AND cybersecurity) OR TITLE-ABS-KEY(input AND manipulation AND attack) OR TITLE-ABS-KEY(data AND poisoning AND attack) OR TITLE-ABS-KEY(model AND inversion AND attack) OR TITLE-ABS-KEY(membership AND inference AND attack) OR TITLE-ABS-KEY(model AND stealing) OR TITLE-ABS-KEY(ai AND supply AND chain AND attacks) OR TITLE-ABS-KEY(transfer AND learning AND attack) OR TITLE-ABS-KEY(ai AND model AND skewing) OR TITLE-ABS-KEY(output AND integrity AND attack) OR TITLE-ABS-KEY(model AND poisoning) OR TITLE-ABS-KEY(broken AND access AND control) OR TITLE-ABS-KEY(cryptographic AND failures) OR TITLE-ABS-KEY(sql AND injection) OR TITLE-ABS-KEY(code AND injection) OR TITLE-ABS-KEY(cross-site AND scripting AND injection) OR TITLE-ABS-KEY(insecure AND design AND cybersecurity) OR TITLE-ABS-KEY(security AND misconfiguration) OR TITLE-ABS-KEY(vulnerable AND outdated AND components) OR TITLE-ABS-KEY(identification AND authentication AND failures) OR TITLE-ABS-KEY(data AND integrity AND failures) OR TITLE-ABS-KEY(software AND failures AND cubersecurity) OR TITLE-ABS-KEY(security AND logging AND monitoring AND failures) OR TITLE-ABS-KEY(server-side AND request AND forgery) OR TITLE-ABS-KEY(prompt AND injection) OR TITLE-ABS-KEY(model AND denial AND of AND service) OR TITLE-ABS-KEY(sensitive AND information AND disclosure)) AND (LIMIT-TO (AFFILCOUNTRY,Çhile")))

La consulta arrojó un resultado de 1550 documentos donde al menos un autor tenía afiliación chilena al momento de la publicación. De este corpus, Scopus entrega un listado de términos frecuentes, los cuales pueden apreciarse en el Cuadro 3.1.

Network Security	118		
Cryptography	84	Biometrics	76
Security	67	Security Systems	57
Security Of Data	54	Access Control	43
Anomaly Detection	40	Authentication	38
Data Privacy	33	Privacy	28
Cybersecurity	26	Artificial Intelligence	26
Monitoring	24	Medium Access Control	24
Mobile Security	23	Computer Crime	23
Quantum Cryptography	22	Security Requirements	21
Forensic Science	21		

Cuadro 3.1: Ejemplo de términos frecuentes encontrados en el corpus de documentos resultantes de la búsqueda

Scopus entrega además diversas opciones para filtrar los resultados, tales como: periodo de tiempo, nombre de autor, área de conocimiento, tipo de documento, fuente, estado de publicación, palabras claves, afiliación, patrocinador, país, tipo de fuente, lenguaje, y acceso abierto. El Cuadro 3.2 indica por ejemplo, la cantidad de documentos clasificados en diferentes disciplinas.

Computer Science	637	Engineering	488
Mathematics	300	Physics and Astronomy	102
Energy	86	Materials Science	66
Decision Sciences	57	Social Sciences	55
Chemistry	35	Biochemistry Genetics and Molecular Biology	28
Multidisciplinary	27	Medicine	26
Business Management and Accounting	26	Environmental Science	20
Agricultural and Biological Sciences	19	Chemical Engineering	13
Health Professions	12	Earth and Planetary Sciences	9
Psychology	6	Arts and Humanities	5
Economics Econometrics and Finance	4	Pharmacology Toxicology and Pharmaceutics	1
Neuroscience	1	Immunology and Microbiology	1

Cuadro 3.2: Disciplinas o áreas de conocimientos en las que se clasifican los documentos encontrados

De manera de refinar el corpus, aplicamos como primer filtro el área de disciplina, el cual fue restringido a: “Computer Science”, “Engineering”, “Mathematics” y“Multidisciplinary”. Esto redujo el conjunto de artículos de 1550 a 946. Como segunda etapa para refinar el corpus de documentos a analizar aplicamos el siguiente criterio de exclusión:

- artículos anteriores al año 2012 (dado que el estudio se restringe a los últimos 10 años),
- estudios sistemáticos de literatura, o estudios de opinión respecto del impacto en derechos de las personas o sociedad en general a menos que sea para entregar contexto.

Posterior a ello, pasamos a la etapa de “screening”, que excluye aquellos artículos que no son del alcance de este estudio en base a la revisión del título, resumen, y palabras claves tanto entregadas por el autor como las asignadas en base al texto por la base de datos científica Scopus.

Conjunto de Artículos sobre el que se basa este estudio de caracterización

Dado este proceso, la caracterización se basa en un corpus compuesto de 200 artículos, un conjunto de 484 autoras y autores distintos, donde aproximadamente un 50 % tienen a fines de noviembre 2023 afiliación chilena en la base de datos científica Scopus (la validez de este dato depende de la oportuna solicitud del autor de actualización de afiliación).

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.

En la Figura 3.1 podemos ver los artículos que han sido publicado estos últimos 10 años que califican en la temática de ciberseguridad, mostrando una considerable baja el año 2020. Es importante considerar que no se está considerando completo el año 2023 dado que la búsqueda fue realizada en Octubre 2023.

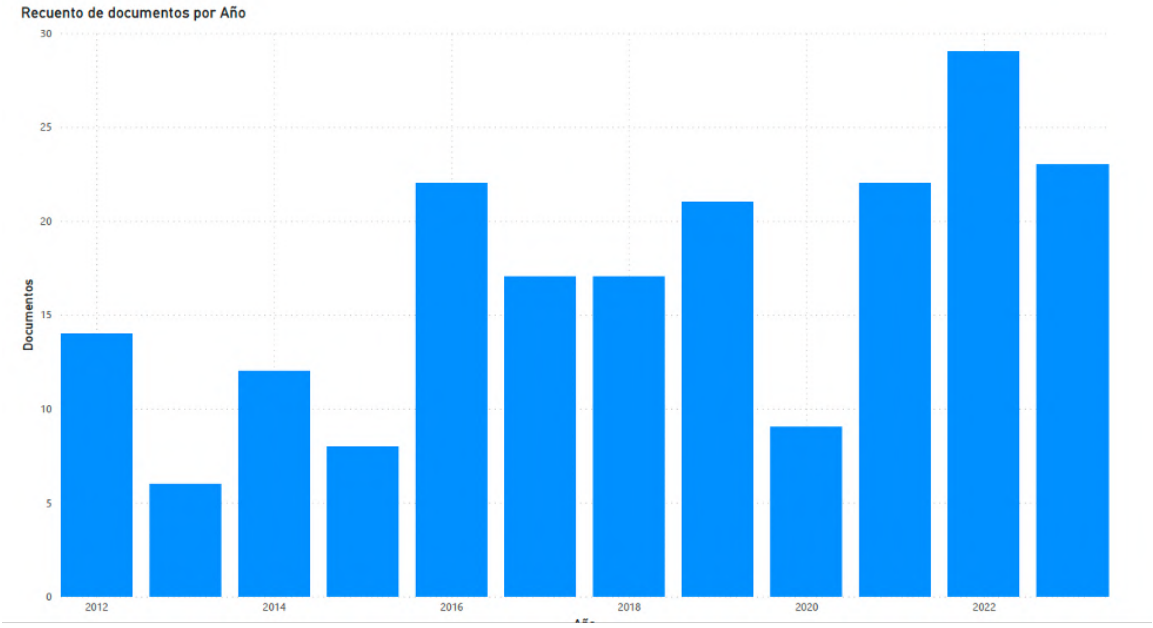


Figura 3.1: Documentos publicados por año.

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 %).

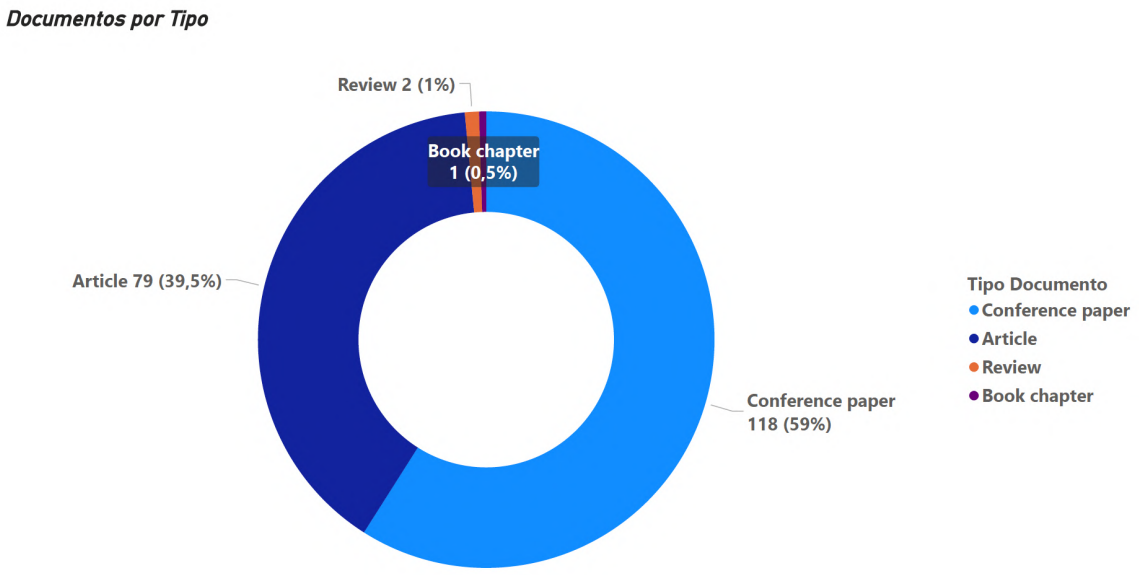


Figura 3.2: Documentos por Tipo.

Los artículos no necesariamente se clasifican en sólo una categoría de la ACM. Podrían tener más de una categoría y por cada una de estas, calificar en una o más subcategorías. Ahora bien, en la 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). **Como trabajo futuro, debería estudiarse esta hipótesis contra bases de datos de patentes.**

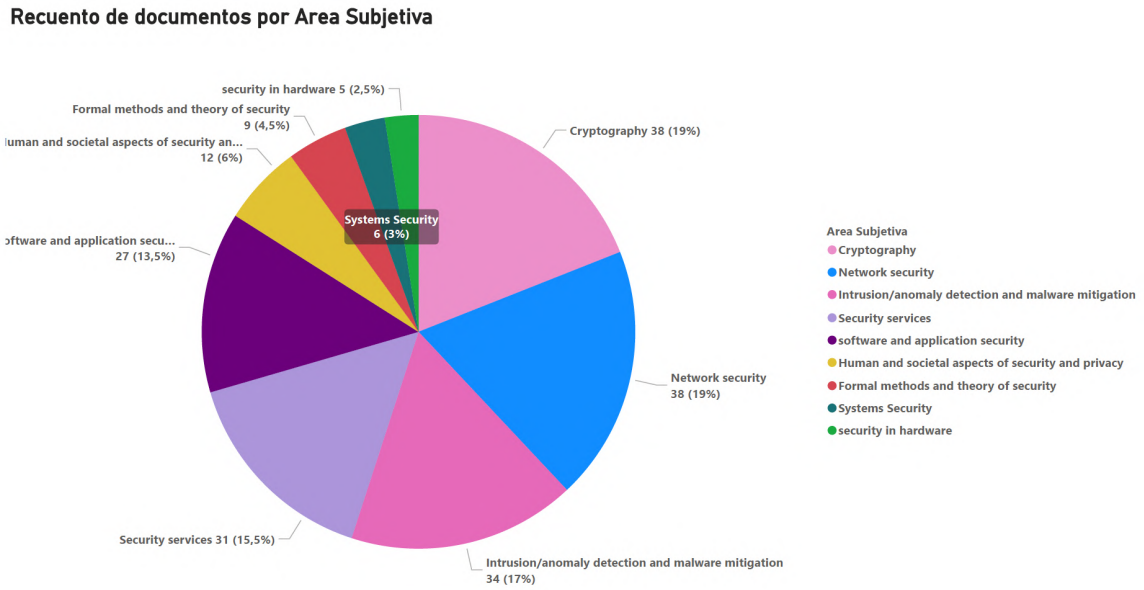


Figura 3.3: Documentos por Área.

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 (fin noviembre 2023).

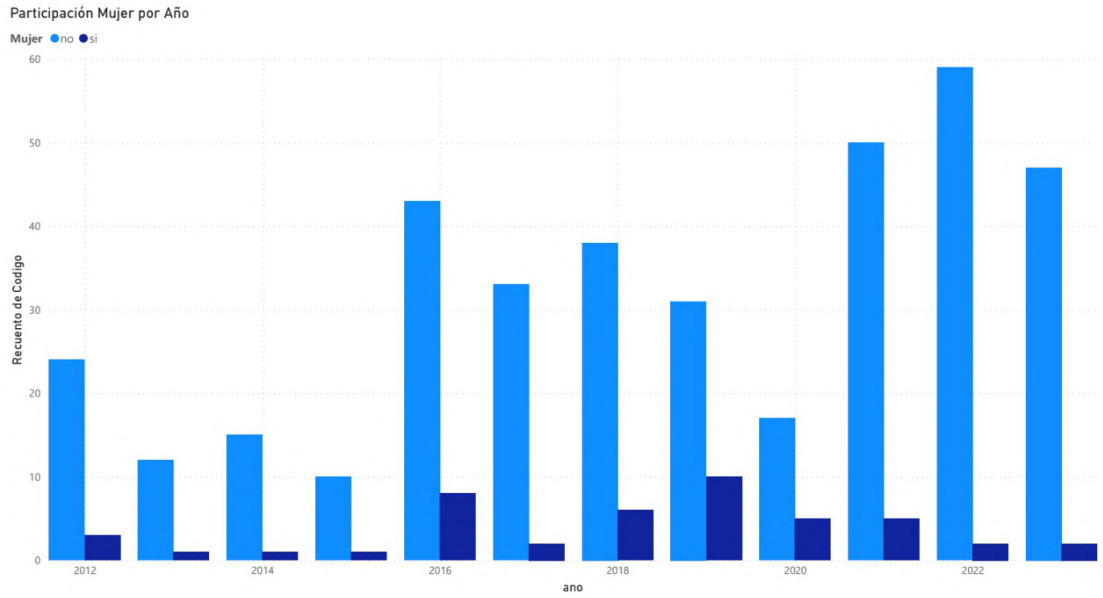


Figura 3.4: Participación Mujer por año.

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

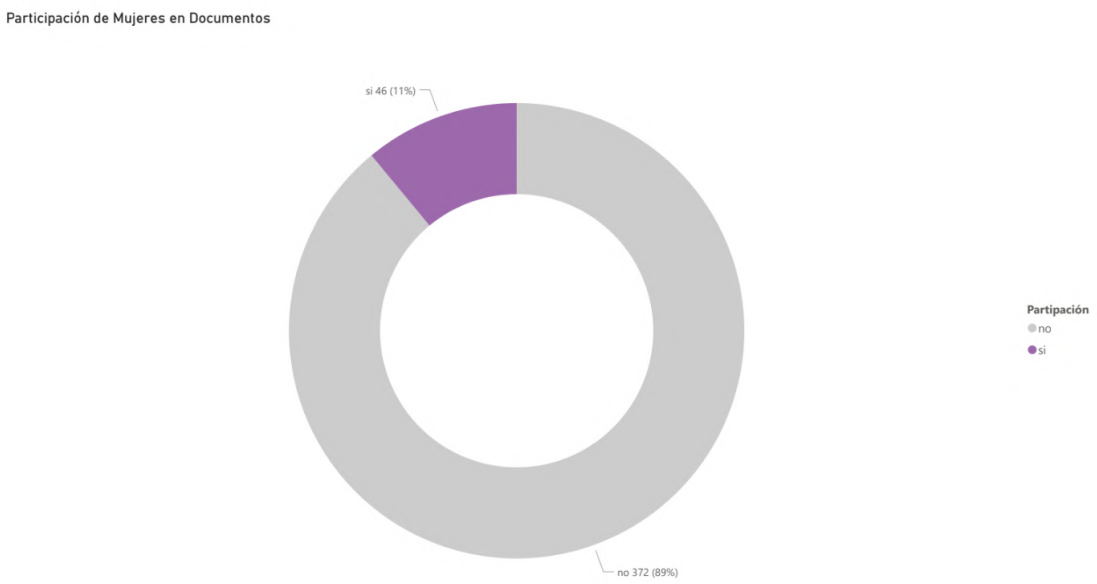


Figura 3.5: Participación de Mujeres en documentos.

3.2 Periodos

En esta sección hacemos un barrido del corpus de documentos resultante de haber aplicado los criterios de inclusión y exclusión ya señalados. 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.

Por cada uno de estos periodos hacemos una subsección generando dos tipos de grafos:

1. **Grafo de tópicos de investigación** donde utilizamos como método minería de texto para extraer términos importantes del corpus de documentos además de la herramienta [1] para construir y visualizar redes bibliométricas.

[1] `https://www.vosviewer.com/`

2. **Grafo de colaboración entre investigadoras/investigadores** donde utilizamos métodos para detectar comunidades [6] para lo cual nos apoyamos de la herramienta Gephi [2] de manera de poder utilizar algoritmos ya implementados para este fin.

Para la construcción de los **grafos de tópicos de investigación**, primero se separa el corpus en cinco subgrupos (uno por cada periodo a estudiar). Utilizando la herramienta VOSviewer[3] se realiza un análisis de co-ocurrencia de términos en el corpus donde se utilicen todas las "keywords", la que inicialmente se obtiene a partir de las palabras en el título, resumen, palabras claves asignadas por las o los autoras/autores así como palabras claves asignadas por scopus. Antes de construir los grafos, la herramienta solicita que se indique la mínima cantidad de co-ocurrencias de estas "keywords" en el corpus. En este estudio se designó como mínimo 2 pues permitía entender con mayor detalle los tópicos de investigación que al utilizar otros valores de umbral probados (como 3, 4, o 5).

Para generar un **grafo de colaboración entre investigadoras/investigadores**, primero representamos a cada autor/autora como un nodo de un grafo. Autores y autoras con nodos de mayor tamaño indican que en ese periodo tienen mayor colaboración con otras autoras y autores que otros u otras en igual periodo. Dos nodos o autoras/autores en un grafo estarán conectados si en el periodo específico han publicado un artículo de manera conjunta. Mientras más artículos posean de manera conjunta durante el periodo, el grosor de la arista será más gruesa. Respecto de los colores, el Cuadro siguiente muestra para cada área de la taxonomía ACM el color asignado tanto para colorear nodos como aristas dependiendo de la clasificación de las publicaciones realizadas durante el periodo en cuestión. Dado que es posible que un autor participe en publicaciones clasificadas en diferentes áreas de la ACM, su nodo se pintará con el color de aquella área que representa su mayor cantidad de artículos en el subperiodo. Mismo caso para asignar el color a la arista que representa la colaboración entre dos autoras/autores; la arista se pintará del color del área más frecuente.

Áreas	CódigoColor	Color
Cryptography	F472D0	rosa suave
Formal methods and theory of security	D64550	rojo oscuro
Human and societal aspects of security and privacy	D9B300	amarillo mostaza
Intrusion/anomaly detection and malware mitigation	B33685	magenta
Network Security	118DFF	azul claro
Security in hardware	1AAB40	verde oscuro
Security Services	B5A1FF	lila
Software and application security	6B007B	morado
Systems Security	197278	verde azulado

Cuadro 3.4: Paleta de colores para pintar nodos y aristas del **Grafo de colaboración entre investigadoras o investigadores**

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

[2] `https://gephi.org/`
[3] `https://www.vosviewer.com/`

de estos tópicos en el grafo de colaboración entre investigadoras o investigadores. Importante mencionar que para referenciar el trabajo en este estudio se menciona al autor con afiliación chilena, independiente de que este no sea autor correspondiente o primer autor, pues permite de manera gradual introducir al lector las investigadoras y los investigadores con afiliación chilena que han aportado a la ciberseguridad en Chile los últimos 10 años.

3.2.1 2012–2015

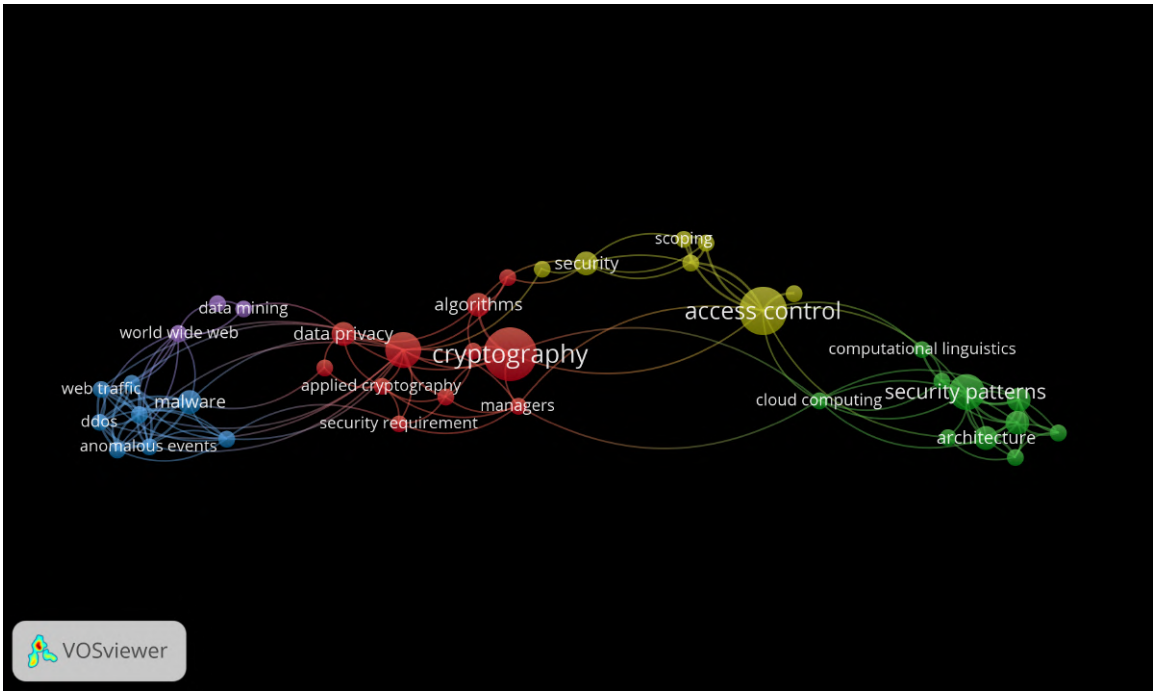


Figura 3.6: Principales tópicos en los que investigadoras o investigadores realizan investigación en periodo 2012–2015.

Iniciamos este recorrido del estado del arte de investigación en ciberseguridad en Chile con el grafo de tópicos de investigación que se muestra en la Figura 3.6 para el periodo 2012–2015. 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. En este contexto, la aplicación de patrones seguros y buenas prácticas juega un papel fundamental. Los patrones seguros son soluciones probadas y estandarizadas para problemas comunes de seguridad en el diseño de software. Estos patrones ofrecen un enfoque consistente y confiable para abordar desafíos específicos, como la gestión de sesiones seguras, la protección contra ataques de inyección, y la implementación de controles de acceso robustos. En esta línea, Fernández E. B. y Monge R. realizaron una contribución importante al proponer una Arquitectura de Referencia de Seguridad (SRA) para sistemas en la nube. Su trabajo proporciona un marco conceptual y práctico para entender y construir sistemas seguros

en entornos de nube, utilizando patrones y modelos UML. Realizaron un análisis de amenazas y patrones de mal uso en sistemas Inter-Cloud federados, contribuyendo a un catálogo de patrones de mal uso y mejorando la comprensión de amenazas específicas en el contexto de sistemas Inter-Cloud. Además, se enfocaron en la autorización avanzada, proponiendo patrones para la autorización dependiente del contenido y el control de acceso mejorado por contexto. Estos patrones ofrecen una mayor granularidad en la gestión de autorización, abordando aspectos específicos de la seguridad. Astudillo H. y colaboradores abordaron el tema de tácticas de seguridad en el diseño de arquitectura de software, proponiendo una manera sistemática de aplicar tácticas para mejorar la seguridad en la arquitectura, contribuyendo a la creación de sistemas más robustos. También revisitaron las tácticas arquitectónicas para la seguridad en sistemas informáticos, refinando y clasificando las tácticas existentes para mejorar la calidad y efectividad de estas tácticas en ciberseguridad. Además, realizaron un estudio comparativo de patrones y tácticas de seguridad para fortalecer sistemas, involucrando a desarrolladores y estudiantes para evaluar la efectividad y velocidad de ambos enfoques. Sepúlveda C. y colaboradores abordaron la seguridad en el contexto específico de composición de servicios RESTful sensibles a la calidad del servicio (QoS), centrándose en la seguridad en un entorno descentralizado y basado en hipermedios.

Camacho P. y colaboradores se centran en el diseño y la implementación de esquemas de acumuladores, específicamente los universales y fuertemente universales, abordando la confianza y seguridad de estos esquemas en entornos donde la confianza en un administrador de acumuladores es limitada. Abarzúa R. y Thériault N. contribuyen al área de criptografía con su enfoque en mejorar la seguridad de bloques atómicos para multiplicación escalar en curvas elípticas sobre campos primos. Xavier, G. y sus colegas presentan un experimento exitoso de implementación del protocolo de criptografía cuántica GV95, destacando la estabilización activa a larga distancia. Vielhaber M. reintroduce el esquema Reduce-By-Feedback en el contexto de implementaciones de RSA, abordando la vulnerabilidad al ataque de Análisis Diferencial de Potencia. El trabajo de Vielhaber M. y Mónica Del Pilar Canales se enfoca en la complejidad lineal en multisecuencias, proporcionando una fórmula cerrada y avanzando en la comprensión de la complejidad lineal. Vásquez D. y colaboradores desarrollan técnicas criptográficas para garantizar un intercambio seguro de mensajes. Grote W. y colaboradores abordan la seguridad en Redes de Sensores Inalámbricos (WSN) proponiendo una nueva técnica de cifrado para garantizar la confidencialidad de los datos. Caragata D. y colaborador analizan un algoritmo de cifrado de imágenes, destacando debilidades que comprometen su seguridad. Xavier, G. se enfoca en tecnologías para avanzar en las comunicaciones cuánticas seguras a larga distancia sobre fibras ópticas. Huerta-Canepa G. aborda preocupaciones de seguridad en la comunicación de dispositivo a dispositivo (D2D), proponiendo un esquema de cifrado. Cáces Alvarez L. y colaboradores se centran en la implementación de un protocolo de criptografía cuántica. En este mismo grupo rojo, vemos un nodo “data privacy” que mirado desde la taxonomía de la ACM se acerca más al área de aspectos humanos y de sociedad respecto de la seguridad y privacidad. En esa línea, Bustos-Jiménez J. examina el impacto de la aceptación automática e inconsciente de consentimientos informados en aplicaciones móviles sobre la privacidad de los usuarios donde se evidencia la falta de comprensión de los usuarios, con menos de 1/9 leyendo los documentos de consentimiento. Hou, R. y colaboradores del centro de Yahoo en Chile, se enfocaron en salvaguardar la privacidad al extraer patrones frecuentes de datos que combinan la privacidad diferencial y el modelo k-anonimato para preservar información sensible mientras se asegura la utilidad de los datos. La privacidad diferencial, es una técnica que agrega ruido aleatorio a los datos para preservar la privacidad de los individuos sin afectar significativamente la utilidad de los datos para fines estadísticos o de análisis. El modelo de k-anonimato es una forma de proteger la privacidad

de los datos personales al anonimizarlos de tal manera que cada individuo sea indistinguible de al menos otros k-1 individuos en el mismo conjunto de datos mediante la supresión o la generalización de los atributos que pueden identificar a las personas, como el nombre, la edad, el género, entre otros.

El grupo amarillo en la Figura 3.6 destaca investigaciones respecto de servicios de seguridad y específicamente en este periodo de control de acceso como las de Bravo L. y colaboradores. Bravo L. y Segovia R. simplifican políticas para bases de datos XML, mejorando eficiencia y alcance. Toledo R. y Tanter É. exploran la modularización completa del control de acceso en un lenguaje de programación, validando su propuesta. Wu J. y su equipo proponen un método jerárquico para la red eléctrica inteligente en entornos de nube.

Los ataques suelen venir de grupos especializados. 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**. En esta línea Ríos S.A. y Muñoz R. abordaron la detección de comunidades en la Dark Web basada en modelos de temas, proporcionando herramientas para analizar y comprender grupos en línea, especialmente en el contexto de amenazas potenciales para la seguridad. En ataques específicos, en este periodo se destacan investigaciones sobre la frecuencia y detección de ataques de denegación de servicio distribuidos (DDoS), como la propuesta de un índice de riesgo por Des Valle P. y colaboradores. Pinacho P. y colegas proponen un enfoque ecológico para la detección de anomalías en sistemas de detección de intrusiones además de un sistema de bioindicadores para la detección de intrusiones en redes, mientras que Vasquez y Simmonds abordan la seguridad de aplicaciones móviles con un marco de monitoreo en tiempo real. Ordóñez y colaboradores desarrollan estrategias de monitoreo para la detección eficiente de amenazas nucleares, y Caragata y colaborador proponen mejoras de seguridad para el sistema UMTS. Wu J. y colaboradores introdujeron un modelo de comunicación seguro basado en la Transformada Discreta de Fourier Fraccional (DFRFT) donde incluyeron un parámetro de señal de distorsión para confundir a posibles atacantes, garantizando ventajas para los socios legítimos. Además, se desarrollan códigos de seguridad adicionales para construir un canal legítimo, libre de errores y prevenir la obtención de información útil por parte de espías.

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,a 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.

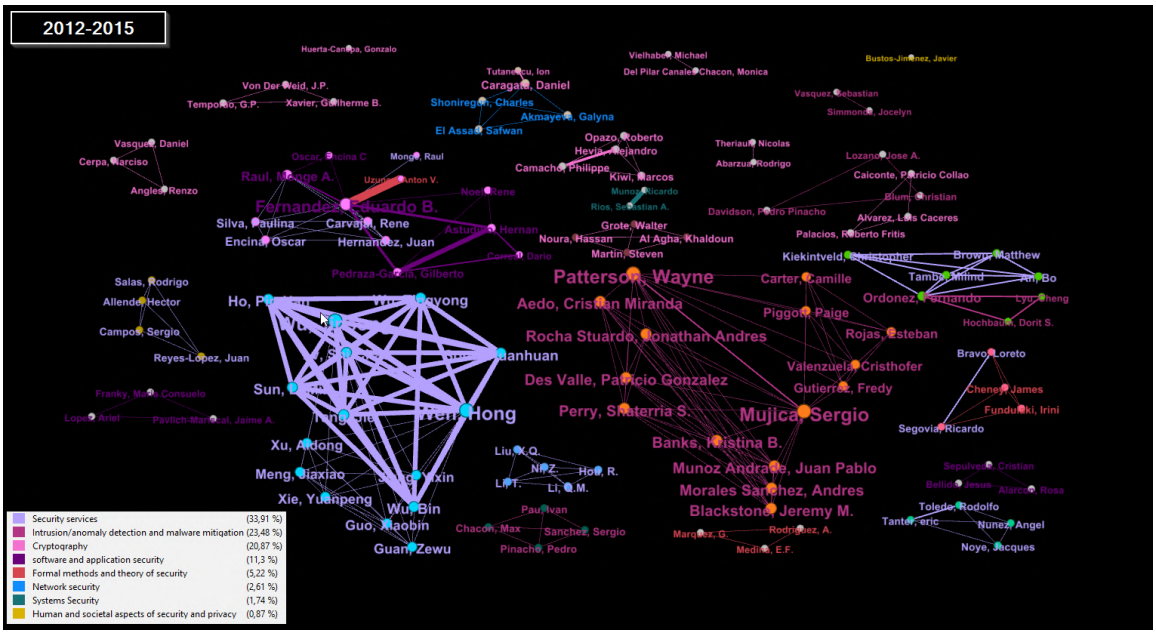


Figura 3.7: Autoras/Autores responsables de las investigaciones consideradas en este estudio publicadas durante periodo 2012–2015.

3.2.2 2016–2017

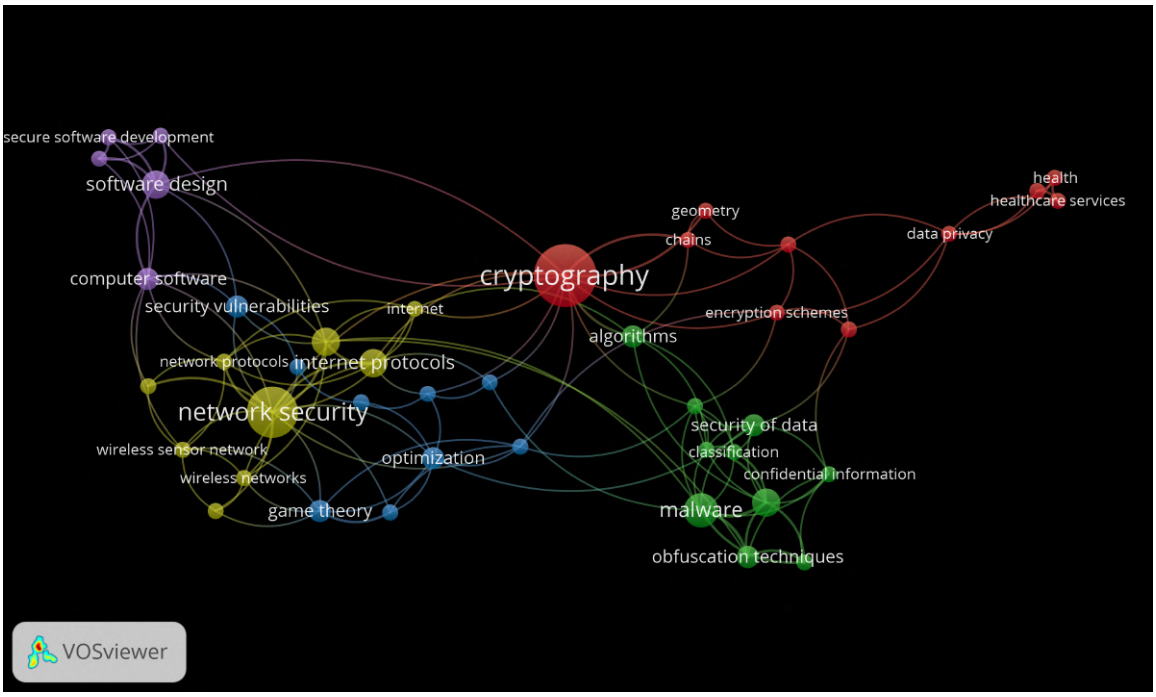


Figura 3.8: Principales tópicos en los que investigadoras o investigadores realizan investigación en periodo 2016–2017.

La comunidad **Seguridad de Software y aplicaciones** que aparecía en verde en la Figura 3.6 aparece como la comunidad en lila en la Figura 3.8. Monge R. y colaboradores continúan su trabajo en SRAs para sistemas en la nube. Márquez G. y colaboradores exploran la relevancia de los artefactos tradicionales de ingeniería de software en la toma de decisiones de seguridad durante el desarrollo de software. Su enfoque experimental agrega evidencia empírica al uso de artefactos como Casos de Uso y Diagramas de Clases, arrojando luz sobre su utilidad en el diseño de arquitecturas de software seguras. Silva P. y colaboradores realizan un mapeo sistemático de tecnologías para identificar y mitigar amenazas de seguridad en el desarrollo de software. Su trabajo proporciona una visión general de las técnicas existentes, destacando su integración en el Ciclo de Vida del Desarrollo de Software y su adopción en la industria. Por último, Osses F. y colaboradores presentan Security Tactic Planning Poker (SToPPER), una técnica colaborativa para seleccionar tácticas de seguridad en el diseño de software. Este enfoque práctico involucra a los interesados en un entorno grupal, fomentando la interacción y asegurando una base común para el uso de tácticas de seguridad. Noël R. y colaboradores contribuyeron a la comprensión de cómo las decisiones de diseño afectan la seguridad en conjunto con otros atributos. La comunidad de **servicios de seguridad**, en particular biometría para control de acceso que aparecía en el periodo anterior presenta bajo crecimiento, donde podemos destacar a Rothhammer F. y colaboradores quienes resaltan las ventajas de utilizar la estructura del oído como marcadores biométricos, ya que estos pueden capturarse fácilmente a distancia con métodos no intrusivos, experimentan cambios mínimos con el tiempo y no se ven afectados por expresiones faciales. Los autoras/autores proponen un método innovador basado en la Morfometría Geométrica y Aprendizaje Profundo (Deep Learning) para la detección automática y extracción de características del oído en forma de landmarks. Por otro lado,Barceló P y colaboradores presenta una lógica capaz de expresar de manera natural restricciones esenciales para analizar mutaciones XSS en aplicaciones web. Enfocándose en la seguridad del navegador, aborda con eficacia las complejidades de desinfección de funciones y transducciones implícitas del navegador, como mutaciones de innerHTML. Este trabajo ofrece un enfoque valioso para analizar y mitigar vulnerabilidades específicas de los navegadores web. Esta contribución se clasifica en la comunidad de **seguridad de sistemas**, que es un área acorde al corpus de documentos bajo estudio, de baja actividad.

Nuevamente importante en este periodo, es la comunidad de **criptografía** que aparece en el centro de la Figura 3.8. González A. y colaboradores propusieron nuevas técnicas para argumentos no interactivos de corrección de mezcla y argumentos de rango, destacando la eficiencia en grupos bilineales asimétricos. Caragata D. y colaboradores se centraron en el criptoanálisis de un esquema de marca de agua frágil, resaltando vulnerabilidades y aspectos relacionados con la seguridad y la protección de datos. Blasco S. y colaboradores exploraron un enfoque de tres capas para preservar la privacidad de los ciudadanos inteligentes en proyectos de crowdsensing, considerando protocolos de privacidad y aspectos éticos y sociales. Por otro lado, Riquelme E. y colaboradores contribuyeron con investigaciones matemáticas. Gonzalez A. C. se enfocó en la eficiencia computacional de emparejamientos criptográficos. Koscina M. y Caragata D. llevaron a cabo un análisis comparativo de algoritmos criptográficos tradicionales y basados en caos con operaciones de ADN, destacando la seguridad y rendimiento en el cifrado de imágenes. Miranda M. y Mundarain D. exploraron la distribución cuántica de claves mediante estados cuánticos mejorados. Munoz, C. y colaboradores abordaron desafíos de seguridad en la gestión de claves en el DNS, proponiendo un sistema de firma distribuido basado en criptografía de umbral. Ravanales W. y Herman K. presentaron un nuevo esquema de cifrado McEliece que mejoró la confiabilidad y robustez contra ataques de espionaje. Finalmente, Araya A. y colaboradores propusieron un criptosistema que combinó el protocolo de

Diffie-Hellman con curvas hiperelípticas para la comunicación visible por luz, destacando mejoras en la seguridad mediante técnicas de sincronización neuronal. 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. Elmisery A. y colaboradores abordan la integración de servicios de salud basados en la nube y el Internet de las Cosas en Salud (IoHT), asegurando al mismo tiempo el cumplimiento de los principios de privacidad de la OCDE. Su middleware basado en la "niebla" (fog computing) garantiza la privacidad de la información de salud de los usuarios finales mediante un proceso de ocultamiento, presentando una solución vital en medio de crecientes preocupaciones sobre la privacidad en los datos de salud. Además, en un artículo separado propusieron un servicio de recomendación en la nube para consejos de atención médica que mejora la privacidad al intercambiar información entre pacientes sin revelar preferencias reales. Cruz R. y colaboradores presentan un enfoque de abstracción de tipo para la no interferencia relajada en seguridad de flujo de información. Aborda la seguridad de la información estática al prevenir que la información confidencial se filtre a canales públicos. Propone un enfoque basado en tipos para políticas de desclasificación más expresivas y simples, utilizando abstracción de tipo para abordar desafíos anteriores y facilitar la integración de políticas de desclasificación en lenguajes de seguridad prácticos.

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. Wu J. y colaboradores se centran en la optimización de la selección de middlebox y enrutamiento para mejorar el rendimiento en redes definidas por software (SDN). Este estudio presenta un algoritmo de aproximación de Markov para abordar el problema NP-duro, logrando soluciones cercanas a lo óptimo y destacando la importancia de una planificación conjunta para evitar congestiones y mitigar ataques en puntos críticos de la red. Destacando la importancia de la seguridad en entornos críticos como las redes eléctricas industriales, el estudio de Lazo, C. y colaboradores proporciona "insights" valiosos para la protección de sistemas de control y monitoreo. En el ámbito de la seguridad móvil, Barragan C. y colaboradores se enfocan en el crecimiento exponencial de amenazas en dispositivos móviles y desarrolla una fórmula matemática para determinar la probabilidad de infección de un dispositivo móvil según su sistema operativo y versión. Font G. y colaboradores contribuyen significativamente al campo de la seguridad de redes centrándose en la privacidad de la ubicación en sistemas de monitoreo de redes móviles, proponiendo un modelo que utiliza cifrado homomórfico para preservar la privacidad de la ubicación. Clasificándose en la subárea de "Privacy-preserving protocols" del área security services, el estudio destaca la importancia de desarrollar protocolos que protejan la privacidad en entornos de monitoreo de redes móviles.

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. Bustos-Jimenez y colaboradores presentan un enfoque innovador utilizando técnicas de minería de procesos para analizar el tráfico del Sistema de Nombres de Dominio (DNS), revelando comportamientos inesperados y ataques de botnets de spam. Destacando la importancia de comprender el comportamiento de los protocolos web para identificar amenazas, Bustos-Jimenez J.y colaboradores contribuye al avance de la seguridad cibernética al explorar nuevas metodologías de análisis de tráfico DNS. En el ámbito de la seguridad en redes satelitales,

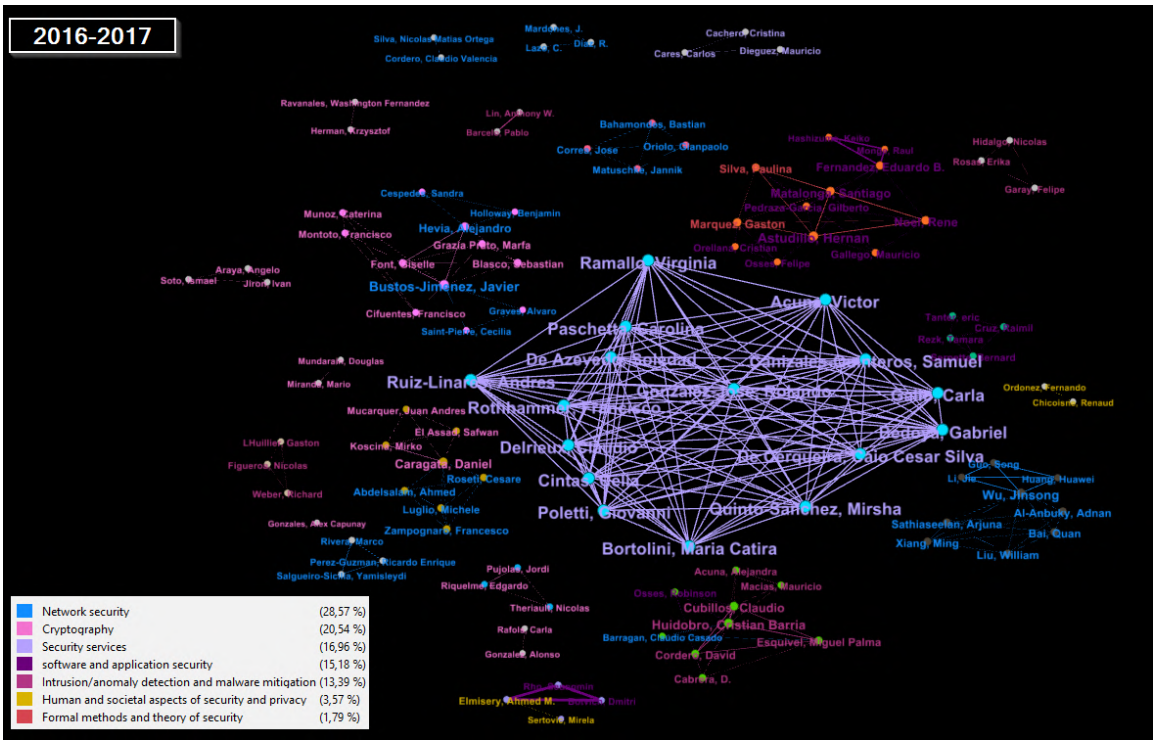


Figura 3.9: Autoras/Autores responsables de las investigaciones consideradas en este estudio publicadas durante periodo 2016–2017.

Abdelsalam A. y colaboradores propone una arquitectura de seguridad robusta para proteger las transmisiones de video digital vía satélite, inspirada en el mecanismo de seguridad de la red de área local inalámbrica IEEE 802.11i. Destacando la eficiencia de un mecanismo de autenticación y gestión de claves de tres rondas, Abdelsalam A. y colaboradores resalta la importancia de asegurar las comunicaciones en redes satelitales. Wu J. y colaboradores contribuye al campo de la seguridad en comunicaciones inalámbricas proponiendo el concepto de “Network-Trustworthiness-as-a-Service” (NTaaS), un marco de evaluación de confianza en redes D2D. En el ámbito de la seguridad de redes físicas, Bahamondes B. y colaboradores aborda un juego de seguridad de red aplicado a la interdicción de evasión de tarifas o contrabando investigando la complejidad de calcular estrategias óptimas para el intruso y el defensor, destacando la adaptabilidad en la planificación de rutas y la colocación de puntos de control.Bahamondes B. y colaboradores proporciona una contribución significativa al estudio de estrategias de seguridad adaptativas en el contexto de la interdicción de redes. Barría C. y colaboradores contribuyen al ámbito de la ciberseguridad proponiendo un procedimiento de ofuscación para el malware, enfatizando técnicas para evadir sistemas antivirus. Esto subraya el juego perpetuo entre las medidas de ciberseguridad y las estrategias en constante evolución del malware.

Otra comunidad activa relacionada es la de Aspectos humanos y de sociedad respecto de la privacidad y seguridad. Aunque no se visualiza explícitamente en la Figura 3.8 vemos contribuciones de investigadoras o investigadores con afiliación chilena. Ordóñez y colaborador presentan un juego de seguridad Stackelberg en el que un defensor protege objetivos contra un adversario que utiliza una respuesta cuántica para decidir qué objetivo atacar. La contribución principal radica en introducir

aversión al riesgo en el comportamiento del defensor mediante una medida de riesgo entrópico. Amplían trabajos anteriores al considerar un modelo con un defensor adverso al riesgo y mejoran los algoritmos reduciendo el número de variables enteras. Los resultados computacionales muestran ventajas cualitativas al utilizar una medida de riesgo en lugar del valor esperado. Dieguez M. y colaboradores explora la gestión de los controles de seguridad de la información y busca mejorar las recomendaciones de los asesores de seguridad mediante la incorporación de métodos cuantitativos, específicamente técnicas de Investigación de Operaciones.

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.

3.2.3 2018–2019

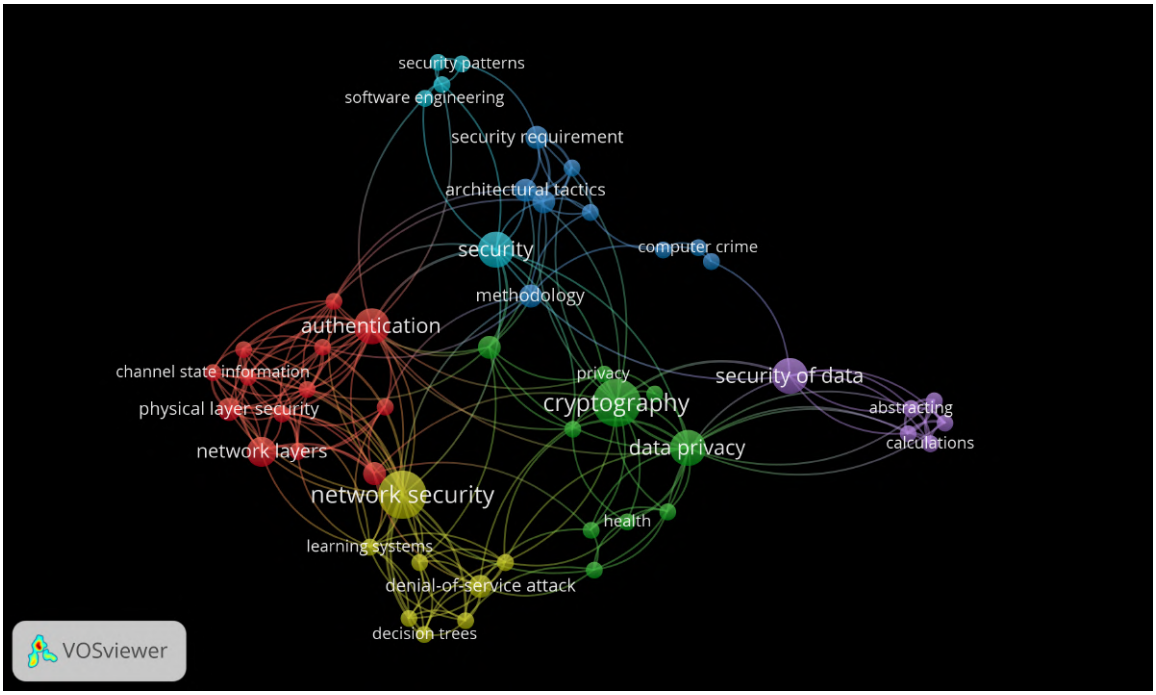


Figura 3.10: Principales tópicos en los que investigadoras e investigadores realizan investigación en periodo 2018–2019.

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**. Rodríguez A. y colaboradores se adentran en la integración de conceptos de seguridad en modelos de procesos de negocio. Proponen el uso de extensiones de BPMN y patrones de seguridad para capturar tempranamente aspectos de seguridad en el ciclo de desarrollo de software, contribuyendo así a una representación más robusta de los requisitos de seguridad en los modelos UML de clases. Barragán

C. y colaboradores exploran la evaluación de la usabilidad en software de seguridad informática. Reconociendo la relación inversa entre usabilidad y seguridad, proponen evaluar cómo la usabilidad impacta la efectividad de las medidas de seguridad implementadas, contribuyendo así al diseño de sistemas más accesibles y seguros. Wun J. y colaboradores introducen un marco de autenticación en la capa física basado en aprendizaje profundo. Su propuesta utiliza algoritmos de redes neuronales para mejorar la seguridad de las redes de sensores inalámbricos industriales, ofreciendo un enfoque ligero y eficiente. Nieves Arreaza G.J. aborda la metodología para desarrollar aplicaciones seguras en la nube. Toro M. y colaboradores presentan GSLRef, lenguaje de tipado estático y fuerte, que usa anotaciones de tipos para especificar las propiedades de seguridad de los datos. GSLRef verifica la seguridad de los programas tanto en tiempo de compilación como en tiempo de ejecución, usando técnicas de análisis estático y dinámico. Osses F. y colaboradores proponen el juego de cartas "Security Tactics Selection Poker (TaSPeR)". Este enfoque gamificado busca facilitar la selección de tácticas de seguridad arquitectónica, involucrando a los miembros del equipo de desarrollo y fomentando la participación de los interesados. Vale A.P. y Fernandez E. B. introducen una ontología que agrega semántica a los patrones de seguridad. Su propuesta busca mejorar la precisión en la utilización de patrones de seguridad, permitiendo el desarrollo de herramientas específicas y contribuyendo a la construcción de catálogos más robustos.

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. Durante este periodo, por ejemplo, Velásquez I. y colaboradores presentan un marco de recomendación de esquemas de autenticación, abordando la diversidad de técnicas disponibles. Su propuesta se basa en la experiencia industrial y se enriquece con la revisión de la literatura académica liberando un marco que recomienda esquemas de autenticación dependiendo de criterios de usabilidad, seguridad y costos.

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**. Ortega N. y Valencia C. exploran la mejora de la seguridad en las comunicaciones inalámbricas usando estrategias de Teoría de Juegos para optimizar la Capacidad de Secreto en redes inalámbricas. Aros M. y Torres R. presentan un enfoque concreto para abordar ataques a servidores XMPP proponiendo la implementación de formas de firma sobre un mecanismo de registro en banda para mitigar la probabilidad de éxito de los ataques. Su enfoque en la implementación práctica sobre OpenFire demuestra resultados positivos al reducir la cantidad de ataques exitosos a cero, destacando la eficacia de su propuesta en la protección contra ataques en entornos de mensajería instantánea. Estos estudios se clasificarían en la subárea "Security protocols" de **seguridad de redes**, ya que aborda la mejora de la seguridad en las comunicaciones inalámbricas a nivel de protocolos de seguridad. Barría Huidobro C. y colaboradores abordan la evaluación de seguridad en redes inalámbricas. Por otro lado, Pavesi J. y colaboradores realizan pruebas para validar una vulnerabilidad en controladores PLC, destacando la importancia de la seguridad en sistemas industriales y la identificación de vulnerabilidades. Montejo-Sanchez S. y colaboradores exploran el uso de señalización gaussiana impropia para mejorar la seguridad en redes de radio cognitivas mejorando el rendimiento de secreto en este tipo de redes. Galeazzi L. y colaboradores investigan las variables que afectan las operaciones normales contribuyendo así a la comprensión y mejora de la seguridad física y de la información en entornos inalámbricos. Montejo-Sanchez S. y colaboradores evalúan el rendimiento de 6LoWPAN bajo ataques de interferencia activa en redes de baja potencia y pérdida, específicamente en escenarios 6LoWPAN con modos TSCH/Orchestra. La variación en términos de Packet Data Rate (PDR) y eficiencia energética destaca la importancia de considerar y mitigar los efectos de ataques de interferencia activa en entornos de redes inalámbricas

de baja potencia y pérdida. Ya más en el área de **detección y mitigación de intrusos y malware** vemos diversos trabajos en este periodo. Wu y colaboradores proponen un método de autenticación a nivel físico para redes 5G utilizando algoritmos de aprendizaje automático utilizando información del canal de radio para detectar ataques de suplantación. Su enfoque en utilizar modelos entrenados de aprendizaje automático destaca la importancia de la autenticación a nivel físico para fortalecer la seguridad en las redes 5G. Wu J. y colaboradores proponen un sistema de monitoreo en línea del tráfico de Internet basado en aprendizaje automático con Spark Streaming para detectar DDoS en tiempo real. El método utiliza selección de características y compara la eficacia de algoritmos como Naive Bayes, Logistic Regression y Decision Tree. Muñoz D. y colaboradores presentan un método de ofuscación utilizando técnicas como AVFUCKER y Binary Division para optimizar recursos y reducir el tiempo de análisis del malware, centrado en evadir la detección de antivirus. Maldonado J. y colaboradores proponen una técnica de detección de intrusiones utilizando un algoritmo evolutivo y C4.5 para seleccionar características clave, mostrando resultados alentadores en conjuntos de datos de intrusión. Muñoz D. y colaboradores desarrollan una metodología para analizar malware scripting, proporcionando una estructura para comprender y mitigar amenazas en entornos controlados. Wu y colaboradores contribuyen significativamente al campo de la seguridad en redes definidas por software (SDN) abordando los desafíos de seguridad en entornos SDN, específicamente en relación con los ataques de Denegación de Servicio Distribuido (DDoS). Identifica un nuevo tipo de ataque DDoS dirigido específicamente a entornos SDN y propone un esquema novedoso de detección en tiempo real utilizando el análisis de Componentes Principales (PCA) para analizar datos de paquetes de tráfico de red. Este enfoque innovador destaca la importancia de adoptar estrategias de detección proactivas en entornos SDN para mitigar los riesgos asociados con los ataques DDoS.

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. González A. y Hevia A. se centran en la composabilidad universal, explorando la viabilidad y seguridad de protocolos en este marco. En el contexto de la Universal Composability Generalizada (GUC), examinan un ataque a un protocolo GUC Zero Knowledge (GUCZK), concluyendo que el protocolo mantiene su seguridad a pesar del ataque. Abarzúa R. y colaboradores abordaron la seguridad de las tarjetas inteligentes, proponiendo sistemas criptográficos más seguros y eficientes. Villanueva A. A. y colaboradores presentaron un novedoso criptosistema que combina el protocolo Diffie-Hellman con curvas hiperelípticas y sincronización neuronal, dirigido a superar vulnerabilidades específicas en la sincronización neuronal. Por otro lado, Mosso E. y colaboradores exploraron técnicas criptográficas de clave pública con un enfoque asimétrico para la encriptación de múltiples imágenes, destacando la resistencia a ataques de criptoanálisis. López Fenner J. y colaboradores contribuyeron al campo de la ciberseguridad con un protocolo de computación segura para la multiplicación de matrices, basado en el algoritmo Strassen-Winograd. Díaz Arancibia J. y colaboradores se centraron en la seguridad en entornos del Internet de las cosas (IoT), proponiendo un protocolo basado en el intercambio de claves de Diffie-Hellman. Finalmente, Monsalve G. y colaboradores presentaron protocolos para generar claves Excalibur bajo jerarquías DAG, utilizando el esquema de cifrado Multikey FHE-NTRU y enfocándose en evitar la transferencia y filtración de claves secretas. Respecto de los tópicos de investigación asociados a privacidad podemos destacar el trabajo de Molina-Martínez C. y colaboradores, quienes proponen un protocolo de enlace a distancia para aplicaciones de ubicación que aborda las preocupaciones de privacidad al ocultar la ubicación del usuario. Kaschel H. y Ahumada C. se centran en la ciberseguridad de dispositivos médicos, destacando riesgos y proponiendo mecanismos de protección. Orellana C. y colaboradores exploran

tácticas arquitectónicas para mitigar amenazas de seguridad en Sistemas Ciber-Físicos. Li Z. y Pino E. J. proponen un enfoque distribuido y desechable para preservar la privacidad en análisis de datos de salud. Elmisery A. M. y colaboradores presentan un marco de atención médica en la nube que prioriza la privacidad, utilizando nodos en la "niebla" (en vez de la "nube") para mantener la confidencialidad de los datos de 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, mediantes cambios en las metodologías, generación de nuevas herramientas para usar en los desarrollos, entre otros.

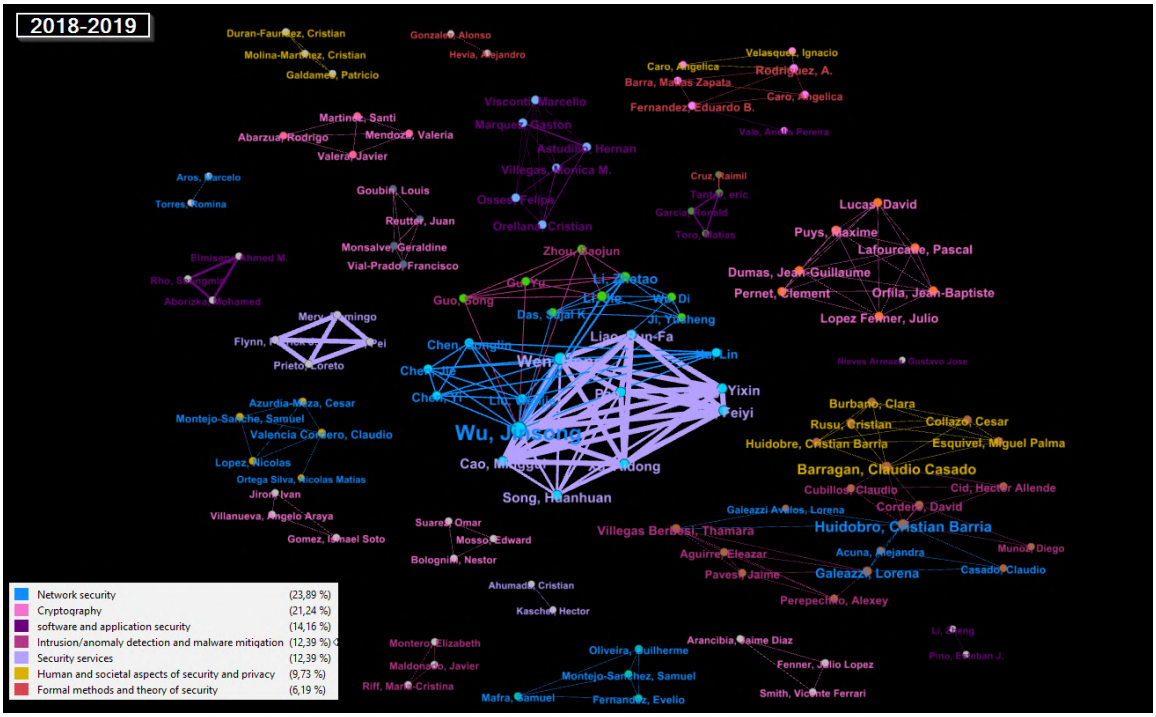


Figura 3.11: Autoras/Autores responsables de las investigaciones consideradas en este estudio publicadas durante periodo 2018–2019.

3.2.4 2020–2021

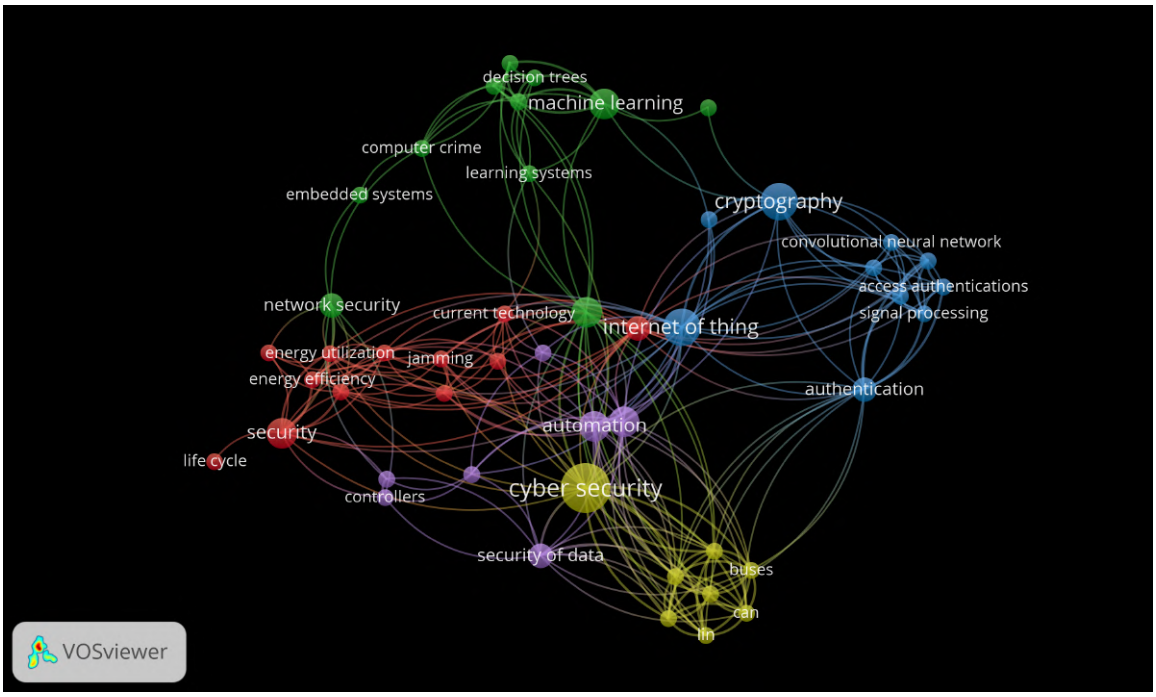


Figura 3.12: Principales tópicos en los que investigadoras e investigadores realizan investigación en periodo 2020–2021.

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. Soto R. y colaboradores propusieron un esquema innovador para el diseño de cajas de sustitución (S-box) con alta no linealidad, destacando la importancia de este componente en la resistencia criptoanalítica de sistemas de cifrado modernos. Azocar J. y colaboradores contribuyeron al campo de la criptografía cuántica mediante la implementación del protocolo BB84 con el objetivo de lograr un intercambio de claves seguro, utilizando una fuente óptica de frecuencia combinada. Villegas F. y Cordero C. realizaron una evaluación experimental de ataques de canal lateral en un dispositivo que emplea criptografía de curva elíptica, utilizando modelos de aprendizaje automático para detectar posibles vulnerabilidades. Ruminot-Ahumada N. y colaboradores se centran en analizar y comparar contramedidas para el Análisis de Correlación Lateral (SCA) en dispositivos de baja potencia con cifrado AES de 128 bits, lo cual es relevante para la seguridad de la información en el contexto de Internet de las cosas (IoT).

Otros tópicos relevante de investigación sigue siendo la **seguridad en redes** que aparece en los tópicos en rojo como “jamming” dadas las investigaciones realizadas durante este periodo. López-Vilos, N. y colaboradores se centran en el análisis del rendimiento del protocolo IEEE 802.15.4 en entornos inteligentes bajo ataques de interferencia (“Jamming attacks”). Corral-Molina C. y Valencia-Cordero C. analizan la seguridad en la capa física de las comunicaciones y proponen métricas prácticas derivadas de la tasa de error de bits (BER) frente a la relación señal-ruido

(SNR) para evaluar la seguridad en la capa física. El enfoque práctico proporciona una perspectiva valiosa para ingenieros de comunicaciones, contribuyendo al desarrollo de medidas de seguridad efectivas contra espionaje y asegurando la legibilidad de mensajes en receptores legítimos. Paez F. y Kaschel H. presentan en el área de **seguridad en redes** también, un análisis de vulnerabilidades de seguridad en buses de comunicación vehiculares y proponen un esquema de autenticación de datos para el bus LIN proponiendo un esquema HMAC para mejorar la seguridad del bus LIN. Aborda preocupaciones cruciales sobre ciberseguridad en vehículos conectados y contribuye al diseño de capas robustas de seguridad para mitigar amenazas locales y remotas. En otro trabajo los Kaschel H. y Rojas R. continúan el enfoque en la seguridad de buses vehiculares proponiendo un esquema HMAC para autenticación de datos, integridad de datos y rechazo de ataques de repetición en el bus LIN. Las y los autoras/autores exploran diversos aspectos de las Redes de Sensores Inalámbricos Submarinos (UWSN) abordando desafíos clave en UWSN, incluyendo seguridad, eficiencia energética y protocolos. Respecto del área ACM **detección y mitigación de intrusos y malware**, a pesar de que la Figura 3.12 no muestra explícitamente estos tópicos, si 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". Por ejemplo, Torres R. y colaboradores utilizaron "clique percolation method" para generar un sistema de aprendizaje y en definitiva un observatorio de tweets respecto a ataques, su ubicación y su esparcimiento en el mundo para poner en aviso a los equipos de incidentes independiente que no hayan sido reportados aún en el país. Manzano C. y colaboradores comparan empíricamente diferentes algoritmos supervisados para identificar ransomware en tráfico de red. Rivera S. y colaboradores proponen específicamente una estrategia en microgrillas para detectar y mitigar ciberataques usando redes neuronales. Martínez V. y colaboradores proponen subconjunto de características relevantes para la detección adecuada de ataques. Madariaga D. y colaboradores presentan un método de detección de anomalías basado en predicción (AD-BoP) diseñado para detectar anomalías en el Sistema de Nombres de Dominio (DNS). La importancia de este trabajo radica en que dado que el DNS es un componente crítico de la infraestructura de Internet, las anomalías, ya sean causadas por ataques o fallos, pueden tener un impacto significativo en todos los recursos basados en Internet. Palma J. y colaboradores aborda específicamente el problema de control bajo ataques de denegación de servicio en sistemas ciber-físicos, lo cual es un aspecto clave en ciberseguridad. Se enfoca en estrategias de control para mitigar los efectos de ataques maliciosos en el seguimiento de señales de referencia en sistemas discretos.

Otros tópicos de investigación en este periodo que se muestran en la Figura 3.12 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 esta línea Espinosa D. M. y colaboradores se centra en proponer una alternativa procedural para ejecutar acciones que permitan elevar privilegios en sistemas Windows. "Convolutional neural networks" fueron utilizadas durante este periodo para autenticación por Wu J. y colaboradores. También se ha usado este tipo de red neuronal para la autenticación biométrica. Por otro lado, desde el punto de vista del área ACM **seguridad en software y aplicaciones** así como de la comunidad de **Métodos formales y teoría de la seguridad**, Orellana C. y colaboradores presenta un patrón para agregar seguridad a un componente clave de la arquitectura de Internet de las cosas, la çosa"de manera de modelar tanto sus amenazas como medidas de seguridad. También otro para los nodos actuadores. Muñoz-Vergara L y colaboradores, representan los requerimientos de seguridad utilizando la notación BPMN. Wu J. y colaboradores se enfocaron en la preservación de la

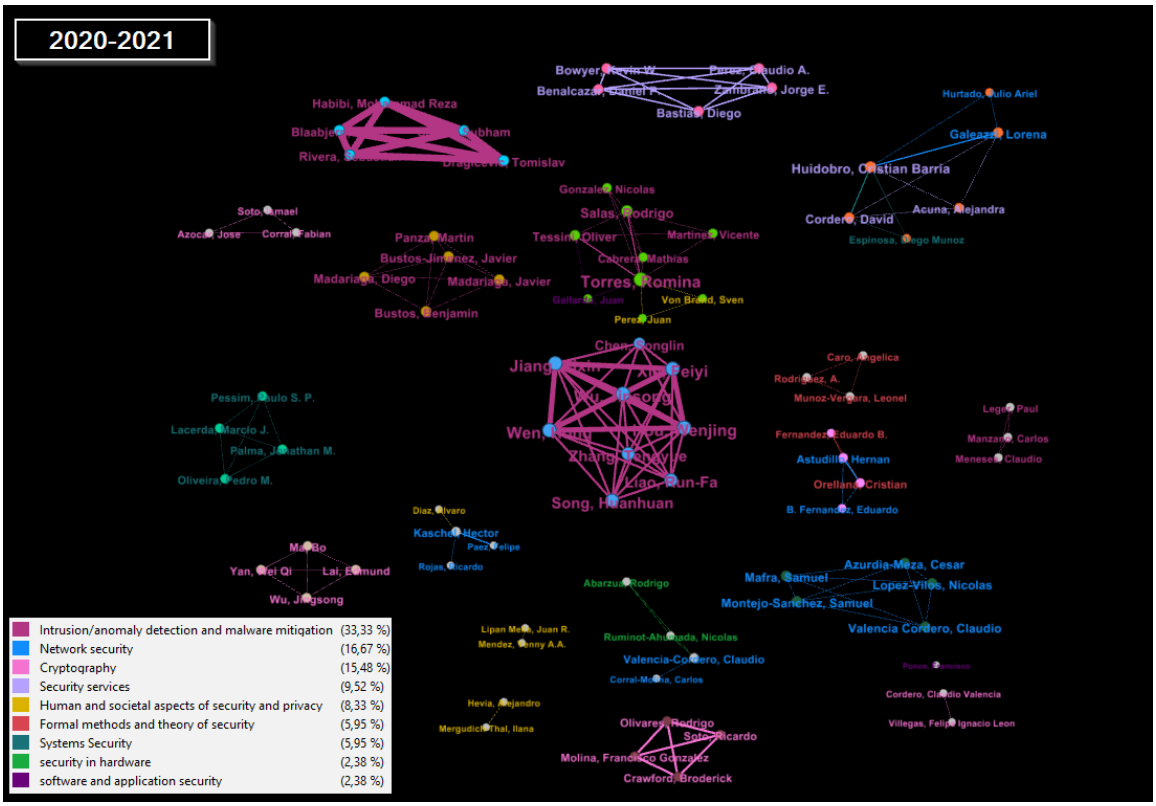


Figura 3.13: Autoras/Autores responsables de las investigaciones consideradas en este estudio publicadas durante periodo 2020–2021.

privacidad en el aprendizaje automático centralizado, proponiendo un nuevo método de generación de ruido basado en la entropía de la información y la privacidad diferencial. Barría Huidobro C. y colaboradores se centran en la elaboración de un modelo integrado que vincula los estándares de seguridad y las mediciones de los niveles de madurez de la organización en el sistema de gestión de seguridad de la información (SGSI). Esto implica una investigación sobre cómo mejorar la ciberseguridad mediante la integración y aplicación efectiva de varios estándares y modelos. Gallardo J. y colaboradores desarrollan una herramienta para que las micro y pequeñas empresas evalúen y mejoren su madurez en ciberseguridad, lo que implica aspectos fundamentales de la investigación en ciberseguridad y la aplicación de modelos de madurez para la adecuada medición de esta. Pérez J. y colaboradores desarrollan un videojuego para educar a niños entre 8 a 12 años sobre seguridad cibernética y conciencia respecto de las responsabilidades asociadas al uso de las tecnologías. Hevia A y Mergudich-Thal I. concentran esfuerzos en mejorar la implementación y eficiencia del protocolo WhoToo, que aborda la seguridad y privacidad alrededor de la denuncia de agresiones sexuales, con el fin de optimizar el proceso de detección de acusaciones duplicadas y coincidentes mientras mantiene el énfasis en la privacidad de las partes involucradas.

En general en el grafo de colaboración de autoras/autores mostrado en la Figura 3.13 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**.

3.2.5 2022–2023

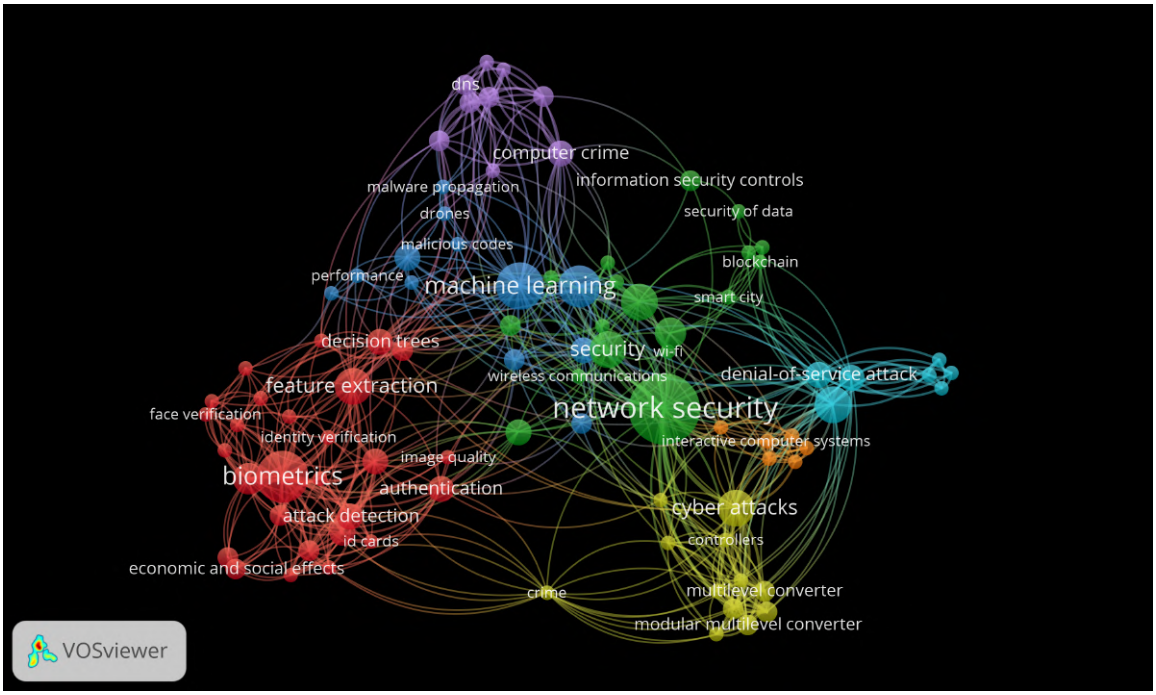


Figura 3.14: Principales tópicos en los que investigadoras e investigadores realizan investigación en periodo 2022–2023.

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. Aún así, en el corpus de documentos existe una serie de artículos respecto de este tópico de investigación. Berres S. y colaboradores proponen un método esteganográfico para ocultar información dentro de una imagen utilizando un mapa caótico Beta, un algoritmo de criptografía basado en el Estándar de Encriptación Avanzada (AES) y una clave privada para generar la expansión de la clave. Mosso E. describe un sistema óptico-criptográfico novedoso basado en un nuevo algoritmo de auto-desordenamiento de imágenes (ISDA). La investigación se centra en el desarrollo de un sistema criptográfico óptico con características de seguridad mejoradas, lo cual es un aspecto clave en la investigación y desarrollo en ciberseguridad. Gonzalez F. y colaboradores proponen diseño y mejora de cajas de sustitución (substitution boxes), esenciales en criptografía simétrica, utilizando enfoques como el algoritmo de búsqueda estocástica de fractales mejorado con aprendizaje basado en oposición. Estos esfuerzos buscan garantizar propiedades clave como la no linealidad para resistir ataques criptoanalíticos. Además, se exploró el ámbito de la seguridad cuántica mediante la implementación de Quantum Key Distribution (QKD) utilizando el protocolo BB84, realizado por Azócar J y colaboradores.

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**. En “Fair Face Verification”, Villalobos E. y colaboradores abordan la equidad en reconocimiento facial con atributos biométricos no sensibles. González S. y Tapia J., en “Refining ID Cards Presentation Attack Detection”, mejoran sistemas de detección de fraudes en verificación de identidad. “Iris Liveness Detection”, de Tapia J. y colaboradores, destaca en la prevención de ataques de presentación. “Synthetic ID Card Image Generation”, desarrollado por Benalcazar D. y colaboradores utiliza aprendizaje profundo para fortalecer sistemas de detección. “SoftVein-WELM”, de Zabala-Blanco D. y colaboradores, clasifica género y edad en patrones de venas en la palma, contribuyendo a la comprensión biométrica en la autenticación y destacando aspectos 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. La propuesta de Wu J. y colaboradores ofrece un servicio de detección seguro para redes de sensores inalámbricos (WSN), utilizando códigos de autenticación de mensajes y network coding, demostrando eficacia contra ataques de contaminación y reproducción. Además, en otro trabajo investigan la seguridad en la capa física (PLS) en redes de interferencia multiusuario, considerando la transmisión segura desde una fuente legítima (Alice) a un destino legítimo (Bob) en presencia de escuchas pasivas (Eves) y múltiples transceptores legítimos. Introducen un esquema de alineación de interferencia asistido por ruido artificial (AN) para mejorar la seguridad. A diferencia de los enfoques tradicionales de seguridad basados en la alineación de interferencia, que pueden resultar en la cancelación de la señal secreta, diseñan un esquema de minimización alternante modificado (AM) que incorpora la formación de haces de modo propio máximo (MEB) para la transmisión segura. Palma J. y colaboradores aborda la seguridad en sistemas ciberfísicos bajo ataques DoS, proponiendo acciones de mitigación y destacando la importancia de considerar la seguridad en el diseño de sistemas ciberfísicos. Burgos-Mellado C. y colaboradores exploran la ciberseguridad en sistemas de control para convertidores modulares multinivel (M2Cs) centrándose en la detección de ataques de inyección de datos falsos (FDIA) mediante un método basado en aprendizaje por refuerzo (RL). López-Vilos N. y colaboradores proponen una estrategia de auto-curación basada en clustering para redes de sensores inalámbricos (WSNs) enfrentadas a ataques de interferencia, como los ataques de jamming. La estrategia, denominada Fairness Cooperation with Power Allocation (FCPA), utiliza la formación de clústeres y ajusta la potencia de transmisión para superar eficientemente los ataques de jamming.

En el ámbito de la detección de malware en dispositivos Android, el estudio de Manzano C. y colaboradores destaca por su enfoque en la selección de características mediante técnicas estadísticas, mejorando la identificación de tráfico malicioso con un énfasis en la eficacia del algoritmo de bosques aleatorios. En el ámbito de la simulación de la propagación de malware en enjambres de drones, Saldaña E. y colaboradores contribuyen con un enfoque basado en epidemiología matemática, proporcionando una base conceptual para entender y mitigar la propagación de códigos maliciosos en este contexto emergente. Leger P. y colaboradores abordan la detección de paquetes sospechosos en tiempo real para defenderse contra ataques DDoS al combinar análisis discriminante lineal (LDA) y un mapa autoorganizado supervisado (SOM) en un enfoque llamado LSSOM. Adasme P. y colaboradores abordan el aumento de las amenazas a los sistemas de Internet de las cosas mediante un método eficiente para detectar ciberataques e intrusiones en la red basado en clasificadores de ML mejorados. Salazar H. y colaboradores abordan la categorización más rápida de gusanos informáticos que tienen obfuscación en su código, proponiendo el desarrollo de un componente tecnológico

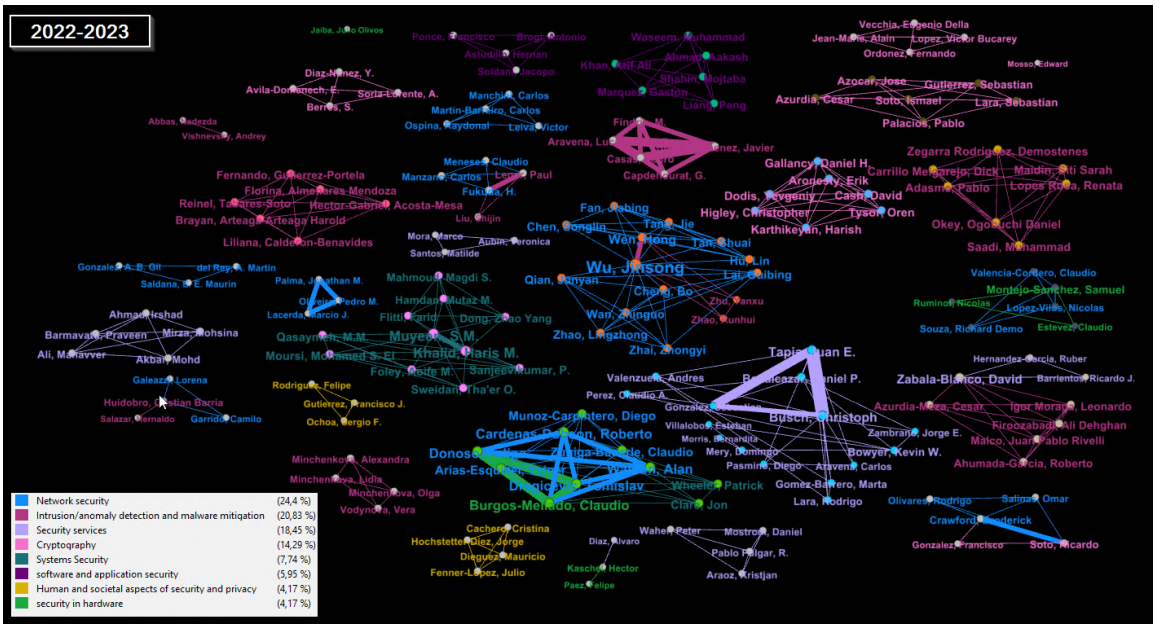


Figura 3.15: Autoras/Autores responsables de las investigaciones consideradas en este estudio publicadas durante periodo 2020–2021.

para facilitar la clasificación automatizada. Aravena L.T. y colaboradores proponen PHISHWEB, un enfoque para la detección de phishing en sitios web. La investigación aborda la detección y categorización de sitios maliciosos, especialmente en el contexto de dominios falsos y generación automática de dominios mediante tecnología DGA (Domain Generation Algorithm). En otro artículo, propone un enfoque para la detección rápida de dominios generados por DGA mediante el análisis de características lexicográficas exclusivamente derivadas del nombre de dominio observado en una consulta DNS. Además, se propone un sistema de puntuación basado en la reputación de nombres de dominio y se emplean técnicas de aprendizaje automático para mejorar el rendimiento de la detección. Igor Moraga L. y colaboradores proponen el uso de un algoritmo de aprendizaje automático (extreme learning machine, ELM) para la detección de malware, centrándose en la lucha contra la obfuscación y la detección de malware oculto. Se menciona la clasificación de virus en familias de troyanos, spyware y ransomware, y se analiza el rendimiento de diferentes variantes de ELM en la clasificación binaria y múltiple. Tabares-Soto R. y colaboradores presentan un nuevo conjunto de datos (IDSAI) el cual es probado con diferentes modelos para estudiar capacidad de generalización obteniendo hasta un 94 % de precisión. Salinas O. y colaboradores proponen una estrategia integral de ciberseguridad que utiliza una estrategia de optimización con múltiples objetivos para un Sistema de Gestión de Información y Eventos de Seguridad (SIEM) con sensores de detección de intrusos en red, permite la identificación y respuesta inmediata a actividades sospechosas. Adicionalmente, Galeazzi L. y colaboradores aportan a la seguridad en redes Wi-Fi con una validación experimental de variables de seguridad para auditorías, destacando la importancia de considerar la evolución de estas redes en términos de seguridad.

Áreas de investigación tales como **seguridad en software y aplicaciones** experimentan una contracción en este periodo. Márquez G. y colaboradores abordan desafíos en la selección e implementación de patrones y estrategias en el ciclo de vida de los microservicios, centrándose en

áreas clave como la descomposición de aplicaciones en microservicios, seguridad, comunicación y descubrimiento de servicios. Leiva V. y colaboradores proponen un novedoso enfoque en privacidad diferencial, centrado en modelos de regresión bajo heterocedasticidad. Este método, respaldado por una sólida base matemática, garantiza la confidencialidad de los datos y la resistencia contra ataques de identificación invasivos.

Tal como puede apreciarse en la Figura 3.15 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**.

4. Áreas Prioritarias de Investigación

Partimos de la base que todas las áreas de investigación en seguridad y privacidad son necesarias.

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". Para ello, el MinCiencia realizó una invitación por correo electrónico a 40 investigadoras e investigadores del subconjunto total parte de este estudio con la restricción de que a Diciembre 2023 tuvieran afiliación chilena según la base de datos Scopus. El panel se conformó con siete investigadoras e investigadores más la presencia de un representante del CSIRT de gobierno [1]. En esta actividad, primero se presentaron los principales hallazgos del estudio respecto de las capacidades actuales de las investigadoras y los investigadores. Segundo, en conjunto con el panel 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, Factor D3.4 Investigación e Innovación en ciberseguridad donde vemos que para el nivel de madurez **establecido** es necesario tener colaboración internacional, que para el nivel **estratégico** en este factor es necesario tener comunidades de I+D alrededor de ciertas temáticas y que para el nivel **dinámico** es necesario mostrar evidencia de que estamos usando la I+D para estar preparados como país para amenazas actuales o futuras.

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

[1] Eduardo Riveros, arquitecto de seguridad de CSIRT

los que debemos trabajar para estar preparados a amenazas actuales y futuras.

4.1 Hacia un Chile con nivel de madurez en ciberseguridad establecido (2024-2027)

La Figura 4.1 muestra en amarillo que aproximadamente el 50 % de las autoras y los autores (que fueron parte de este estudio) a Diciembre 2023 tienen afiliación chilena. Similar al nacimiento de la la red nacional de investigación en ciberseguridad en España, es relevante reconocer esta red de investigadoras e investigadores a lo largo del país como punto inicial de la red nacional de investigadoras e investigadores en ciberseguridad de Chile.

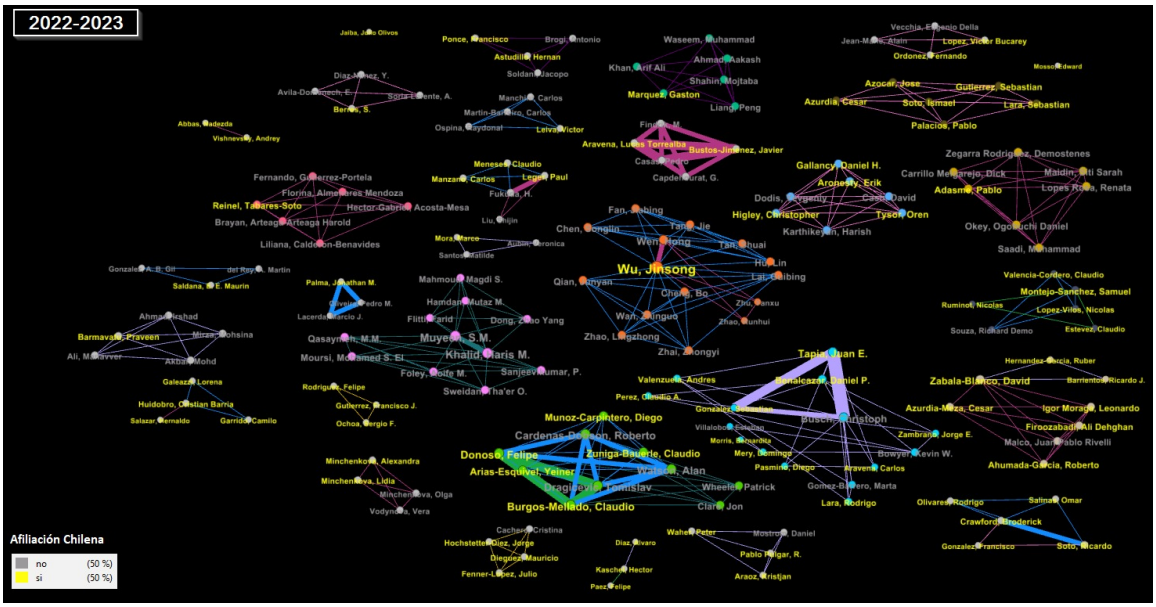


Figura 4.1: Investigadoras e Investigadores del último periodo que presentan afiliación chilena versus las y los que no.

Tal como podemos ver en la Figura 4.2, 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.

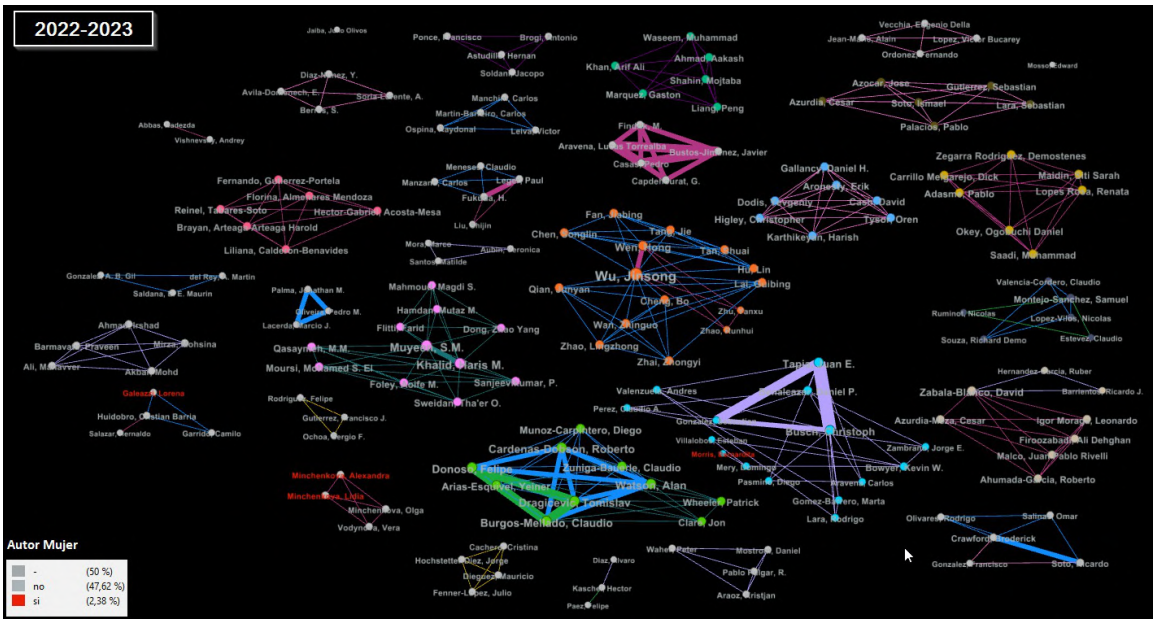


Figura 4.2: Mujeres con afiliación chilena responsables de la producción científica en ciberseguridad en Chile coloreadas en rojo.

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 el factor D3.4 un nivel de madurez establecido en el corto plazo.

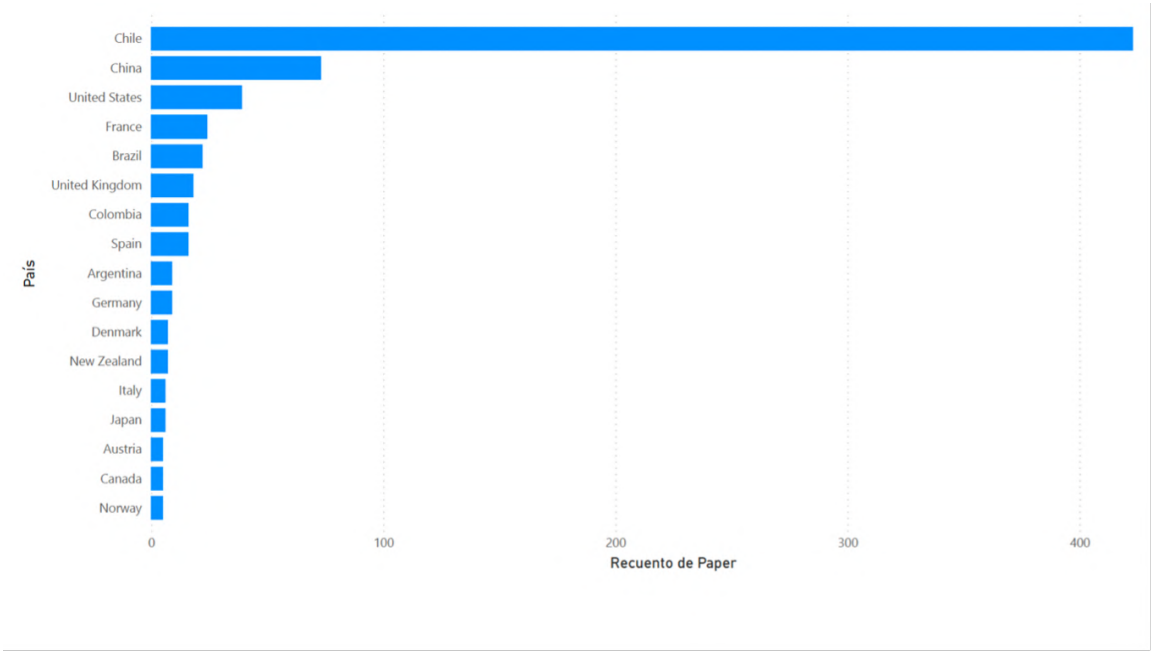


Figura 4.3: Los países con los que Chile compartió autoría para artículos publicados en el periodo 2012–2023.

4.2 Hacia un Chile con nivel de madurez en ciberseguridad estratégico (2028-2031)

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 (ver subáreas de investigación de ACM en Anexo).

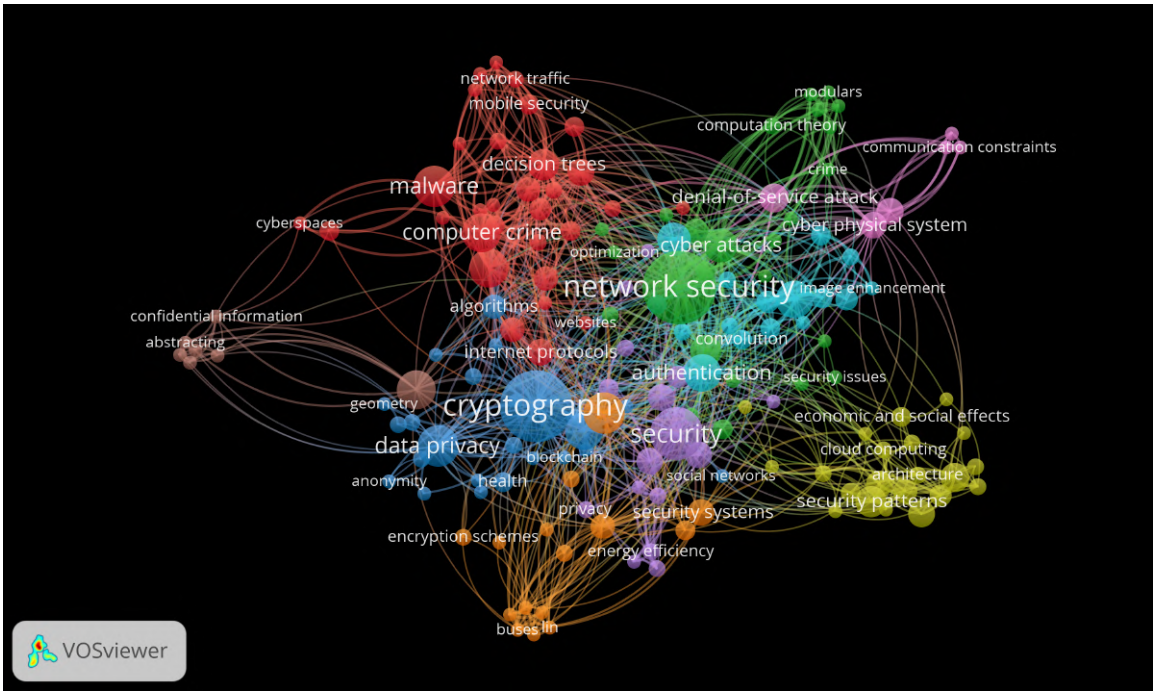


Figura 4.4: Principales tópicos en los que investigadores en publicaron resultados durante periodo 2012–2023

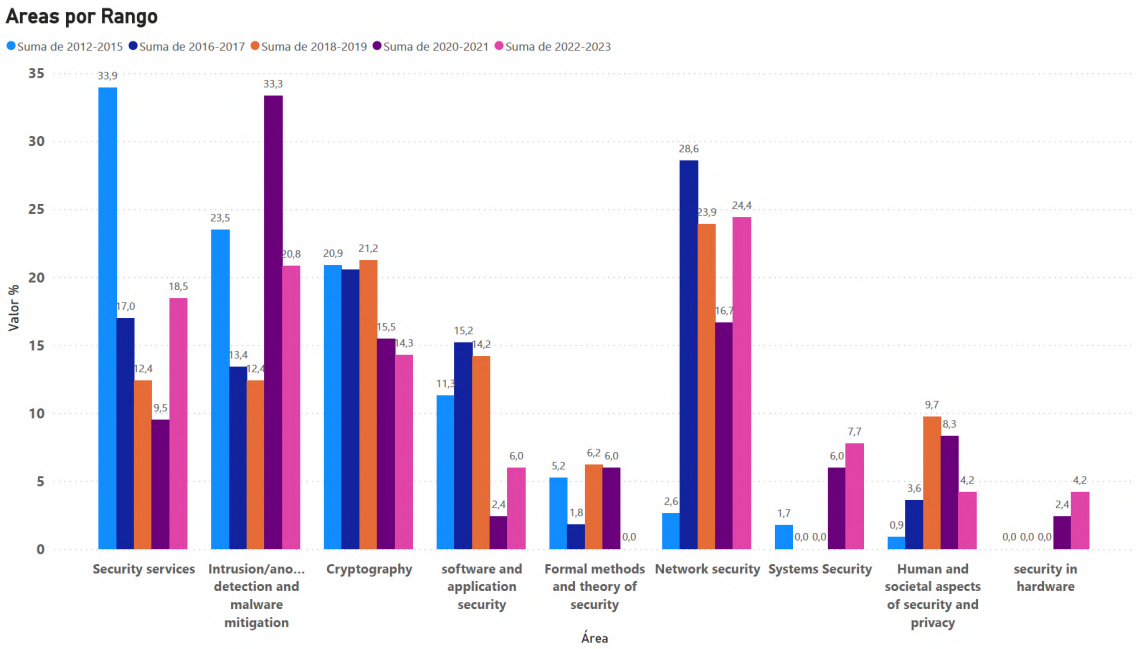


Figura 4.5: Detalle de las áreas de la ACM en la que han hecho contribuciones los investigadores durante periodo 2012–2023.

4.3 Hacia un Chile con nivel de madurez en ciberseguridad establecido (2032-2035)

Para que Chile eventualmente pueda alcanzar el nivel dinámico es necesario mostrar evidencia de que se está usando la I+D para estar preparados como país para amenazas actuales o futuras. En ese sentido, 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.

4.3.1 Criptografía postcuántica

A corto plazo, la curva elíptica puede ser atractiva, pero la incertidumbre respecto a su futuro resalta la necesidad de orientar esfuerzos hacia la criptografía poscuántica. En un contexto donde la incertidumbre se convierte en una característica clave, es crucial fortalecer el desarrollo del capital humano y la ejecución de proyectos que consoliden un grupo fuerte en este campo, no solo en términos teóricos, sino también en su implementación.

En este panorama de incertidumbre, las amenazas y oportunidades inherentes a la computación cuántica se entrelazan. 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). Esta área se centra en desarrollar métodos de cifrado que permanezcan seguros incluso en un entorno amenazado por la computación cuántica. De manera crucial, las técnicas que aprovechan los efectos cuánticos, como la superposición, la entrelazación y la incertidumbre, ejemplificadas por la Distribución Cuántica

de Claves (QKD), representan un enfoque prometedor. Al basarse en principios de la mecánica cuántica, estas técnicas ofrecen la generación de claves de cifrado seguras, resistentes a ciertos tipos de ataques y contribuyen al avance hacia un futuro cuántico más seguro. Áreas a abordar:

1. **Criptoanálisis y otros ataques:**
   Investigación en métodos para analizar y contrarrestar posibles ataques a algoritmos postcuánticos.
2. **Técnicas de teoría de la información:**
   Aplicación de conceptos de teoría de la información específicos para la seguridad de la información postcuántica.
3. **Gestión de claves:**
   Desarrollo de métodos para la generación, distribución y gestión segura de claves criptográficas resistentes a ataques cuánticos.
4. **Fundamentos matemáticos de la criptografía:**
   Investigación de los fundamentos matemáticos que respaldan los algoritmos criptográficos postcuánticos.
5. **Técnicas de clave pública (asimétricas):**
   a) **Firmas digitales:**
   Estudio y aplicación de firmas digitales para autenticación y verificación en un entorno postcuántico.
   b) **Cifrado de clave pública:**
   Desarrollo de algoritmos para cifrar información con claves públicas resistentes a ataques cuánticos.
6. **Criptografía simétrica y funciones hash:**
   a) **Cifrado de bloques y de flujo:**
   Investigación de algoritmos de cifrado simétrico en un contexto postcuántico.
   b) **Funciones hash y códigos de autenticación de mensajes:**
   Desarrollo de funciones hash y códigos de autenticación resistentes a ataques cuánticos.

4.3.2 Desarrollo seguro de sistemas ciberfísicos

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. Esto es relevante tanto a nivel "micro" pensando en sistemas embebidos, pasando por dispositivos médicos vestibles o portables a Infraestructura crítica. Dado que la Infraestructura crítica comprende activos físicos, sistemas, redes y funciones esenciales para el funcionamiento continuo de una sociedad abordando sectores como energía, agua, transporte, entre otros, es que esta área se cree necesaria para proteger la Infraestructura crítica por diseño.

Los sistemas ciberfísicos al igual que los software son composiciones de componentes (locales o distribuidos, físicos o lógicos, propios o de terceros), la falla de uno de ellos puede producir fallas en cascada de múltiples sistemas con impactos devastadores no predecibles. La cadena de suministro global, en la que se enmarcan estos sistemas, incluso superan límites geográficos. Un fallo en un componente puede desencadenar consecuencias en cascada que afectan no solo la resiliencia local, sino también la integridad de sistemas críticos a escala global con impactos graves en la salud, seguridad y bienestar económico de una nación. Para ello es importante considerar que estos componentes pueden tener brechas de seguridad pronunciada de origen en el área de las Operaciones Técnicas (OT) más que de Tecnologías de Información (TI). Para ello la Figura 4.6 muestra tácticas

y técnicas de ataque a las que son vulnerables los sistemas de control industrial acorde a MITRE ATT&CK.

En ese sentido, en esta área de investigación prioritaria es necesario considerar:

- Seguridad en hardware: Investigación y desarrollo de mecanismos de seguridad para sistemas integrados, ataques y contramedidas en hardware, ingeniería inversa de hardware, e implementación de seguridad en hardware.
- Aspectos Humanos y Sociales de la Seguridad y Privacidad en Sistemas Ciberfísicos que consideren desarrollo de métodos y tecnologías para proteger la privacidad de los individuos en sistemas ciberfísicos.
- Tecnologías emergentes, como la interacción humano-computadora redefinida generan nuevos riesgos.
- 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: en particular investigación de requisitos específicos para garantizar la seguridad en sistemas ciberfísicos desde el diseño así como marcos de Confianza para Sistemas Ciberfísicos Seguros.
- Arquitectura segura para sistemas ciberfísicos interconectados y distribuidos. Nuevas generaciones de comunicaciones móviles (5G a 6G), introducen nuevos riesgos. El diseño de enfoques para la monitorización de sistemas a gran escala, interconectados y la exploración de algoritmos biomiméticos en ciberseguridad son áreas clave. Incorporar el concepto de seguridad por diseño, evaluando la seguridad frente a diferentes intentos maliciosos, y preservar la privacidad y confidencialidad del flujo de información son elementos esenciales. Se requiere investigación en desarrollo de nuevos enfoques para evaluar el impacto de dependencias e interdependencias y la Definición de interfaces seguras e interoperables entre diferentes sistemas ciberfísicos (y eventualmente infraestructuras críticas) para prevenir efectos en cascada.
- Seguridad de base de datos y almacenamiento de Sistemas Ciberfísicos Seguros. La gran cantidad de datos que generan potencialmente estos sistemas, tensionan los actuales modelos de anonimización y en los mecanismos de protección que sigan los requisitos de privacidad por diseño y por defecto. Saneamiento de datos, monitoreo, responsabilidad, así como la gestión y Consulta de Datos Cifrados en Sistemas Ciberfísicos.

Figura 4.6: Matriz de técnicas y tácticas en Sistemas de Control Industrial

4.3.3 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 [2].

[2]Más Información en Proyecto ATLAS de MITRE ATT&CK `https://atlas.mitre.org/`

Figura 4.7: Matriz de técnicas y tácticas en Sistemas para Inteligencia Artificial

4.3.4 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:

- Desarrollo de Herramientas Educativas Avanzadas: Crear herramientas interactivas y educativas que ayuden a las organizaciones y usuarios a comprender la importancia de la ciberseguridad. Integrar simulaciones y escenarios realistas para ilustrar las consecuencias de vulnerabilidades y ataques.
- Investigación en Aspectos Humanos y Sociales: Estudiar la economía de la seguridad y privacidad para comprender los incentivos y desincentivos asociados con la implementación de medidas de seguridad. Desarrollar métodos y tecnologías para proteger la privacidad, considerando las expectativas y necesidades de los individuos.
- Campañas de Concientización Efectivas: Diseñar campañas de concientización que sean efectivas y adaptables a diversos públicos, destacando los riesgos y mejores prácticas de seguridad. Evaluar experimentalmente la eficacia de estas campañas en la mejora de la conciencia y el comportamiento de seguridad.
- Usabilidad en Soluciones de Seguridad y Privacidad: 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. Desarrollar interfaces intuitivas que faciliten la adopción de medidas de seguridad. Si hay uso de Inteligencia Artificial entonces se debe utilizar métodos de la Inteligencia Artificial explicable centrada en el usuario (HCXAI).
- Enfoque Interdisciplinario: Esta área busca no solo mejorar la comprensión técnica de la ciberseguridad, sino también abordar los desafíos humanos y sociales, garantizando que las soluciones sean efectivas, respeten la privacidad y sean adoptadas de manera generalizada. Se debe fomentar la colaboración entre expertos en ciberseguridad, educadores, psicólogos y profesionales de la comunicación para diseñar enfoques holísticos. Integrar la ciberseguridad en programas educativos formales e informales.

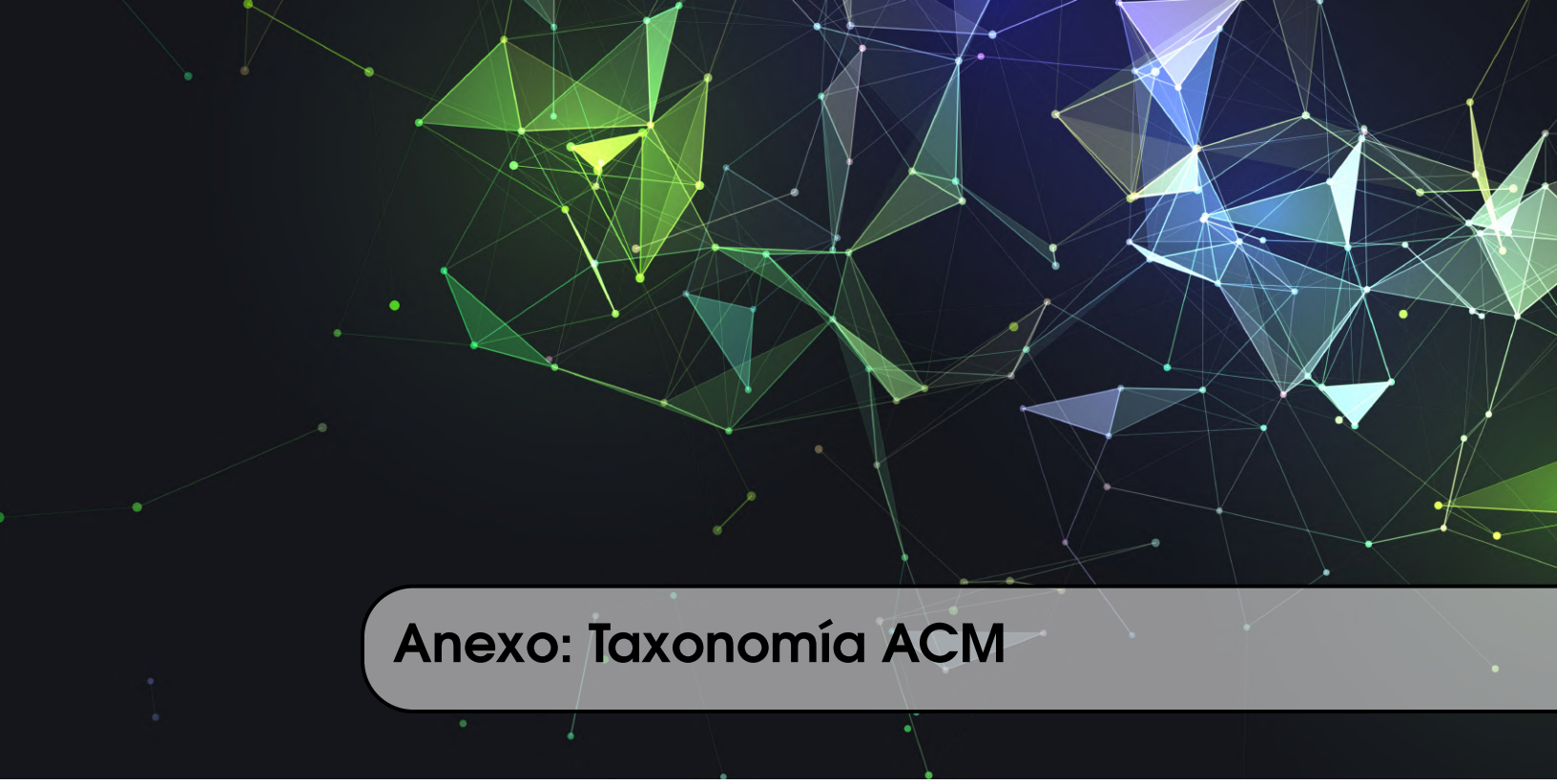
5. Conclusiones y trabajo futuro

En este trabajo, se ha realizado un análisis de los investigadores con afiliación chilena en el área de ciberseguridad durante los últimos 10 años. En particular, se ha realizado una 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. Esta propuesta se ha formulado considerando las capacidades identificadas, contrastadas con los lineamientos derivados del factor **D3.4 Investigación e Innovación en ciberseguridad del modelo de capacidades de madurez en ciberseguridad de Oxford**, y siempre en directa relación al **Eje 5 de la actual política nacional de ciberseguridad 2023-2028**.

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.

En un contexto más amplio, se espera que este informe sirva como catalizador para el desarrollo de una industria de empresas de base científico tecnológica en ciberseguridad en Chile. Se busca crear las condiciones propicias para que investigadores, que actualmente trabajan en silos, converjan en comunidades de investigación centradas en las áreas prioritarias identificadas, entre otras. Importante recalcar que el compromiso del Ministerio CTCI es fundamental para el desarrollo de estas cuatro áreas, fomentando la consolidación de las comunidades de I+D en ciberseguridad identificadas, apoyándolas con instrumentos que fomenten la colaboración nacional/regional/internacional/multidisciplinar, la descentralización, la consolidación y constante crecimiento en el tiempo con más investigadoras e investigadores, además de la data abierta, el código abierto y buenas prácticas de seguridad y privacidad para desarrollar la Industria I+D+i en ciberseguridad en nuestro país.

Como trabajo futuro, primero es importante mencionar que al revisar los proyectos entregados por la Agencia Nacional de Investigación y Desarrollo (ANID), no se identificaron proyectos de investigación aplicada en ciberseguridad. Tampoco se encontraron a Octubre 2023 en los reportes de EBCT de empresas de base científica tecnológica en ciberseguridad en Chile (`https://www.observa.minciencia.gob.cl/encuestas/directorio-ebct`). Para abordar esta brecha, se presenta como trabajo futuro en el **Anexo: Instrumento de Consulta** un instrumento de encuesta diseñado para evaluar las capacidades de ciberseguridad en centros y laboratorios en Chile. Este instrumento puede aplicarse incluso en aquellos casos en los que la investigación aplicada en ciberseguridad no sea el objetivo principal. Por ejemplo, un centro basal investigando en una cierta patología donde existan investigadoras e investigadores contribuyendo en temáticas específicas, como la criptografía postcuántica para garantizar la seguridad de la información médica que se transmite o almacena.



Anexo: Taxonomía ACM

1. **Criptografía (ACM: Cryptography)**
   - *a*) **Criptoanálisis y otros ataques (ACM: Cryptanalysis and other attacks):** Estudio y desarrollo de métodos para analizar y contrarrestar ataques criptográficos.
   - *b*) **Técnicas de teoría de la información (ACM: Information-theoretic techniques):** Aplicación de conceptos de teoría de la información a la seguridad de la información.
   - *c*) **Gestión de claves (ACM: Key management):** Desarrollo de métodos para la generación, distribución y gestión segura de claves criptográficas.
   - *d*) **Fundamentos matemáticos de la criptografía (ACM: Mathematical foundations of cryptography):** Investigación de los fundamentos matemáticos que respaldan los algoritmos criptográficos.
   - *e*) **Técnicas de clave pública (asimétricas) (ACM: Public key techniques):**
     1) **Firmas digitales (ACM: Digital signatures):** Estudio y aplicación de firmas digitales para autenticación y verificación.
     2) **Cifrado de clave pública (ACM: Public key encryption):** Desarrollo de algoritmos para cifrar información con claves públicas.
   - *f*) **Criptografía simétrica y funciones hash (ACM: Symmetric cryptography and hash functions):**
     1) **Cifrado de bloques y de flujo (ACM: Block and stream ciphers):** Investigación de algoritmos de cifrado simétrico.
     2) **Funciones hash y códigos de autenticación de mensajes (ACM: Hash functions and message authentication codes):** Desarrollo de funciones hash y códigos de autenticación.
2. **Seguridad de bases de datos y almacenamiento (ACM: Database and storage security)**
   - *a*) **Anonimización y saneamiento de datos (ACM: Data anonymization and sanitization):** Métodos para proteger la privacidad al anonimizar y limpiar datos.
   - *b*) **Monitoreo de actividad en bases de datos (ACM: Database activity monitoring):**

Desarrollo de herramientas para monitorear y auditar la actividad en bases de datos.

   c) **Responsabilidad de la información y control de uso (ACM: Information accountability and usage control):** Investigación de mecanismos para garantizar la responsabilidad y controlar el uso de la información.
   d) **Gestión y consulta de datos cifrados (ACM: Management and querying of encrypted data):** Desarrollo de técnicas para gestionar y consultar datos cifrados de manera segura.
3. **Métodos formales y teoría de la seguridad (ACM: Formal methods and theory of security)**
   a) **Modelos formales de seguridad (ACM: Formal security models):** Desarrollo y estudio de modelos formales para describir y analizar la seguridad.
   b) **Lógica y verificación (ACM: Logic and verification):** Aplicación de la lógica y métodos de verificación en el diseño seguro de sistemas.
   c) **Requisitos de seguridad (ACM: Security requirements):** Investigación de requisitos específicos para garantizar la seguridad en sistemas.
   d) **Marcos de confianza (ACM: Trust frameworks):** Desarrollo de marcos que establecen la confianza en entornos seguros.
4. **Aspectos humanos y sociales de la seguridad y privacidad (ACM: Human and societal aspects of security and privacy)**
   a) **Economía de la seguridad y privacidad (ACM: Economics of security and privacy):** Estudio de los aspectos económicos relacionados con la seguridad y privacidad.
   b) **Protecciones de privacidad (ACM: Privacy protections):** Desarrollo de métodos y tecnologías para proteger la privacidad de los individuos.
   c) **Aspectos sociales de la seguridad y privacidad (ACM: Social aspects of security and privacy):** Investigación de los aspectos sociales relacionados con la seguridad y privacidad.
   d) **Usabilidad en seguridad y privacidad (ACM: Usability in security and privacy):** Estudio de la usabilidad de las soluciones de seguridad y privacidad.
5. **Detección de intrusiones/mitigación de malware (ACM: Intrusion/anomaly detection and malware mitigation)**
   a) **Sistemas de detección de intrusiones (ACM: Intrusion detection systems):** Desarrollo y evaluación de sistemas para detectar intrusiones en redes y sistemas.
   b) **Malware y su mitigación (ACM: Malware and its mitigation):** Investigación de métodos para prevenir y mitigar el impacto del malware.
   c) **Ataques de ingeniería social (ACM: Social engineering attacks):**
      1) **Phishing (ACM: Phishing):** Estudio y contramedidas contra ataques de phishing.
      2) **Ataques de suplantación (ACM: Spoofing attacks):** Investigación sobre ataques que involucran suplantación de identidad.
6. **Seguridad de redes (ACM: Network security)**
   a) **Ataques de denegación de servicio (ACM: Denial-of-service attacks):** Investigación y mitigación de ataques que buscan interrumpir servicios.
   b) **Firewalls (ACM: Firewalls):** Desarrollo y configuración de firewalls para proteger redes.
   c) **Seguridad móvil e inalámbrica (ACM: Mobile and wireless security):** Investigación de amenazas y soluciones de seguridad en entornos móviles e inalámbricos.
   d) **Protocolos de seguridad (ACM: Security protocols):** Desarrollo y análisis de protocolos de seguridad para la comunicación segura.
   e) **Seguridad de protocolos web (ACM: Web protocol security):** Investigación y mejora

de la seguridad en protocolos web.

7. **Seguridad en hardware (ACM: Security in hardware)**
   - *a*) **Seguridad en sistemas integrados (ACM: Embedded systems security):** Investigación y desarrollo de mecanismos de seguridad para sistemas integrados.
   - *b*) **Ataques y contramedidas en hardware (ACM: Hardware attacks and countermeasures):**
     1) **Modificaciones maliciosas de diseño (ACM: Malicious design modifications):** Estudio y prevención de modificaciones maliciosas en el diseño de hardware.
     2) **Análisis de canales secundarios y contramedidas (ACM: Side-channel analysis and countermeasures):** Investigación sobre análisis de canales secundarios y contramedidas.
   - *c*) **Ingeniería inversa de hardware (ACM: Hardware reverse engineering):** Métodos para analizar y comprender hardware existente.
   - *d*) **Implementación de seguridad en hardware (ACM: Hardware security implementation):**
     1) **Protocolos de seguridad basados en hardware (ACM: Hardware-based security protocols):** Desarrollo de protocolos de seguridad basados en hardware.
     2) **Diseños a prueba de manipulaciones y resistentes a manipulaciones (ACM: Tamper-proof and tamper-resistant designs):** Desarrollo de hardware que es resistente a manipulaciones maliciosas.
8. **Servicios de seguridad (ACM: Security services)**
   - *a*) **Control de acceso (ACM: Access control):** Desarrollo de políticas y mecanismos para controlar el acceso a recursos.
   - *b*) **Autenticación (ACM: Authentication):**
     1) **Biometría (ACM: Biometrics):** Uso de características biológicas para la autenticación.
     2) **Contraseñas gráficas/visuales (ACM: Graphical/visual passwords):** Desarrollo y evaluación de métodos visuales para autenticación.
     3) **Autenticación multifactor (ACM: Multi-factor authentication):** Implementación de métodos de autenticación que utilizan múltiples factores.
   - *c*) **Autorización (ACM: Authorization):** Desarrollo de sistemas para autorizar y controlar acciones de usuarios.
   - *d*) **Gestión de derechos digitales (ACM: Digital rights management):** Métodos para proteger y gestionar los derechos digitales de los usuarios.
   - *e*) **Protocolos de preservación de la privacidad (ACM: Privacy-preserving protocols):** Desarrollo de protocolos que permiten la colaboración sin revelar información privada.
   - *f*) **Pseudonimato, anonimato e inrastreabilidad (ACM: Pseudonymity, anonymity and untraceability):** Investigación y desarrollo de técnicas que permiten el uso de identidades ficticias o anónimas.
9. **Seguridad de software y aplicaciones (ACM: Software and application security)**
   - *a*) **Arquitecturas de seguridad y privacidad específicas de dominio (ACM: Domain-specific security and privacy architectures):** Desarrollo de arquitecturas de seguridad específicas para dominios particulares.
   - *b*) **Seguridad y privacidad en redes sociales (ACM: Social network security and privacy):** Investigación de amenazas y soluciones de seguridad y privacidad en redes sociales.
   - *c*) **Ingeniería inversa de software (ACM: Software reverse engineering):** Análisis y comprensión de software existente.
   - *d*) **Ingeniería de seguridad de software (ACM: Software security engineering):** Desarrollo

de métodos y prácticas para construir software seguro.

e) **Seguridad de aplicaciones web (ACM: Web application security):** Investigación y desarrollo de técnicas para proteger aplicaciones web contra amenazas.

10. **Seguridad de sistemas (ACM: Systems security)**
    a) **Seguridad de navegadores (ACM: Browser security):** Investigación y desarrollo de medidas de seguridad para navegadores web.
    b) **Ataques de denegación de servicio (ACM: Denial-of-service attacks):** Investigación y mitigación de ataques diseñados para interrumpir servicios.
    c) **Seguridad de sistemas distribuidos (ACM: Distributed systems security):** Investigación y desarrollo de medidas de seguridad para sistemas distribuidos.
    d) **Seguridad de sistemas de archivos (ACM: File system security):** Desarrollo de métodos para proteger la integridad y confidencialidad de sistemas de archivos.
    e) **Firewalls (ACM: Firewalls):** Desarrollo y configuración de firewalls para proteger sistemas.
    f) **Control de flujo de información (ACM: Information flow control):** Desarrollo de técnicas para controlar y monitorear el flujo de información en sistemas.
    g) **Seguridad de sistemas operativos (ACM: Operating systems security):**
        1) **Seguridad de plataformas móviles (ACM: Mobile platform security):** Investigación y desarrollo de medidas de seguridad específicas para plataformas móviles.
        2) **Computación de confianza (ACM: Trusted computing):** Desarrollo y evaluación de entornos de cómputo confiables.
        3) **Virtualización y seguridad (ACM: Virtualization and security):** Investigación de medidas de seguridad en entornos virtualizados.
    h) **Gestión de vulnerabilidades (ACM: Vulnerability scanners)**: Desarrollo y uso de herramientas para identificar vulnerabilidades en sistemas

Anexo: Instrumento de Consulta

En este estudio, buscamos levantar las capacidades de ciberseguridad que los centros podrían tener, entendiendo que la ciberseguridad es transversal. El objetivo es identificar nodos a nivel nacional que puedan convertirse en una red nacional de investigación en ciberseguridad, permitiendo que las comunidades de equipos de investigación desarrollen proyectos conjuntos en apoyo al Pilar 5 de la PNC.
Formulario `http://tinyurl.com/5eu9kn4y`
Ejemplo de salida: `https://www.renic.es/es/mapa-idi-en-ciberseguridad`
Indica que la pregunta es obligatoria (*)

Nombre del Centro/Lab/Spin-off (*)

Institución en la que se aloja (si aplica)

Descripción del Centro/Lab/Spin-off (indicar sus objetivos)

Sitio web del Centro/Lab/Spin-off (*)

Representante del Centro/Lab/Spin-off (indicar modo de contacto) (*)

Regimen (*)

- Público
- Privado
- Otro: _____

Tipo (*)

- Centro tecnológico
- Centro de Investigación
- Laboratorio
- Institución de Educación Superior
- Otro: _____

Mencione las regiones en las que está presente (físicamente) (*)

- Región de Arica y Parinacota
- Región de Tarapacá
- ... (Agregar todas las regiones)

Fecha desde la que opera el Centro/lab/Spin-off (*)

Realiza actividad de I+D de manera sistemática (*)

¿Cuáles son las áreas de investigación? (*)

- Análisis Big Data enfocado respecto de la privacidad
- Análisis de datos a gran escala
- ... (Agregar todas las áreas)

¿El trabajo de investigación del laboratorio se enfoca en aspectos teóricos y fundamentales del conocimiento científico o en aplicaciones prácticas y soluciones específicas? (*)

- Aspectos teóricos y fundamentales
- Aplicaciones prácticas y soluciones específicas

---

3 Principales proyectos los últimos 10 años (título, activo, ¿Apoyo obtenido por concurso a Fondo público en I+D+i)? (*)

---

3 Principales publicaciones (título y doi) - adicionar patentes si las hay (*)

---

3 Principales patentes si las hay (*)

¿Basa su operación en tecnologías desarrolladas en este centro/lab/spin-off? (*)

---

3 Enlaces a noticias de difusión general de la tecnología desarrollada (*)

Cantidad de colaboradores altamente calificados aplicados a tareas de I+D (Magister o Doctor)(*)

- hasta 1
- entre 2 y 4

- entre 5 y 10
- más de 10

Cantidad de investigadores que aborda o que potencialmente debería abordar aspectos de ciberseguridad en su investigación (*)

- hasta 5
- entre 6 y 10
- entre 11 y 15
- más de 15

Cantidad de personas que trabajan en el centro/laboratorio/spin-off (*)

- hasta 5
- entre 6 y 10
- entre 11 y 15
- más de 15

Cantidad de alumnos en formación en I+D en ciberseguridad (*)

- hasta 5
- entre 6 y 10
- entre 11 y 15
- más de 15

Cantidad de mujeres en en formación o en I+D en ciberseguridad (app porcentaje) (*)

- hasta 5
- entre 6 y 10
- entre 11 y 15
- más de 15

¿Entrega servicios? (*)

- Acceso para investigación y pruebas reales
- Acceso para investigación y pruebas en plantas piloto
- ... (Agregar todos los servicios)

¿Qué áreas identifican tu centro/laboratorio/spin-off? (*)

- ... (Agregar todas las áreas)

¿En qué sectores opera el laboratorio? (*)

- Energía
- Telecomunicaciones

– ... (Agregar todos los sectores)

¿Cuáles son las áreas de aplicación? (*)

– Análisis Big Data enfocado respecto de la privacidad
– Análisis de datos a gran escala
– ... (Agregar todas las áreas)

Indique tipo de Software y aplicaciones disponibles en la infraestructura de software relacionados al fin del laboratorio (*)

– Herramientas de simulación
– Herramientas de supervisión
– ... (Agregar todos los tipos)

Indique programas y aplicaciones disponibles en la infraestructura de software relacionados al fin del laboratorio (ejemplo: LabView). (*)

Comentarios (*)

Referencias

[1] Comisión del Senado de la República de Chile: Desafíos del Futuro, Ciencia, Tecnología e Innovación. (2023). Construyendo la ciberseguridad en Chile. Editorial:Biblioteca del Congreso Nacional de Chile.

[2] Elango, B., Matilda, S., Martina Jose Mary, M., & Arul Pugazhendhi, M. (2023). Mapping the cybersecurity research: A scientometric analysis of Indian publications. Journal of Computer Information Systems, 63(2), 293-309.

[3] Espino, Y. M., & Pérez, L. R. V. (2022). Análisis bibliométrico de la producción científica sobre México en temas de ciberseguridad (2015-2020). CIENCIA ergo-sum, 29(3).

[4] Di Franco, F. (2018). Analysis of the European R & D Priorities in Cybersecurity: Strategic Priorities in Cybersecurity for a Safer Europe. ENISA. 2018. `https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity`

[5] ENISA. Research and Innovation Brief - Annual Report on Cybersecurity Research and Innovation Needs and Priorities. ENISA. 2022. `https://www.enisa.europa.eu/publications/research-and-innovation-brief`

[6] Fortunato, S. "Community detection in graphs," Phys. Rep., vol. 486, nos. 3–5, pp. 75–174, Feb. 2010.

[7] Camacho, P., Hevia, A., Kiwi, M., & Opazo, R. (2012). Strong accumulators from collision-resistant hashing. *International Journal of Information Security, 11*(5), 349-363.

[8] Xavier, G. B., Temporão, G. P., & Von Der Weid, J. P. (2012). Employing long fibre-optical Mach-Zehnder interferometers for quantum cryptography with orthogonal states. *Electronics Letters, 48*(13), 775-777.

[9] Camacho, P., & Hevia, A. (2012). Short transitive signatures for directed trees. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7178 LNCS*, 35-50.

[10] Abarzúa, R., & Thériault, N. (2012). Complete atomic blocks for elliptic curves in Jacobian coordinates over prime fields. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7533 LNCS*, 37-55.

[11] Vielhaber, M. (2012). Reduce-by-feedback: Timing resistant and DPA-aware modular multiplication plus: How to break RSA by DPA. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7428 LNCS*, 463-475.

[12] Vielhaber, M., & Del Pilar Canales Chacón, M. (2012). The linear complexity deviation of multisequences: Formulae for finite lengths and asymptotic distributions. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7280 LNCS*, 168-180.

[13] Vásquez, D., Cerpa, N., & Angles, R. (2013). A secure discussion system with anonymous participation through web services; [Un sistema de discusión seguro con participación anónima a través de servicios web]. *Ingeniare, 21*(1), 82-98.

[14] Noura, H., Martin, S., Al Agha, K., & Grote, W. (2013). Key dependent cipher scheme for sensor networks. In *12th Annual Mediterranean Ad Hoc Networking Workshop, MED-HOC-NET 2013*, 148-154.

[15] Caragata, D., & Tutanescu, I. (2014). On the security of a new image encryption scheme based on a chaotic function. *Signal, Image and Video Processing, 8*(4), 641-646.

[16] Xavier, G. B. (2014). Applications of optical and electronic instrumentation on secure long-distance quantum communications in optical fibers. In *Latin America Optics and Photonics Conference, LAOP 2014*.

[17] Huerta-Canepa, G. (2015). An encryption scheme based on trust for device-to-device communication on 5G. In *International Conference on ICT Convergence 2015: Innovations Toward the IoT, 5G, and Smart Media Era, ICTC 2015*, 360-362.

[18] Alvarez, L. C., Palacios, R. F., & Caiconte, P. C. (2015). Development of a simulator for the quantum cryptography protocol E91 in a distributed environment; [Desarrollo de un simulador para el protocolo de criptografía cuántica E91 en un ambiente distribuido]. *Ingeniare, 23*(2), 245-258.

[19] Bravo, L., & Segovia, R. (2012). Simplified access control policies for XML databases. In *CEUR Workshop Proceedings, 866*, 20-34.

[20] Uzunov, A. V., & Fernandez, E. B. (2014). An extensible pattern-based library and taxonomy of security threats for distributed systems. *Computer Standards and Interfaces, 36*(4), 734-747.

[21] Liu, S., Fukuda, H., & Leger, P. (2023). Real-time DDoS Attack Defense System in SDN Using LSSOM. In *Proceedings of the 26th Conference on Innovation in Clouds, Internet and Networks, ICIN 2023*, 69-73.

[22] Banks, K. B., Blackstone, J. M., Perry, S. S., Patterson, W., Des Valle, P. G., Mujica, S., Aedo, C. M., Morales Sanchez, A., Muñoz Andrade, J. P., & Rocha Stuardo, J. A. (2012). DDoS and

other anomalous web traffic behavior in selected countries. In *Conference Proceedings - IEEE SOUTHEASTCON*.

[23] Pinacho, P., Pau, I., Chacón, M., & Sánchez, S. (2012). An ecological approach to anomaly detection: The EIA model. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7597 LNCS*, 232-245.

[24] Reyes-Lopez, J., Campos, S., Allende, H., & Salas, R. (2012). Zernike's feature descriptors for iris recognition with SVM. In *Proceedings - International Conference of the Chilean Computer Science Society, SCCC*, 283-288.

[25] Toledo, R., Núñez, A., Tanter, E., & Noyé, J. (2012). Aspectizing Java access control. *IEEE Transactions on Software Engineering, 38*(1), 101-117.

[26] Brown, M., An, B., Kiekintveld, C., Ordóñez, F., & Tambe, M. (2012). Multi-objective optimization for security games. In *11th International Conference on Autonomous Agents and Multiagent Systems 2012, AAMAS 2012: Innovative Applications Track*, 600-607.

[27] Ríos, S. A., & Muñoz, R. (2012). Dark web portal overlapping community detection based on topic models. In *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*.

[28] Piggott, P., Carter, C., Patterson, W., Gutierrez, F., Mujica, S., Rojas, E., & Valenzuela, C. (2013). Development of an indicator to distinguish DDoS attacks from other anomalous events. In *Conference Proceedings - IEEE SOUTHEASTCON*.

[29] Vasquez, S., & Simmonds, J. (2013). Mobile Application Monitoring. In *Proceedings - International Conference of the Chilean Computer Science Society, SCCC*, 30-32.

[30] Toledo, R., & Tanter, É. (2013). Secure and modular access control with aspects. In *AOSD 2013 - Proceedings of the 2013 ACM on Aspect-Oriented Software Development*, 157-169.

[31] Pavlich-Mariscal, J. A., Franky, M. C., & Lopez, A. (2013). Towards security assurance in round-trip engineering: A type-based approach. *Electronic Notes in Theoretical Computer Science, 292*, 83-94.

[32] Bravo, L., Cheney, J., Fundulaki, I., & Segovia, R. (2012). Consistency and repair for XML write-access control policies. *VLDB Journal, 21*(6), 843-867.

[33] Bustos-Jiménez, J. (2014). Do we really need an online informed consent? Discussion from a technocratic point of view. In *UbiComp 2014 - Adjunct Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 629-634.

[34] Hochbaum, D. S., Lyu, C., & Ordóñez, F. (2014). Security routing games with multivehicle Chinese postman problem. *Networks, 64*(3), 181-191.

[35] Caragata, D., El Assad, S., Shoniregun, C., & Akmayeva, G. (2014). Confidential initial identification and other improvements for UMTS security. *Security and Communication Networks, 7*(3), 558-566.

[36] Fernandez, E. B., & Monge, R. (2014). A Security Reference Architecture for cloud systems. In *ACM International Conference Proceeding Series*, 3.

[37] Márquez, G., Rodríguez, A., & Medina, E. F. (2014). Obtaining secure BPEL from secure business process specified with BPMN. *IEEE Latin America Transactions, 12*(2), 315-320.

[38] Pedraza-Garcia, G., Astudillo, H., & Correal, D. (2014). A methodological approach to apply security tactics in software architecture design. In *2014 IEEE Colombian Conference on Communications and Computing, COLCOM 2014 - Conference Proceedings*, 6860432.

[39] Noël, R., Pedraza-García, G., Astudillo, H., & Fernández, E. B. (2014). An exploratory comparison of security patterns and tactics to harden systems. In *CIBSE 2014: Proceedings of the 17th Ibero-American Conference Software Engineering*, 378-391.

[40] Oscar, E. C., Fernandez, E. B., & Raúl, M. A. (2014). Threat analysis and misuse patterns of federated Inter-Cloud systems. In *ACM International Conference Proceeding Series, 09-13-July-2014*, 2721986.

[41] Fernández, E. B., Raúl, M. A., Carvajal, R., Encina, O., Hernández, J., & Silva, P. (2014). Patterns for content-dependent and context-enhanced authorization. In *ACM International Conference Proceeding Series, 09-13-July-2014*, 2721974.

[42] Ni, Z., Li, Q. M., Liu, X. Q., Li, T., & Hou, R. (2015). Mining Frequent patterns through microaggregation in differential privacy. *Journal of Digital Information Management, 13*(2), 126-131.

[43] Blum, C., Lozano, J. A., & Davidson, P. P. (2015). An artificial bioindicator system for network intrusion detection. *Artificial Life, 21*(2), 93-118.

[44] Wen, H., Tang, J., Wu, J., Song, H., Wu, T., Wu, B., Ho, P.-H., Lv, S.-C., & Sun, L.-M. (2015). A cross-layer secure communication model based on discrete fractional Fourier transform (DFRFT). *IEEE Transactions on Emerging Topics in Computing, 3*(1), 119-126.

[45] Xie, Y., Wen, H., Wu, J., Jiang, Y., Meng, J., Guo, X., Xu, A., & Guan, Z. (2015). Three-layers secure access control for cloud-based smart grids. In *IEEE Vehicular Technology Conference*, VOL, 7391174.

[46] Sepulveda, C., Alarcon, R., & Bellido, J. (2015). QoS aware descriptions for RESTful service composition: security domain. *World Wide Web, 18*(4), 767-794.

[47] Fernandez, E. B., Astudillo, H., & Pedraza-García, G. (2015). Revisiting architectural tactics for security. In *IFIP Advances in Information and Communication Technology, 9278*, 55-69.

[48] Elmisery, A. M., Rho, S., & Botvich, D. (2016). A fog based middleware for automated compliance with OECD privacy principles in the Internet of Healthcare Things. *IEEE Access, 4*, 7805329, 8418-8441.

[49] Fernandez, E. B., Monge, R., & Hashizume, K. (2016). Building a security reference architecture for cloud systems. *Requirements Engineering, 21*(2), 225-249.

[50] Lin, A. W., & Barceló, P. (2016). String solving with word equations and transducers: Towards a logic for analyzing mutation XSS. In *Conference Record of the Annual ACM Symposium on Principles of Programming Languages, 20-22-January-2016*, 123-136.

[51] Huang, H., Guo, S., Wu, J., & Li, J. (2016). Joint middlebox selection and routing for software-defined networking. In *2016 IEEE International Conference on Communications, ICC 2016*, 7510816.

[52] González, A., & Ráfols, C. (2016). New techniques for non-interactive shuffle and range arguments. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9696*, 427-444.

[53] Barría, C., Cordero, D., Cubillos, C., & Osses, R. (2016). Obfuscation procedure based on dead code insertion into crypter. In *2016 6th International Conference on Computers Communications and Control, ICCCC 2016*, 7496733, 23-29.

[54] Barría, C., Cordero, D., Cubillos, C., & Palma, M. (2016). Proposed classification of malware, based on obfuscation. In *2016 6th International Conference on Computers Communications and Control, ICCCC 2016*, 7496735, 37-44.

[55] Caragata, D., Mucarquer, J. A., Koscina, M., & El Assad, S. (2016). Cryptanalysis of an improved fragile watermarking scheme. *AEU - International Journal of Electronics and Communications, 70*(6), 777-785.

[56] Márquez, G., Silva, P., Noel, R., Matalonga, S., & Astudillo, H. (2016). Identifying emerging security concepts using software artifacts through an experimental case. In *Proceedings - International Conference of the Chilean Computer Science Society, SCCC 2016-February*, 7416581.

[57] Bustos-Jimenez, J., Saint-Pierre, C., & Graves, A. (2016). Applying Process Mining Techniques to DNS Traces Analysis. In *Proceedings - International Conference of the Chilean Computer Science Society, SCCC 2016-September*, 7559664, 12-16.

[58] Silva, P., Noël, R., Matalonga, S., Astudillo, H., Gatica, D., & Marquez, G. (2016). Software development initiatives to identify and mitigate security threats-two systematic mapping studies. CLEI Electronic Journal, 19(3), 5-1.

[59] Blasco, S., Bustos-Jimenez, J., Font, G., Hevia, A., & Grazia Prato, M. (2016). A three-layer approach for protecting smart-citizens privacy in crowdsensing projects. In *Proceedings - International Conference of the Chilean Computer Science Society, SCCC 2016-February*, 7416585.

[60] Font, G., Bustos, J., & Hevia, A. (2016). Location Privacy for a Monitoring System of the Quality of Access to Mobile Internet. *IEEE Latin America Transactions, 14*(6), 2894-2896, 7555272.

[61] Garay, F., Rosas, E., & Hidalgo, N. (2016). Reliable routing protocol for delay tolerant networks. In *Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS 2016-January*, 7384311, 320-327.

[62] Macias, M., Barria, C., Acuna, A., & Cubillos, C. (2016). SGSI support throught malware's classification using a pattern analysis. In *2016 IEEE International Conference on Automatica, ICA-ACCA 2016*, 7778516.

[63] Pujolàs, J., Riquelme, E., & Thériault, N. (2016). Trisection for non-supersingular genus 2 curves in characteristic 2. *International Journal of Computer Mathematics, 93*(8), 1254-1264.

[64] Gonzales, A. C. (2016). Multibase scalar multiplications in cryptographic pairings. *Applicable Algebra in Engineering, Communications and Computing, 27*(3), 219-236.

[65] Koscina, M., & Caragata, D. (2016). Bench-marking of traditional cryptographic algorithms and chaos-based algorithms with DNA operations. In *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, 7412050, 26-31.

[66] Lazo, C., Mardones, J., & Diaz, R. (2016). Security proposal for AMI network on an industrial wireless sensor network. In *CHILECON 2015 - 2015 IEEE Chilean Conference on Electrical, Electronics Engineering, Information and Communication Technologies, Proceedings of IEEE Chilecon 2015*, 7400398, 333-338.

[67] Holloway, B., Cespedes, S., & Hevia, A. (2016). Analysis of attacks to automated vehicular coordination systems at intersections. In *CEUR Workshop Proceedings, 1727*, 38-40.

[68] Barragan, C. C., Huidobro, C. B., & Esquivel, M. P. (2016). Malware on mobile devices odds of infection based on running operating system version. In *Proceedings - International Conference of the Chilean Computer Science Society, SCCC 2016-February*, 7416590.

[69] Chicoisne, R., & Ordóñez, F. (2016). Risk averse Stackelberg security games with quantal response. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9996 LNCS*, 83-100.

[70] Cintas, C., Quinto-Sánchez, M., Acuña, V., Paschetta, C., De Azevedo, S., De Cerqueira, C. C. S., Ramallo, V., Gallo, C., Poletti, G., Canizales-Quinteros, S., Rothhammer, F., Bedoya, G., Ruiz-Linares, A., González-José, R., Delrieux, C. (2017). Automatic ear detection and feature extraction using Geometric Morphometrics and convolutional neural networks. *IET Biometrics, 6*(3), 211-223.

[71] Pérez-Guzmán, R. E., Salgueiro-Sicilia, Y., & Rivera, M. (2017). Communication systems and security issues in smart microgrids. In *Proceedings - 2017 IEEE Southern Power Electronics Conference, SPEC 2017, 2018-January*, 1-6.

[72] Miranda, M., & Mundarain, D. (2017). Two-way QKD with single-photon-added coherent states. *Quantum Information Processing, 16*(12), 298.

[73] Figueroa, N., L'Huillier, G., & Weber, R. (2017). Adversarial classification using signaling games with an application to phishing detection. *Data Mining and Knowledge Discovery, 31*(1), 92-133.

[74] Elmisery, A. M., & Sertovic, M. (2017). Privacy enhanced cloud-based recommendation service for implicit discovery of relevant support groups in healthcare social networks. *International Journal of Grid and High Performance Computing, 9*(1), 75-91.

[75] Silva, N. M. O., & Cordero, C. V. (2017). Towards physical layer security systems design using game theory approaches. In *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies, CHILECON 2017 - Proceedings, 2017-January*, 1-6.

[76] Cruz, R., Rezk, T., Serpette, B., & Tanter, É. (2017). Type abstraction for relaxed noninterference. In *Leibniz International Proceedings in Informatics, LIPIcs 74*, 71-727.

[77] Abdelsalam, A., Caragata, D., Luglio, M., Roseti, C., & Zampognaro, F. (2017). Robust security framework for DVB-RCS satellite networks (RSSN). *International Journal of Satellite Communications and Networking, 35*(1), 17-43.

[78] Xiang, M., Liu, W., Bai, Q., Al-Anbuky, A., Wu, J., & Sathiaseelan, A. (2017). NTaaS: Network trustworthiness as a service. In *2017 27th International Telecommunication Networks and Applications Conference, ITNAC 2017, 2017-January*, 1-6.

[79] Bahamondes, B., Correa, J., Matuschke, J., & Oriolo, G. (2017). Adaptivity in Network Interdiction. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10575 LNCS*, 40-52.

[80] Barría, C., Cordero, D., Cubillos, C., Palma, M., & Cabrera, D. (2017). Obfuscation-based malware update: A comparison of manual and automated methods. *International Journal of Computers, Communications and Control, 12*(4), 461-474.

[81] Muñoz, C., Montoto, F., Bustos-Jiménez, J., & Cifuentes, F. (2017). Building a threshold cryptographic distributed HSM with docker containers. In *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies, CHILECON 2017 - Proceedings, 2017-January*, 1-5.

[82] Osses, F., Márquez, G., Orellana, C., & Astudillo, H. (2017). Towards the selection of security tactics based on non-functional requirements: Security tactic planning poker. In *Proceedings - International Conference of the Chilean Computer Science Society, SCCC 2017-October*, 1-8.

[83] Noël, R., Matalonga, S., Pedraza, G., Astudillo, H., & Fernandez, E.B. (2017). Generating software security knowledge through empirical methods. In *Empirical Research for Software Security: Foundations and Experience*, 95-137.

[84] Ravanales, W.F., & Herman, K. (2017). Union of code and encryption for channels with class a noise. In *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies, CHILECON 2017 - Proceedings*, 1-5.

[85] Araya, A., Jiron, I., & Soto, I. (2017). A new key exchange algorithm over a VLC indoor channel. In *2017 1st South American Colloquium on Visible Light Communications, SACVLC 2017*, 1-5.

[86] Dieguez, M., Cares, C., & Cachero, C. (2017). Methodology for the information security controls selection. In *Iberian Conference on Information Systems and Technologies, CISTI*.

[87] González, A., & Hevia, A. (2018). A second note on the feasibility of generalized universal composability. *Mathematical Structures in Computer Science, 28*(2), 141-154.

[88] Abarzúa, R., Martínez, S., Mendoza, V., & Valera, J. (2018). Avoiding Side-Channel Attacks by Computing Isogenous and Isomorphic Elliptic Curves. *Mathematics in Computer Science, 12*(3), 295-307.

[89] Barra, M.Z., Rodríguez, A., Caro, A., & Fernández, E.B. (2018). Towards obtaining UML class diagrams from secure business processes using security patterns. *Journal of Universal Computer Science, 24*(10), 1472-1492.

[90] Zhou, B., Li, J., Wu, J., Guo, S., Gu, Y., & Li, Z. (2018). Machine-learning-based online distributed denial-of-service attack detection using spark streaming. In *IEEE International Conference on Communications 2018-May*.

[91] Wu, D., Li, J., Das, S.K., Wu, J., Ji, Y., & Li, Z. (2018). A novel distributed denial-of-service attack detection scheme for software defined networking environments. In *IEEE International Conference on Communications 2018-May*.

[92] Ortega Silva, N.M., & Valencia Cordero, C. (2018). Secrecy capacity bounds analysis for physical layer security based on game theory. *IEEE Latin America Transactions, 16*(9), 2385-2391.

[93] Huidobro, C.B., Cordero, D., Cubillos, C., Cid, H.A., & Bárragan, C.C. (2018). Obfuscation procedure based on the insertion of the dead code in the crypter by binary search. In *2018 7th International Conference on Computers Communications and Control, ICCCC 2018 - Proceedings*, 183-192.

[94] Molina-Martínez, C., Galdames, P., & Duran-Faundez, C. (2018). A distance bounding protocol for location-cloaked applications. *Sensors (Switzerland), 18*(5), 1337.

[95] Barragán, C.C., Esquivel, M.P., Huidobre, C.B., Rusu, C., Collazo, C., & Burbano, C. (2018). Usability in computer security software. In *Advances in Intelligent Systems and Computing, 558*, 895-898.

[96] Velásquez, I., Caro, A., & Rodríguez, A. (2018). Kontun: A Framework for recommendation of authentication schemes and methods. *Information and Software Technology, 96*, 27-37.

[97] Aros, M., & Torres, R. (2018). Implementing a signing forms mechanism in an open XMPP Server to reduce successful network attacks. In *CEUR Workshop Proceedings, 2178*, 79-82.

[98] Villanueva, A.A., Araya, I.J., & Gomez, I.S. (2018). Diffie-hellman protocol with a combination of hyperelliptic curves and neural synchronization. In *Ingeniare, 26*, 6-11.

[99] Barría, C., Galeazzi, L., Acuña, A., & Casado, C. (2018). Security evaluation in wireless networks. In *Communications in Computer and Information Science, 944*, 13-23.

[100] Oliveira, G., Fernandez, E., Mafra, S., & Montejo-Sanchez, S. (2018). Physical Layer Security in Cognitive Radio Networks Using Improper Gaussian Signaling. *IEEE Communications Letters, 22*(9), 1886-1889.

[101] Chen, S., Wen, H., Wu, J., Chen, J., Liu, W., Hu, L., & Chen, Y. (2018). Physical-Layer Channel Authentication for 5G via Machine Learning Algorithm. *Wireless Communications and Mobile Computing, 2018*, 6039878.

[102] Toro, Matías; Garcia, Ronald; Tanter, Éric (2018). Type-driven gradual security with references. *ACM Transactions on Programming Languages and Systems, 40*(4), 16.

[103] Osses, Felipe; Márquez, Gastón; Villegas, Mónica M.; Orellana, Cristian; Visconti, Marcello; Astudillo, Hernán (2018). Security tactics selection poker (TaSPeR): A card game to select security tactics to satisfy security requirements. *ACM International Conference Proceeding Series*, a54.

[104] Cruz, R., & Tanter, É. (2019). Existential types for relaxed noninterference. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11893 LNCS*, 73-92.

[105] Cruz, Raimil; Tanter, Eric (2019). Polymorphic relaxed noninterference. *Proceedings - 2019 IEEE Secure Development, SecDev 2019*, 8901642, 101-113.

[106] Liao, R.-F., Wen, H., Wu, J., Pan, F., Xu, A., Jiang, Y., Xie, F., & Cao, M. (2019). Deep-learning-based physical layer authentication for industrial wireless sensor networks. *Sensors (Switzerland), 19*(11), 2440.

[107] Liao, R.-F., Wen, H., Wu, J., Pan, F., Xu, A., Song, H., Xie, F., Jiang, Y., & Cao, M. (2019). Security enhancement for mobile edge computing through physical layer authentication. *IEEE Access, 7*, 2934122, 116390-116401.

[108] Kaschel, H., & Ahumada, C. (2019). Security Mechanism to Protect the Privacy and Security of Patients Who have cardiovascular Diseases (ECG). In *IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies, CHILECON 2019*, 8987984.

[109] Mosso, Edward; Suárez, Omar; Bolognini, Néstor (2019). Asymmetric multiple-image encryption system based on a chirp z-transform. *Applied Optics, 58*(21), 5674-5680.

[110] Márquez, Gastón; Astudillo, Hernán (2019). Identifying availability tactics to support security architectural design of microservice-based systems. *ACM International Conference Proceeding Series, 2*, 123-131.

[111] Vale, Anelis Pereira; Fernandez, Eduardo B. (2019). An Ontology for Security Patterns. *Proceedings - International Conference of the Chilean Computer Science Society, SCCC 2019-November*, 8966393.

[112] Pavesi, Jaime; Villegas, Thamara; Perepechko, Alexey; Aguirre, Eleazar; Galeazzi, Lorena (2019). Validation of ICS Vulnerability Related to TCP/IP Protocol Implementation in Allen-Bradley Compact Logix PLC Controller. *Communications in Computer and Information Science, 1053 CCIS*, 355-364.

[113] Maldonado, Javier; Riff, Maria-Cristina; Montero, Elizabeth (2019). Improving Attack Detection of C4.5 using an Evolutionary Algorithm. *2019 IEEE Congress on Evolutionary Computation, CEC 2019 - Proceedings*, 8790199, 2229-2235.

[114] Orellana, Cristian; Villegas, Mónica M.; Astudillo, Hernán (2019). Mitigating security threats through the use of security tactics to design secure cyber-physical systems (CPS). *ACM International Conference Proceeding Series, 2*, 109-115.

[115] Galeazzi Avalos, Lorena; Barría Huidobro, Cristian; Villegas Berbesi, Thamara (2019). Identifying Components Belonging to Wireless Connectivity Security. *Communications in Computer and Information Science, 1053 CCIS*, 365-373.

[116] Dumas, Jean-Guillaume; Lafourcade, Pascal; Lopez Fenner, Julio; Lucas, David; Orfila, Jean-Baptiste; Pernet, Clément; Puys, Maxime (2019). Secure multiparty matrix multiplication based on Strassen-Winograd algorithm. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11689 LNCS*, 67-88.

[117] Lopez, Nicolas; Azurdia-Meza, Cesar; Valencia, Claudio; Montejo-Sanche, Samuel (2019). On the performance of 6LoWPAN using TSCH/Orchestra mode against a jamming attack. *IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies, CHILECON 2019*, 8988035.

[118] Li, Zheng; Pino, Esteban J. (2019). DD: A distributed and disposable approach to privacy preserving data analytics in user-centric healthcare. *Proceedings - 2019 IEEE 12th Conference on Service-Oriented Computing and Applications, SOCA 2019*, 8953033, 176-183.

[119] Li, P., Prieto, L., Mery, D., & Flynn, P.J. (2019). On Low-Resolution Face Recognition in the Wild: Comparisons and New Techniques. *IEEE Transactions on Information Forensics and Security, 14*(8), 2000-2012.

[120] Arancibia, Jaime Diaz; Smith, Vicente Ferrari; Fenner, Julio Lopez (2019). On-The-Fly Diffie-Hellman for IoT. *Proceedings - International Conference of the Chilean Computer Science Society, SCCC 2019-November*, 8966440.

[121] Goubin, Louis; Monsalve, Geraldine; Reutter, Juan; Vial-Prado, Francisco (2019). Excalibur key-generation protocols for dag hierarchic decryption. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11396 LNCS*, 103-120.

[122] Muñoz, Diego; Cordero, David; Barría Huidobro, Cristian (2019). Methodology for Malware Scripting Analysis in Controlled Environments Based on Open Source Tools. *Communications in Computer and Information Science, 1053 CCIS*, 345-354.

[123] Nieves Arreaza, Gustavo Jose (2019). Methodology for Developing Secure Apps in the Clouds. (MDSAC) for IEEECS Confererences. *Proceedings - 6th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2019 and 5th IEEE International Conference on Edge Computing and Scalable Cloud, EdgeCom 2019*, 8854038, 102-106.

[124] Elmisery, Ahmed M.; Rho, Seungmin; Aborizka, Mohamed (2019). A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services. *Cluster Computing, 22*, 1611-1638.

[125] Benalcazar, Daniel P.; Zambrano, Jorge E.; Bastias, Diego; Perez, Claudio A.; Bowyer, Kevin W. (2020). A 3D Iris Scanner from a Single Image Using Convolutional Neural Networks. *IEEE Access, 8*, 9097841, 98584-98599.

[126] Xie, Feiyi; Wen, Hong; Wu, Jinsong; Chen, Songlin; Hou, Wenjing; Jiang, Yixin (2020). Convolution Based Feature Extraction for Edge Computing Access Authentication. *IEEE Transactions on Network Science and Engineering, 7*(4), 8919989, 2336-2346.

[127] Xie, Feiyi; Wen, Hong; Wu, Jinsong; Hou, Wenjing; Song, Huanhuan; Zhang, Tengyue; Liao, Runfa; Jiang, Yixin (2020). Data Augmentation for Radio Frequency Fingerprinting via Pseudo-Random Integration. *IEEE Transactions on Emerging Topics in Computational Intelligence, 4*(3), 8887221, 276-286.

[128] Manzano, Carlos; Meneses, Claudio; Leger, Paul (2020). An Empirical Comparison of Supervised Algorithms for Ransomware Identification on Network Traffic. *Proceedings - International Conference of the Chilean Computer Science Society, SCCC 2020-November*, 9281283.

[129] Perez, Juan; Torres, Romina; Von Brand, Sven (2020). CyberKids: Video game for raising cybersecurity awareness in children. *Proceedings - International Conference of the Chilean Computer Science Society, SCCC 2020-November*, 9281253.

[130] Gallardo, Juan; Torres, Romina; Tessini, Oliver (2020). Surveillance Platform of cybersecurity maturity of micro and small enterprises. *Proceedings - International Conference of the Chilean Computer Science Society, SCCC 2020-November*, 9281264.

[131] Ávalos, Lorena Galeazzi; Huidobro, Cristian Barría; Hurtado, Julio Ariel A review of the security information controls in wireless networks wi-fi. *Communications in Computer and Information Science*, 1280, 420-427, 2020.

[132] Lipán Mella, Juan R.; Méndez, Yenny A.A. (2020). Identifying usability activities integrated into the planning phase of the secure software development cycle through a systematic review. *CEUR Workshop Proceedings, 2747*, 215-223.

[133] Muñoz-Vergara, Leonel; Rodríguez, Alfonso; Caro, Angélica (2020). Representation of security requirements in BPMN: A systematic review of the literature. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, 2020, E28*, 286-298.

[134] Soto, Ricardo; Crawford, Broderick; Molina, Francisco Gonzalez; Olivares, Rodrigo (2021). Human Behaviour Based Optimization Supported with Self-Organizing Maps for Solving the S-Box Design Problem. *IEEE Access, 2021, 9*, 9448057, 84605-84618.

[135] López-Vilos, Nicolás; Valencia-Cordero, Claudio; Azurdia-Meza, Cesar; Montejo-Sánchez, Samuel; Mafra, Samuel Baraldi (2021). Performance analysis of the IEEE 802.15.4 protocol for smart environments under jamming attacks. *Sensors, 2021, 21(12)*, 4079.

[136] Kaschel, Hector; Diaz, Alvaro (2021). High security ubiquitous H-IoT on a WBAN-based EHR using blockchain. *2021 IEEE International Conference on Automation/24th Congress of the Chilean Association of Automatic Control, ICA-ACCA 2021*.

[137] Paez, Felipe; Kaschel, Hector (2021). Towards a robust computer security layer for the LIN bus. *2021 IEEE International Conference on Automation/24th Congress of the Chilean Association of Automatic Control, ICA-ACCA 2021*.

[138] Azocar, Jose; Soto, Ismael; Corral, Fabian (2021). A Quantum Key distribution using Optical Frequency Comb Source. *SACVLC 2021 - Proceedings: 2021 3rd South American Colloquium on Visible Light Communications*.

[139] Corral-Molina, Carlos; Valencia-Cordero, Claudio (2021). BER and SNR based physical layer security analysis with cooperative Jamming. *2021 IEEE International Conference on Automation/24th Congress of the Chilean Association of Automatic Control, ICA-ACCA 2021*.

[140] Barria, Cristian; Cordero, David; Galeazzi, Lorena; Acuña, Alejandra (2021). Proposal of a multi-standard model for measuring maturity business levels with reference to information security standards and controls. *Advances in Intelligent Systems and Computing, 2021, 1243 AISC*, 121-132.

[141] Ponce, Francisco (2021). Towards Resolving Security Smells in Microservice-Based Applications. *Communications in Computer and Information Science, 2021, 1360*, 133-139.

[142] Martinez, Vicente; Salas, Rodrigo; Tessini, Oliver; Torres, Romina (2021). Machine learning techniques for behavioral feature selection in network intrusion detection systems. *IET Conference Proceedings, 2021, 1*, 109-114.

[143] Espinosa, Diego Muñoz; Vidal, David Cordero; Huidobro, Cristian Barría (2021). Methodological Proposal for Privilege Escalation in Windows Systems. *Communications in Computer and Information Science, 2021, 1430 CCIS*, 138-150.

[144] Paez, Felipe; Kaschel, Hector (2021). A Proposal for Data Authentication, Data Integrity and Replay Attack Rejection for the LIN Bus. *2021 IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies, CHILECON 2021*.

[145] Orellana, Cristian; Astudillo, Hernán; Fernandez, Eduardo B. (2021). A Pattern for a Secure Actuator Node. *ACM International Conference Proceeding Series, 2021*, 29.

[146] Fernandez, Eduardo B.; Astudillo, Hernan; Orellana, Cristian (2021). A pattern for a Secure IoT Thing. *ACM International Conference Proceeding Series, 2021*, 16.

[147] Villegas, Felipe Ignacio Leon; Cordero, Claudio Valencia (2021). Machine Learning Analysis for Side-Channel Attacks over Elliptic Curve Cryptography. *2021 IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies, CHILECON 2021*.

[148] Kaschel, Hector; Rojas, Ricardo (2021). Security, energy efficiency, routing protocols and algorithms applied to underwater wireless sensor network. *2021 IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies, CHILECON 2021*.

[149] Hevia, Alejandro; Mergudich-Thal, Ilana (2021). Implementing Secure Reporting of Sexual Misconduct - Revisiting WhoToo. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2021, 12912 LNCS*, 341-362.

[150] Torres, Romina; González, Nicolás; Cabrera, Mathías; Salas, Rodrigo (2021). Taxonomies using the clique percolation method for building a threats observatory. *Proceedings - 2021 47th Latin American Computing Conference, CLEI 2021*.

[151] Ma, Bo; Yan, Wei Qi; Lai, Edmund; Wu, Jingsong (2021). A New Noise Generating Method Based on Gaussian Sampling for Privacy Preservation. *Communications in Computer and Information Science, 2021, 1386 CCIS*, 1-12.

[152] Ruminot-Ahumada, Nicolas; Valencia-Cordero, Claudio; Abarzua-Ortiz, Rodrigo (2021). Side channel attack countermeasure for low power devices with AES encryption. *2021 IEEE International Conference on Automation/24th Congress of the Chilean Association of Automatic Control, ICA-ACCA 2021*.

[153] Oliveira, Pedro M.; Pessim, Paulo S. P.; Palma, Jonathan M.; Lacerda, Marcio J. (2021). Reference tracking control for cyber-physical systems under DoS attacks. *2021 IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies, CHILECON 2021*.

[154] Madariaga, Diego; Madariaga, Javier; Panza, Martín; Bustos-Jiménez, Javier; Bustos, Benjamin (2021). Detecting Anomalies at a TLD Name Server Based on DNS Traffic Predictions. *IEEE Transactions on Network and Service Management, 2021, 18(1)*, 9320589, 1016-1030.

[155] Habibi, Mohammad Reza; Sahoo, Subham; Rivera, Sebastian; Dragicevic, Tomislav; Blaabjerg, Frede (2021). Decentralized Coordinated Cyberattack Detection and Mitigation Strategy in DC Microgrids Based on Artificial Neural Networks. *IEEE Journal of Emerging and Selected Topics in Power Electronics, 2021, 9(4)*, 9319658, 4629-4638.

[156] Burgos-Mellado, Claudio; Donoso, Felipe; Dragicevic, Tomislav; Cardenas-Dobson, Roberto; Wheeler, Patrick; Clare, Jon; Watson, Alan (2022). Cyber-Attacks in Modular Multilevel Converters. *IEEE Transactions on Power Electronics, 2022, 37(7)*, 8488-8501.

[157] Manzano, C.; Meneses, C.; Leger, P.; Fukuda, H. (2022). An Empirical Evaluation of Supervised Learning Methods for Network Malware Identification Based on Feature Selection. *Complexity, 2022*.

[158] Gonzalez, Francisco; Soto, Ricardo; Crawford, Broderick (2022). Stochastic Fractal Search Algorithm Improved with Opposition-Based Learning for Solving the Substitution Box Design Problem. *Mathematics, 2022, 10(13)*, 2172.

[159] Okey, Ogobuchi Daniel; Maidin, Siti Sarah; Adasme, Pablo; Lopes Rosa, Renata; Saadi, Muhammad; Carrillo Melgarejo, Dick; Zegarra Rodríguez, Demóstenes (2022). BoostedEnML: Efficient Technique for Detecting Cyberattacks in IoT Systems Using Boosted Ensemble Machine Learning. *Sensors, 2022, 22(19)*, 7409.

[160] Rodríguez, Felipe; Ochoa, Sergio F.; Gutierrez, Francisco J. (2022). Supporting asymmetric interaction in the age of social media. *Journal of Ambient Intelligence and Humanized Computing, 2022, 13(11)*, 5391-5404.

[161] Mery, Domingo; Morris, Bernardita (2022). On Black-Box Explanation for Face Verification. *Proceedings - 2022 IEEE/CVF Winter Conference on Applications of Computer Vision, WACV 2022*, 1194-1203.

[162] Zambrano, Jorge E.; Benalcazar, Daniel P.; Perez, Claudio A.; Bowyer, Kevin W. (2022). Iris Recognition Using Low-Level CNN Layers Without Training and Single Matching. *IEEE Access, 2022, 10*, 41276-41286.

[163] Ponce, Francisco; Soldani, Jacopo; Astudillo, Hernán; Brogi, Antonio (2022). Should Microservice Security Smells Stay or be Refactored? Towards a Trade-off Analysis. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2022, 13444 LNCS*, 131-139.

[164] Waher, Peter; Araoz, Kristjan; Pablo Pulgar, R.; Mostrom, Daniel (2022). Tokenization of sustainable real estate in Smart Cities: Monetization as basis for construction, authorization and carbon neutralization in CPS. *IECON Proceedings (Industrial Electronics Conference), 2022-October*.

[165] Burgos-Mellado, Claudio; Donoso, Felipe; Dragicevic, Tomislav (2022). AC Battery: Modular Layout and Cyber-secure Cell-level Control for Cost-Effective Transportation Electrification. *2022 IEEE Transportation Electrification Conference and Expo, ITEC 2022*, 1163-1167.

[166] Aravena, Lucas Torrealba; Bustos-Jiménez, Javier; Casas, Pedro (2022). PHISHWEB – a Progressive, Multi-Layered System for Phishing Websites Detection. *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, 764-765.

[167] Waseem, Muhammad; Liang, Peng; Ahmad, Aakash; Shahin, Mojtaba; Khan, Arif Ali; Márquez, Gastón (2022). Decision Models for Selecting Patterns and Strategies in Microservices Systems and their Evaluation by Practitioners. *Proceedings - International Conference on Software Engineering*, 135-144.

[168] Villalobos, Esteban; Mery, Domingo; Bowyer, Kevin (2022). Fair Face Verification by Using Non-Sensitive Soft-Biometric Attributes. *IEEE Access, 2022, 10*, 30168-30179.

[169] González, Sebastián; Tapia, Juan (2022). Towards Refining ID Cards Presentation Attack Detection Systems using Face Quality Index. *European Signal Processing Conference, 2022-August*, 1027-1031.

[170] Aronesty, Erik; Cash, David; Dodis, Yevgeniy; Gallancy, Daniel H.; Higley, Christopher; Karthikeyan, Harish; Tysor, Oren (2022). Encapsulated Search Index: Public-Key, Sub-linear, Distributed, and Delegatable. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2022, 13178 LNCS*, 256-285.

[171] Zhai, Zhongyi; Lai, Guibing; Cheng, Bo; Qian, Junyan; Zhao, Lingzhong; Wu, Jinsong; Wan, Zhinguo (2022). Lightweight Secure Detection Service for Malicious Attacks in WSN With Timestamp-Based MAC. *IEEE Transactions on Network and Service Management, 2022, 19(4)*, 5299-5311.

[172] Páez, Felipe; Kaschel, Héctor (2022). Design and Testing of a Computer Security Layer for the LIN Bus. *Sensors, 2022, 22(18)*, 6901.

[173] Diaz, Alvaro; Kaschel, Hector (2022). Scalable Management Architecture for Electronic Health Records Based on Blockchain. *2022 IEEE International Conference on Automation/25th*

Congress of the Chilean Association of Automatic Control: For the Development of Sustainable Agricultural Systems, ICA-ACCA 2022.

[174] Lacerda, Marcio J.; Oliveira, Pedro M.; Palma, Jonathan M. (2022). Control design for cyber-physical systems under DoS attacks. *2022 IEEE International Conference on Automation/25th Congress of the Chilean Association of Automatic Control: For the Development of Sustainable Agricultural Systems, ICA-ACCA 2022*.

[175] Saldaña, E. E. Maurin; del Rey, A. Martín; González, A. B. Gil (2022). An Approach to Simulate Malware Propagation in the Internet of Drones. *Communications in Computer and Information Science, 2022, 1659 CCIS*, 364-373.

[176] Jaiba, Julio Olivos (2022). Methodology for the Acquisition and Forensic Analysis of a Remote Piloted Aircraft System (RPAS). *Communications in Computer and Information Science, 2022, 1659 CCIS*, 297-321.

[177] Salazar, Hernaldo; Barría, Cristian (2022). Construction of a Technological Component to Support ISMS for the Detection of Obfuscation in Computer Worm Samples. *Communications in Computer and Information Science, 2022, 1659 CCIS*, 215-224.

[178] Azócar, José; Soto, Ismael; Lara, Sebastián; Gutiérrez, Sebastián; Palacios, Pablo; Azurdia, Cesar (2022). Performance analysis of the QKD algorithm using RS and AES. *2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing, CSNDSP 2022*, 344-349.

[179] Galeazzi, Lorena; Garrido, Camilo; Barría, Cristian (2022). Validation of Security Variables for Audits in Wireless Wi-Fi Networks. *Communications in Computer and Information Science, 2022, 1659 CCIS*, 422-433.

[180] Oliveira, Pedro M.; Palma, Jonathan M.; Lacerda, Márcio J. (2022). H2 state-feedback control for discrete-time cyber-physical uncertain systems under DoS attacks. *Applied Mathematics and Computation, 2022, 425*, 127091.

[181] Tapia, Juan E.; Gonzalez, Sebastian; Busch, Christoph (2022). Iris Liveness Detection Using a Cascade of Dedicated Deep Learning Networks. *IEEE Transactions on Information Forensics and Security, 2022, 17*, 42-52.

[182] Aubin, Verónica; Mora, Marco; Santos, Matilde (2022). A new approach for writer verification based on segments of handwritten graphemes. *Logic Journal of the IGPL, 2022, 30(6)*, 965-978.

[183] Tapia, Juan E.; Valenzuela, Andres; Lara, Rodrigo; Gomez-Barrero, Marta; Busch, Christoph (2022). Selfie Periocular Verification Using an Efficient Super-Resolution Approach. *IEEE Access, 2022, 10*, 67573-67589.

[184] Soria-Lorente, A.; Berres, S.; Díaz-Nuñez, Y.; Avila-Domenech, E. (2022). Hiding data inside images using orthogonal moments. *Journal of Information Security and Applications, 2022, 67*, 103192.

[185] Aravena, L. Torrealba; Casas, P.; Bustos-Jimenez, J.; Capdehourat, G.; Findrik, M. (2023). Phish Me if You Can - Lexicographic Analysis and Machine Learning for Phishing

Websites Detection with PHISHWEB. *2023 IEEE 9th International Conference on Network Softwarization: Boosting Future Networks through Advanced Softwarization, NetSoft 2023 - Proceedings*, 252-256.

[186] Aravena, L. Torrealba; Casas, P.; Bustos-Jimenez, J.; Capdehourat, G.; Findrik, M. (2023). Not all DGAs are Born the Same - Improving Lexicographic based Detection of DGA Domains through AI/ML. *TMA 2023 - Proceedings of the 7th Network Traffic Measurement and Analysis Conference*.

[187] Minchenkova, L.; Minchenkova, A.; Vodynova, V.; Minchenkova, O. (2023). The Use of Cryptocurrencies as a Tool for the Development of Marketing in Tourism. *Smart Innovation, Systems and Technologies, 2023, 337 SIST*, 3-11.

[188] Pasmino, Diego; Aravena, Carlos; Tapia, Juan E.; Busch, Christoph (2023). Flickr-PAD: New Face High-Resolution Presentation Attack Detection Database. *2023 11th International Workshop on Biometrics and Forensics, IWBF 2023*.

[189] Igor Moraga, Leonardo; Malco, Juan Pablo Rivelli; Zabala-Blanco, David; Ahumada-Garcia, Roberto; Azurdia-Meza, Cesar A.; Firoozabadi, Ali Dehghan (2023). Detection of Obfuscated Malware by Engineering Memory Functions Applying ELM. *2023 IEEE Colombian Conference on Applications of Computational Intelligence, ColCACI 2023 - Proceedings*.

[190] Vishnevsky, Andrey; Abbas, Nadezda (2023). Application of Sonification Method in Teaching Information Security. *Lecture Notes in Networks and Systems, 2023, 692 LNNS*, 483-496.

[191] Benalcazar, Daniel; Tapia, Juan E.; Gonzalez, Sebastian; Busch, Christoph (2023). Synthetic ID Card Image Generation for Improving Presentation Attack Detection. *IEEE Transactions on Information Forensics and Security, 2023, 18*, 1814-1824.

[192] Khalid, Haris M.; Qasaymeh, M.M.; Muyeen, S.M.; Moursi, M.S.E.; Foley, A.M.; Sweidan, T.O.; Sanjeevikumar, P. (2023). WAMS Operations in Power Grids: A Track Fusion-Based Mixture Density Estimation-Driven Grid Resilient Approach Toward Cyberattacks. *IEEE Systems Journal, 2023, 17(3)*, 3950-3961.

[193] Lopez, Victor Bucarey; Vecchia, Eugenio Della; Jean-Marie, Alain; Ordonez, Fernando (2023). Stationary Strong Stackelberg Equilibrium in Discounted Stochastic Games. *IEEE Transactions on Automatic Control, 2023, 68(9)*, 5271-5286.

[194] Hu, Lin; Tan, Shuai; Wen, Hong; Wu, Jinsong; Fan, Jiabing; Chen, Songlin; Tang, Jie (2023). Interference Alignment for Physical Layer Security in Multi-User Networks With Passive Eavesdroppers. *IEEE Transactions on Information Forensics and Security, 2023, 18*, 3692-3705.

[195] Akbar, Mohd; Ahmad, Irshad; Mirza, Mohsina; Ali, Manavver; Barmavatu, Praveen (2023). Enhanced authentication for de-duplication of big data on cloud storage system using machine learning approach. *Cluster Computing, 2023*.

[196] Manchini, Carlos; Ospina, Raydonal; Leiva, Víctor; Martin-Barreiro, Carlos (2023). A new approach to data differential privacy based on regression models under heteroscedasticity with applications to machine learning repository data. *Information Sciences, 2023, 627*, 280-300.

[197] Salinas, Omar; Soto, Ricardo; Crawford, Broderick; Olivares, Rodrigo (2023). An Integral Cybersecurity Approach Using a Many-Objective Optimization Strategy. *IEEE Access, 2023, 11*, 91913-91936.

[198] Burgos-Mellado, Claudio; Zuniga-Bauerle, Claudio; Munoz-Carpintero, Diego; Arias-Esquivel, Yeiner; Cardenas-Dobson, Roberto; Dragicevic, Tomislav; Donoso, Felipe; Watson, Alan (2023). Reinforcement Learning-Based Method

to Exploit Vulnerabilities of False Data Injection Attack Detectors in Modular Multilevel Converters. *IEEE Transactions on Power Electronics, 2023, 38(7)*, 8907-8921.

[199] Hochstetter-Diez, Jorge; Diéguez-Rebolledo, Mauricio; Fenner-López, Julio; Cachero, Cristina (2023). AIM Triad: A Prioritization Strategy for Public Institutions to Improve Information Security Maturity. *Applied Sciences (Switzerland), 2023, 13(14)*, 8339.

[200] López-Vilos, Nicolás; Valencia-Cordero, Claudio; Souza, Richard Demo; Montejo-Sánchez, Samuel (2023). Clustering-Based Energy-Efficient Self-Healing Strategy for WSNs Under Jamming Attacks. *Sensors, 2023, 23(15)*, 6894.

[201] Fernando, Gutierrez-Portela; Brayan, Arteaga-Arteaga Harold; Florina, Almenares Mendoza; Liliana, Calderon-Benavides; Hector-Gabriel, Acosta-Mesa; Reinel, Tabares-Soto (2023). Enhancing Intrusion Detection in IoT Communications Through ML Model Generalization With a New Dataset (IDSAI). *IEEE Access, 2023, 11*, 70542-70559.

[202] Zhu, Yanxu; Wen, Hong; Wu, Jinsong; Zhao, Runhui (2023). Online data poisoning attack against edge AI paradigm for IoT-enabled smart city. *Mathematical Biosciences and Engineering, 2023, 20(10)*, 17726-17746.

[203] Mosso, Edward (2023). Optical-cryptographic scheme based on an image self-disordering algorithm. *Journal of the Optical Society of America A: Optics and Image Science, and Vision, 2023, 40(4)*, C74-C86.

[204] Ruminot, Nicolás; Estevez, Claudio; Montejo-Sánchez, Samuel (2023). A Novel Approach of a Low-Cost Voltage Fault Injection Method for Resource-Constrained IoT Devices: Design and Analysis. *Sensors, 2023, 23(16)*, 7180.

[205] Khalid, Haris M.; Flitti, Farid; Mahmoud, Magdi S.; Hamdan, Mutaz M.; Muyeen, S.M.; Dong, Zhao Yang (2023). Wide area monitoring system operations in modern power grids: A median regression function-based state estimation approach towards cyber attacks. *Sustainable Energy, Grids and Networks, 2023, 34*, 101009.

[206] Zabala-Blanco, David; Hernández-García, Ruber; Barrientos, Ricardo J. (2023). SoftVein-WELM: A Weighted Extreme Learning Machine Model for Soft Biometrics on Palm Vein Images. *Electronics (Switzerland), 2023, 12(17)*, 3608.


Ministerio de
Ciencia,
Tecnología,
Conocimiento
e Innovación
Gobierno de Chile