Hacia una ciberseguridad integral: divergencias y puentes entre los enfoques de la academia, la industria y la comunidad hacker

Revista Latinoamericana de Economía y Sociedad Digital

Issue Especial 2

Autores: Federico Pacheco

DOI: 10.53857/RLESD.04.2023.03

Publicado: 10 marzo, 2024

Recibido: 4 agosto, 2023

Cita sugerida: Pacheco, F. (2023). Hacia una ciberseguridad integral: divergencias y puentes entre los enfoques de la academia, la industria y la comunidad hacker, Revista Latinoamericana de Economía y Sociedad Digital(4)

Tipo: Ensayo

Resumen

Este ensayo se encuadra en un enfoque exploratorio sobre las perspectivas de la ciberseguridad que caracterizan a tres partes del denominado modelo multisectorial: el sector privado, la comunidad técnica y la academia.

La primera hipótesis propuesta es que existe divergencia en las perspectivas; la segunda es que un enfoque integrador, basado en la comprensión de sus fundamentos sociotécnicos, puede contribuir a tejer puentes entre las partes y configurar plataformas multisectoriales robustas para una gobernanza sostenible.

El trabajo se fundamenta en la triangulación de técnicas cualitativas, como la observación participante, el análisis sociotécnico y la revisión de literatura especializada; si bien se plantea una aproximación con tendencias generales, sistémicas y globales, su foco es Argentina. Para cada actor analizado se considera un evento de referencia a nivel nacional: Ekoparty, en la comunidad técnica; Segurinfo, en el sector privado, y Argencon, en el académico. En cada caso, se analizaron las características centrales del tipo de actor, en relación con un enfoque estilizado e identificando semejanzas y diferencias entre

perspectivas, así como los modos en que la emergencia de diversos caminos para el ejercicio profesional refleja tensiones y dinámicas arraigadas en procesos sociohistóricos de larga duración.

En la segunda parte del trabajo se contrasta el planteo con un abordaje prescriptivo, proponiendo elementos teóricos y prácticos que podrían contribuir a una integración de enfoques.

Abstract

This essay is framed as an exploratory approach to the perspectives on cybersecurity that characterize three parts of the so-called multi-sector model: the private sector, the technical community and academia.

The first hypothesis proposed is that there is divergence in perspectives; the second is that an integrative approach, based on an understanding of their socio-technical underpinnings, can help bridge the parties and shape robust multi-sector platforms for sustainable governance.

The work is based on the triangulation of qualitative techniques, such as participant observation, socio-technical analysis and review of specialized literature; although it proposes an approach with general, systemic and global tendencies, its focus is on Argentina. For each actor analyzed, a national reference event is considered: Ekoparty, in the technical community; Segurinfo, in the private sector, and Argencon, in the academic sector. In each case, the central characteristics of the type of actor were analyzed, in relation to a stylized approach and identifying similarities and differences between perspectives, as well as the ways in which the emergence of diverse paths for professional practice reflects tensions and dynamics rooted in long-lasting socio-historical processes.

The second part of the paper contrasts the approach with a prescriptive approach, proposing theoretical and practical elements that could contribute to an integration of approaches.

Resumo

Este ensaio adota uma abordagem exploratória das perspectivas sobre segurança cibernética que caracterizam três partes do chamado modelo multissetorial: o setor privado, a comunidade técnica e a academia.

A primeira hipótese proposta é que há divergência nas perspectivas; a segunda é que uma abordagem integradora, baseada na compreensão de seus fundamentos sociotécnicos, pode ajudar a construir pontes entre as partes e moldar plataformas multissetoriais robustas para

a governança sustentável.

O trabalho baseia-se na triangulação de técnicas qualitativas, como a observação participante, a análise sociotécnica e a revisão da literatura especializada; embora proponha uma abordagem com tendências gerais, sistêmicas e globais, seu foco é a Argentina. Para cada ator analisado, é considerado um evento de referência nacional: Ekoparty, na comunidade técnica; Segurinfo, no setor privado; e Argencon, no setor acadêmico. Em cada caso, foram analisadas as características centrais do tipo de ator, em relação a uma abordagem estilizada e identificando semelhanças e diferenças entre as perspectivas, bem como as maneiras pelas quais o surgimento de diversos caminhos para a prática profissional reflete tensões e dinâmicas enraizadas em processos sócio-históricos de longa data.

A segunda parte do artigo contrasta a abordagem com uma abordagem prescritiva, propondo elementos teóricos e práticos que poderiam contribuir para uma integração de abordagens.

Palabras clave: ciberseguridad, brecha, industria, academia, comunidad

1. Introducción

Este estudio exploratorio de los enfoques sobre ciberseguridad se inscribe en los debates acerca de la gobernanza en esta materia como gobernanza multisectorial (Bradshaw, 2015); en especial, se enmarca en las discusiones sobre cooperación multisectorial en ciberseguridad en América Latina (Hurel, 2016; Bustos y Aguerre, 2022). En el trabajo, se procura describir algunas dinámicas sociotécnicas e históricas de la relación entre academia, industria y comunidad técnica locales, en tanto partes interesadas en la gobernanza de la ciberseguridad, con sus cualidades particulares.

La primera hipótesis exploratoria propuesta sugiere la existencia de una divergencia significativa en el conjunto de las perspectivas de dichos sectores, que se manifiesta en tendencias e indicadores observables (Urgessa, 2020). Este punto de partida asume que, entre las partes interesadas en la gobernanza de la ciberseguridad en América Latina, en especial industria y academia, pero también entre estas y la comunidad de los denominados *hackers*, existe una divergencia de abordajes con raigambre de larga duración, que es necesario reconocer si se pretende facilitar cierta convergencia sobre bases sostenibles.

La segunda hipótesis postula que una estrategia integradora, fundamentada en una comprensión profunda de los aspectos sociotécnicos inherentes a la temática, puede facilitar la creación de puentes entre los diversos actores involucrados, a partir de la consideración de los objetivos en común y las herramientas propias de cada actor. Además, se plantea que este tipo de estrategia podría ayudar a establecer plataformas multisectoriales más sólidas y eficientes, lo cual es crucial para promover una gobernanza sostenible.

Tras la descripción de la metodología, el ensayo se divide en dos secciones. La primera

consiste en un análisis sociotécnico centrado en las partes interesadas estilizadas y asociadas a casos empíricos, para comparar lo que se presenta como sus “enfoques”, en tanto diferentes maneras en que cada grupo considera, entiende o aborda situaciones. Asimismo, el análisis se apoya en la revisión de literatura especializada y observación participante. También, se describe a cada uno de los actores, en busca de puntos de interés con los que puedan ser comparados, desde una perspectiva histórica; en cada caso, se examinan sus características fundamentales en relación con un enfoque estilizado, con el objetivo de identificar similitudes y diferencias entre sus respectivas aproximaciones. Además, se observan las formas en que la emergencia de diversos caminos para el ejercicio profesional refleja las tensiones y dinámicas arraigadas con profundidad en los procesos sociohistóricos de duración prolongada.

En la segunda sección se plantea una lógica abiertamente más ensayística, que presenta los lineamientos generales de un enfoque integrador y diversas recomendaciones para lograrlo. Así, se contrasta el planteo con un abordaje más bien prescriptivo, en el que se propone un conjunto de elementos teóricos y prácticos, que podrían contribuir a una integración sustentable. La propuesta de enfoque integrado reconoce la necesidad de transformar esta disciplina en una ciencia formal, y muestra una serie de sugerencias para acotar las divergencias, reflejando los esfuerzos de los distintos actores y sus efectos potenciales en el ecosistema de la ciberseguridad.

Aunque muchas de las cuestiones caracterizan tendencias globales y sistémicas, el foco principal del estudio es el contexto argentino, con un evento (congreso o conferencia) referente para cada uno de los actores analizados: Ekoparty representando la esfera de la comunidad técnica y *hacker*; Segurinfo, al sector privado, y Argencon reflejando el ámbito académico. A fin de expresar sus cualidades, se realiza un análisis comparativo por cada dimensión propuesta y se resumen en una tabla final, con características por indicador y actor.

• Estrategia metodológica

Para la metodología, se combinaron diversas técnicas cualitativas. Como fuente primaria se contó con observación participante y, en términos de trabajo de escritorio, con el análisis de literatura secundaria, bajo un acento histórico y sociotécnico, y el análisis de tipo-ideales.

La observación participante permite situar el proceso en Argentina a nivel nacional, en tanto el autor ha participado como asistente y orador en múltiples actividades multisectoriales del ámbito de la ciberseguridad, tanto en la industria como en la comunidad técnica y la academia, a lo largo de las dos últimas décadas.

El análisis histórico se limita al proceso de la emergencia de los discursos en torno a la seguridad de la información, la ciberseguridad y los *hackers* en Estados Unidos, desde los

años noventa del siglo anterior, en particular, a partir de la comercialización de Internet, ya que su impacto técnico y cultural conformó la base ideológica de las comunidades alrededor del mundo.

El análisis exploratorio se centró en problematizar y distinguir el carácter de los motivos de las divergencias, para luego encontrar una matriz de indicadores que permitiera operacionalizar la noción más general de "enfoque". Para ello, se consideran tres dimensiones: producción y difusión de conocimiento, valores, y objetivos e implicaciones sociales. En cada una se contemplan distintos indicadores, como se observa en la tabla 1.

Tabla 1. Operacionalización de dimensiones comparativas sobre enfoques de la ciberseguridad

Dimensión	**Indicador**
Producción y difusión de conocimiento.	Tiempos de investigación. Tiempos de publicación. Dificultad de publicación. Validación de la calidad. Financiación y métodos.
Actores y sus valores.	Reputación profesional. Motivación. Valores. Ética y legalidad.
Objetivos e implicaciones sociales.	Objetivos. Partes interesadas.

Fuente: elaboración propia.

El período de tiempo considerado se centra en el siglo XXI, aunque se incluyen ciertas tendencias ancladas en siglo XX. En cuanto al análisis exploratorio-descriptivo, con base en la bibliografía se reconocen las cualidades comparables y se interpretan a la luz de la experiencia del autor, con prioridad en Argentina. A este respecto, a continuación se describe, de manera breve, la principal conferencia, congreso o evento de referencia a nivel nacional para cada ámbito, en los cuales el autor ha participado en casi todas sus ediciones, ya sea como asistente, orador, o bien como miembro de comité de revisión.

- Comunidad: Ekoparty (ekoparty.org). Conferencia anual abierta al público, organizada desde el año 2007 por un grupo de miembros de la comunidad. Desde entonces es considerada la conferencia más importante de Latinoamérica y uno de los diez

principales eventos del mundo para la comunidad internacional de *hacking*, así como punto neurálgico para profesionales y practicantes. Destaca por su rol de generadora de comunidad.

- Industria: Segurinfo (segurinfo.org). Congreso anual organizado desde el año 2005 por Usuaria (organización no gubernamental constituida en 1982). Único de su tipo en Argentina, con ediciones en varios países de Latinoamérica, basado en el patrocinio de empresas del sector y con apoyo de organizaciones como la OEA (Organización de los Estados Americanos) y varias universidades. En la región, este congreso es la referencia por antonomasia en materia de ciberseguridad a nivel corporativo.
- Academia: Argencon (site.ieee.org/argencon). Congreso bianual de ingeniería, organizado desde el año 2012 por la sección argentina del IEEE (Institute of Electrical and Electronics Engineers) y un conjunto de universidades nacionales, que incluye a la ciberseguridad entre sus temas de interés y cuyo alcance se apalanca en la mencionada organización, siendo la más importante del mundo en su tipo. Vale mencionar, además, los congresos académicos CoNaIISI (Congreso Nacional de Ingeniería Informática / Sistemas de Información) y JAIIO (Jornadas Argentinas de Informática), más focalizados en informática y con menos impacto en términos de publicaciones.

Las características de cada tipo de actor fueron analizadas en relación con la ciberseguridad. De este análisis, se recogieron diferencias y similitudes entre los abordajes, así como los modos en que el surgimiento de múltiples trayectorias profesionales revela las complejas tensiones y dinámicas enraizadas en procesos sociohistóricos prolongados.

Los indicadores descriptivos bajo estudio se refieren a dimensiones comparables, que son susceptibles de presentar distinciones entre actores. Dichos indicadores se agrupan en tres categorías; la primera está relacionada con la producción y difusión de conocimiento: tiempos de investigación y de publicación, dificultad de publicación, validación de la calidad, financiación y métodos; la segunda, con los actores y sus valores: reputación profesional, motivación, valores, ética y legalidad, y la tercera categoría corresponde a los objetivos e implicaciones sociales: objetivos y partes interesadas. Esta clasificación se centra en la naturaleza de las dimensiones, aunque existen otras agrupaciones posibles. Quedan fuera del análisis otras categorías, como grado de colaboración y diversidad, grado de originalidad e innovación, impacto social y calidad y cantidad de personas involucradas, las cuales serán examinadas en futuros trabajos.

Respecto a las limitaciones de este estudio, debe destacarse que parte de una experiencia profesional del autor con predominio en la comunidad e industria, más que en el ámbito académico.

Por su parte, estudios futuros podrían considerar la anterior base metodológica, ya sea ampliando el número de indicadores y su clasificación, comparando distintas geografías y

buscando abstracciones que permitan describir al conjunto, o bien realizando análisis de casos empíricos de alcance más específico.

• Resultados

3.1 Enfoques de la ciberseguridad según las partes interesadas

A partir de la premisa de que cada enfoque representa una forma de relacionarse con los distintos aspectos de la ciberseguridad, se analiza cada una de las partes interesadas, a fin de identificar sus particularidades y extraer puntos en común que permitan una mirada integradora.

3.1.1 Academia y ciberseguridad

La comunidad científica se centra en comprender y explicar fenómenos así como en desarrollar teorías basadas en pruebas verificadas mediante experimentos rigurosos, los cuales son diseñados para poner a prueba las hipótesis y resaltan la precisión, la fiabilidad y la reproducibilidad, con estrictas directrices éticas.

La mayoría de los profesionales en ciberseguridad no están entrenados en investigación científica; a su vez, la mayor parte de los investigadores académicos tienen poca experiencia de campo y no logran resultados aplicables con consistencia, además de que la industria no suele resultarles territorio atractivo (De Grande et al., 2014). De hecho, la academia se presenta como elección profesional poco compatible con otros actores.

La investigación académica en ciberseguridad se ha orientado sobre todo hacia una pequeña fracción del campo, que incluye las ciencias de la computación, la criptografía y, en los últimos años, los sistemas ciberfísicos. No obstante, existe un marcado desequilibrio entre los datos (en tanto materia prima) asequibles en la industria y los que están a disposición de los investigadores académicos (Benzel, 2020).

En los orígenes del *software* libre –subcultura hermana del *hacking*–, el modelo de creación de conocimiento de la academia gozó de gran popularidad, ya que los avances acontecen mediante el desarrollo colectivo y la mejora gradual de los modelos y teorías con base en la apertura a la comunidad de pares (Couture, 2020). Además, se considera más importante el modelo abierto que permite su evolución, que los resultados en sí.

Es posible investigar en ciberseguridad solo en busca de comprensión, o bien para desarrollar soluciones a problemas inmediatos. Ambas direcciones son necesarias porque el avance requiere el saber profundo de principios subyacentes así como un estrecho contacto con problemáticas reales. Esto trae aparejada la crítica en los dos frentes para la academia, dado que trabajar sobre el entendimiento no ayuda a resolver las dificultades del momento,

y orientarse a problemas inmediatos puede resultar evanescente, sin dejar resultados generales útiles.

Un último matiz por revisar es que la academia tiende a moverse hacia áreas adyacentes del conocimiento, ya que las líneas de investigación cercanas al saber de los tomadores de decisión y los pares tienen más posibilidades de ser aceptadas, que aquellas que rompen normas y se alejan de lo establecido (estilo *hacker* típico) por ser más difíciles de evaluar y por evidenciar limitaciones personales.

Como resultado de las divergencias estructurales, los estándares actuales de investigación en ciberseguridad son bajos desde el punto de vista científico, incluso en la academia (Maxion et al., 2010).

3.1.2 *Hackers* y comunidad técnica

El concepto de *hacker* nació en los años cincuenta en el contexto universitario estadounidense y fue mencionado por primera vez en los años sesenta en la prensa. En la década de los setenta comenzó a usarse en los medios para referirse a actos delictivos realizados con herramientas tecnológicas. Durante la década de los ochenta y los noventa, conocidos como "la era romántica del *hacking*", dicho término se transformó con actividades consideradas como forma de rebelión o medio para expresar la individualidad y la inteligencia, más que como acción técnica, y sin el fin de causar perjuicio (Holt, 2020). En este periplo surgieron grupos de *hackers* influyentes, famosos por irrumpir en sistemas de gobiernos y empresas dejando mensajes desafiantes al poder e instituciones. Las acciones eran de corte ilegal –aunque no hubiera leyes específicas– y se consideraban una forma de desobediencia tecnológica civil que buscaba un llamamiento a la atención sobre los errores del *software* y a la necesidad de protección de los datos personales.

Los entonces autodenominados *hackers* se unieron en círculos que valoraban la anonimidad y rechazaban las formalidades, las instituciones y a las autoridades. Mientras, el mercado traccionó la educación formal, con la consecuente conversión natural de los egresados de carreras técnicas en empleados de organizaciones. Un grupo más rebelde y con convicciones antisistema se alejó ideológicamente, promulgando una filosofía basada en la libertad de expresión, la protección de la privacidad y los derechos individuales. Esta actitud tomó forma de declaración de principios en muchos que, incluso sin estar vinculados a la tecnología, se identificaban con sus manifiestos (Blankenship, 1986).

En la primera década del siglo XXI, la comunidad técnica comenzó a asociar a los *hackers* con el uso de habilidades para encontrar y explotar debilidades en sistemas, denotando una connotación positiva desde la denominada seguridad ofensiva, la cual busca mejorar la seguridad mediante un proceso indirecto que implica descubrir vulnerabilidades para que puedan ser reparadas. Esto derivó en el concepto de "*hacking* ético" por medio de las llamadas pruebas de penetración, con una lógica equivalente a las pruebas de colisión de vehículos en la industria automotriz para determinar la calidad de las protecciones. Esta

práctica, aunque metodológica, estructurada y planteada como tarea profesional, fue rechazada por la industria, y la controversia contribuyó a crear confusión sobre el significado de *hacker,* al punto que aún hoy es difícil de desarraigar. En la actualidad, los medios continúan señalando como *hackers* a quienes usan habilidades técnicas para fines maliciosos, que, en rigor de la verdad, estos últimos debieran ser nombrados ciberdelincuentes. Mientras tanto, la comunidad busca concientizar sobre un uso más apropiado del término, para desmitificar ideas populares que no hacen honor a sus aportes.

Con la comercialización global de Internet, algunos frentes de la cultura *hacker* tomaron postura explícita contra los títulos universitarios como validadores de conocimientos, y se produjo una especie de romantización del aprendizaje informal en tecnología. En los países con economías en desarrollo de América Latina y el denominado Sur Global, esa tendencia se agudizó, ya que el tiempo y dedicación a una carrera universitaria pueden ser prohibitivos para muchos, dadas las necesidades más urgentes de ingresar al mercado laboral al finalizar la educación secundaria, incluso siendo necesario trabajar durante toda la carrera (Novella et al., 2018). Esta fragmentación de la trayectoria formativa es una suerte de brecha respecto a países desarrollados, donde sí es posible dedicarse exclusivamente a estudiar. En este escenario, la introducción de certificaciones profesionales sirvió como modo alternativo de validar conocimientos, habilitando el acceso a empleos de calidad con salarios competitivos. Así, muchos lograron compensar la falta de títulos o formalizar sus habilidades mientras completaban sus estudios. Otros, más fieles a la ortodoxia originaria, incluso rechazaron esa opción y se mantuvieron al margen, contando solo con sus conocimientos para progresar y proclamando no necesitar validación externa mientras pudieran demostrar resultados de calidad, bajo la antigua premisa de que un *hacker* debe ser juzgado “por su hacking” y no por otros criterios (Levy, 1984).

Esta menor importancia atribuida a los títulos universitarios se relacionó con la relevancia percibida de creer que las habilidades prácticas y conocimientos aplicados son más importantes que las calificaciones y puntajes, que no son, estos últimos, indicadores fiables de las capacidades. Además, muchos adquieren conocimiento por medio del autoaprendizaje y la experiencia, sin educación formal, ya sea por desinterés o falta de acceso a las oportunidades (Fisk et al., 2023).

Por su parte, la filosofía *hacker* original consistía en usar con creatividad la tecnología para resolver problemas y “mejorar el mundo”, a partir de los principios de construir, colaborar, compartir y aprender haciendo, así como del desafío intelectual de superar limitaciones, de manera ingeniosa y con espíritu lúdico y exploratorio. Entonces, la característica que define a un *hacker* no son sus actividades, sino cómo las realiza y si son significativas (Gehring, 2004). Además, al compartir principios con el *software* libre, encuentra en el código abierto, el cenit de la inteligencia colectiva. Este encuadre para el aprendizaje prepondera la exploración de los límites de las posibilidades y está relacionado con la desestructura, el pensamiento lateral y la ausencia de reglas estrictas; lo que benefició a entornos en que eso era inaceptable.

En correspondencia, la cultura *hacker* hace referencia a la comunidad y se asocia con el espíritu de experimentación, curiosidad y deseo de aprender, en un ambiente de camaradería y respeto, basado en el intercambio de conocimiento y la voluntad de asumir riesgos y desafiar a las instituciones imperantes. La comunidad se conforma por individuos de diversos rangos etarios, antecedentes, experiencias y objetivos; algunos pueden tener intenciones innobles, pero la mayoría está comprometida con las causas filosóficas profundas y con poder construir un ecosistema digital más seguro. Si bien ello excede el alcance de este trabajo, un detalle no menor es que pese a las iniciativas de los últimos años, las tasas de participación de mujeres en comunidades de *hacking* son drásticamente más bajas que en la industria y la academia (Dunbar-Hester, 2019).

En adelante, mencionaremos de manera indistinta a la comunidad *hacker* como comunidad de ciberseguridad, comunidad técnica o simplemente comunidad.

3.1.3 Industria de la ciberseguridad

A lo largo de las últimas décadas, la ciberseguridad se convirtió en industria, como consecuencia de la creciente dependencia de la tecnología en la sociedad. La necesidad de protección llevó al desarrollo de medidas defensivas y los avances tecnológicos propiciaron la aparición de nuevos riesgos. A medida que las empresas fueron requiriendo profesionales, surgieron nuevos roles, pero, en cualquier caso, con baja complementariedad con la academia y la comunidad *hacker*.

La evolución de la disciplina ocurrió por etapas; al principio no se consideraba un campo independiente, sino un aspecto de las tecnologías de la información, y las protecciones técnicas se basaban en medidas elementales de *software* y *hardware*. Frente al avance de Internet y la tecnología, aumentó la cantidad, frecuencia y complejidad de las amenazas, lo que hizo necesarias medidas más específicas y sofisticadas. Como resultado, las organizaciones empezaron a crear equipos especializados, que luego se transformaron en áreas de “seguridad informática”, e inició la inversión en tecnologías más avanzadas de monitoreo, detección y prevención. También, se empezaron a aplicar conjuntos de buenas prácticas, procesos de respuesta ante incidentes y métodos tomados de otras áreas de conocimiento, como la gestión de riesgos, gestión de continuidad de operaciones y planificación estratégica. Sumado a la necesidad de implementación y cumplimiento de requisitos legales y regulatorios específicos, el campo pasó a ser nombrado “seguridad de la información”, una denominación más amplia que la anterior porque involucra entornos físicos y gestión, además de tecnología. De manera más reciente, los esfuerzos se desplazaron hacia la prevención de violaciones de datos e información sensible, protección de infraestructura crítica y defensas contra las llamadas amenazas persistentes avanzadas, lo que llevó a la adopción de enfoques más proactivos e integrales, como la inteligencia de ciberamenazas y la automatización de controles. Con este advenimiento, más la necesidad de internacionalización de los términos, comenzó a usarse el nombre de “ciberseguridad” para referir a esta industria y campo de estudio (Alexei y Alexei, 2022).

El desarrollo de la industria se articuló con las contribuciones de la comunidad en técnicas, algoritmos, métodos y procesos. De hecho, muchos proyectos comenzaron como soluciones personales a problemas cotidianos y se expandieron por su utilidad para un grupo mayor (Raymond, 1999). La industria permite a la comunidad técnica ser remunerada por su trabajo, ya que ser contratados por una empresa, en especial si es de vanguardia, es una forma de validación profesional. La aptitud práctica, la experiencia y la pericia demostrada son importantes y muchos *hackers* de éxito se han consolidado como referentes en grandes empresas. En contrapartida, la comunidad es muy crítica con la industria, en particular con las corporaciones, por desacuerdos sobre valores y ética, al punto que en algunos casos se las confronta, como forma de protesta o activismo por razones políticas o ideológicas. Muchas veces son percibidas como demasiado preocupadas por su propio beneficio y poder, más que por la privacidad de los individuos, al tiempo que priorizan sus propios intereses sobre los de la sociedad o no se responsabilizan por sus acciones a largo plazo. Esta representación del *establishment* las transforma en objeto de escrutinio profundo para la comunidad *hacker*, que además puede verse intimidada por decisiones del mercado que afectan su bienestar utópico.

Asimismo, existe una discusión histórica acerca de la forma inapropiada en que muchas empresas abordan los fallos de seguridad en sus productos, que lleva a la comunidad a hacerlos públicos tras el largo tiempo de inacción (Arora et al., 2010). Por ejemplo, si una corporación lanza un nuevo *software* o dispositivo, este se convierte en objeto de investigación de nuevas vulnerabilidades, orientada a garantizar la seguridad y privacidad de los usuarios. Así, las empresas pueden verse perjudicadas o no, según cómo planteen su estrategia de relacionamiento tecnológico con terceros, y deberán reaccionar reparando los errores, por quedar obligadas a enfocarse en resolver aquello que la comunidad identificó. Esta condición produce una relación simbiótica en la que cada parte se nutre de la otra, aunque se presenten como aparentes antagonistas.

Al investigar, la industria intenta establecer protocolos para realizar experimentos reproducibles, sin embargo, para tener rigor científico, requiere publicar los datos utilizados, lo cual no es posible por confidencialidad o protección de información personal identificable. Esto deriva en la creación de conjuntos de datos artificiales que coincidan con las estadísticas de los datos reales, lo que es aceptable para fines corporativos, pero insuficiente para la investigación científica (Gernhardt y Groš, 2022).

• Análisis comparativo

A continuación, se presentan los indicadores descriptivos según la clasificación planteada, sin un orden de importancia determinado y comenzando por los relacionados con la producción y difusión de conocimiento.

En la primera variable, *tiempos de investigación*, la academia marca la referencia de

máxima en cuanto al ritmo y temporalidad, ya que la producción formal de conocimiento se apoya en la prudencia de los métodos y exige un tratamiento sistematizado que deriva en tiempos más prolongados hasta obtener resultados confiables y concluyentes (Khader et al., 2021). Respecto a la industria, esta responde a los tiempos del mercado, ajustando muchas veces sus ciclos a lo realizable en los períodos propuestos, y no al revés. La comunidad, en cambio, maneja un estilo intermedio, más cercano a la industria y traccionado por sucesos.

Los *tiempos de publicación* también tienen a la academia como referencia. La necesidad de publicar y transferir conocimiento marca límites de un mundo que premia la inmediatez, aunque usualmente a costa de la calidad. Si bien los tiempos de la academia se eficientizan cada vez más, tanto la revisión de pares como la corrección de manuscritos revisados, más la producción en sí, determinan cotas mínimas de tiempo que, aunque permiten garantizar la calidad e integridad de lo investigado y publicado, pueden ser frustrantes para los otros actores. Además, el fantasma de "publicar o perecer" asedia a la academia de una forma que ningún otro entorno sufre, aunque esto mismo tiene múltiples aristas beneficiosas (Lee, 2014). La industria, por su parte, obedece a la estacionalidad y temporalidad del año, buscando predictibilidad y periodicidad (mensual, trimestral, anual, etc.). La comunidad, ante sus nulos requisitos e informalidad en entornos propios y redes sociales, no suele realizar aportes significativos a la producción escrita formal.

En cuanto a la *dificultad de publicación*, en la academia el proceso sigue reglas estrictas de referato y aumenta su complejidad y accesibilidad conforme crece la calidad y reconocimiento de la publicación. En la comunidad, tanto las publicaciones como la participación en congresos pasan, en el mejor caso, por revisión de un comité de expertos, que no suele ser a ciegas, lo cual los somete a sesgos que tienden a devenir en decisiones no objetivas. Además, la evaluación de propuestas no exige la existencia previa de trabajos de investigación escritos de manera formal. Incluso, en caso de querer moverse hacia ese lado, la ausencia de requisitos como credenciales, títulos o afiliación a instituciones aleja a la comunidad de la posibilidad de publicar en contextos formales, y esta sumatoria promueve su desinterés, obligando a encontrar caminos propios y menos tradicionales. Por su parte, en la industria, en razón de que cada organización define su estándar de calidad, la dificultad se asocia a lo que esta permita, lo cual se materializa en lo que el mercado valida.

La *validación* de la calidad de los resultados también varía entre actores, siendo la academia la referencia máxima. Allí, la revisión de pares a ciegas conforma el eje central de las decisiones y la asignación de métricas que determinan la calidad de las publicaciones, lo que se refleja en congresos, conferencias, simposios y otros encuentros académicos. En la industria, si bien se apela a opiniones de expertos, es el cliente quien define, en última instancia, la calidad en función de los resultados que obtiene y del problema que aquella resuelve. La comunidad, por su parte, se maneja con un criterio equivalente.

La *financiación* de la investigación diverge también entre actores. El entorno más organizado es la industria, con fondos propios o de otros privados, que permiten

escalabilidad según las necesidades del mercado. La academia suele depender de agencias gubernamentales, fundaciones e instituciones y en algunos casos recibe fondos de empresas y organizaciones, que tienen intereses en ciertos campos. La comunidad, por lo común, encara proyectos de investigación de manera independiente, lo que limita en gran medida su alcance, ya que depende del propio dinero de los investigadores. También puede solventarse por medio de mecenazgos, o bien ser patrocinada por empresas, en una búsqueda de utilidad conjunta.

Los *métodos*, si bien se encuentran disponibles para todos los actores, difieren a la hora de aplicarlos. La academia se ubica en el máximo escalón de calidad con el método científico, contextualmente ineludible; así, su aproximación a los problemas se basa en metodologías, formas estrictas y estructuras como pilares de la generación de conocimiento. En la industria existen opciones metodológicas según el propósito, tipo de preguntas y recursos; son comunes los informes de casos que describen soluciones aplicadas, pero no suelen proporcionar suficiente contexto, o bien hacen demasiadas suposiciones y al no detallar la metodología, constituyen la forma más baja de investigación empírica. Algunos métodos podrían generar conocimiento si se aplicaran de modo adecuado: las encuestas son muy propensas a errores metodológicos, las pruebas de referencia (*benchmarks*) no replican condiciones reales y las pruebas de validación, aunque son procesos más rigurosos, se enfrentan a la complejidad de recrear entornos reales (Edwards, 2016). Por su parte, en la comunidad, si bien pueden realizarse abordajes metodológicos, se admite la desestructura e informalidad, según la necesidad y el objetivo, lo cual limita la calidad de los resultados. Esto permite cortar caminos por vías irregulares, probar cosas más diversas y moverse con bordes más difusos, lo que en específico no es mejor, pero en ocasiones produce buenos resultados; sin embargo, puede dar lugar a una menor preocupación por las consecuencias a largo plazo y a que los métodos no sean siempre transparentes y reproducibles.

Otro conjunto de variables son las relacionadas con los actores en sí y sus valores. En este sentido, la *reputación profesional* cuenta con claras ecuaciones de valoración, que se transitan con el tiempo. En la academia, el estatus de autoridad está abierto a cualquiera que logre resultados, pero la reputación se relaciona con la consistencia de dichos resultados, que se manifiesta a través de publicaciones formales, citas y factores de impacto asociados así como de una carrera sostenida dentro del sistema científico. De modo similar, aunque sin métricas estrictas, en la comunidad la reputación requiere de una combinación de educación, experiencia y contribuciones al campo, y los practicantes se movilizan sobre todo por el reconocimiento de sus pares, siendo el grupo identitario el que principalmente valida a sus miembros, de diversas maneras. De hecho, se dice que “solo un hacker puede reconocer a otro” (Graham, 2005). Además, se logra validación al colaborar en proyectos abiertos, publicar artículos, blogs o libros, presentar trabajos en eventos especializados y lograr visibilizar los valores de la comunidad ante la sociedad. También, se puede construir reputación obteniendo certificaciones profesionales que, si bien en un principio no fueron del todo bien recibidas, son un medio válido para demostrar conocimientos y habilidades (Davis, 2019). En la industria, en cambio, la reputación está asociada al logro de objetivos

(en general relacionados al negocio), el nivel jerárquico alcanzado y el rol en empresas destacadas, lo que limita la transparencia (Himanen, 2001). Además, se valora la participación en asociaciones profesionales y de sectores.

En cuanto a la *motivación*, las cuestiones personales conforman la base para todos los actores, coincidiendo en la búsqueda de reputación profesional, el reconocimiento de pares y la satisfacción por los logros. Más allá de ello, en la academia y la comunidad se destaca la curiosidad, la pertenencia a un grupo y el impacto social como factores motivadores intrínsecos (Chng et al., 2022), en tanto que en la industria se persiguen compensaciones económicas y objetivos comerciales de posicionamiento.

Con relación a los *valores*, si bien las cuestiones humanas básicas coinciden entre terrenos, la academia pondera en especial la libertad, la verdad, la calidad y la responsabilidad social. Por su parte, la comunidad alinea su propósito mayor con valores como la libertad de información, ya que presume que esta debe ser de libre acceso, poder compartirse y ser usada a voluntad; la privacidad, referida al derecho a que la información personal esté protegida, por defecto, de ser recopilada y usada sin consentimiento, y la transparencia en las acciones y procesos de toma de decisiones, en especial en organizaciones y gobiernos, de los que dependen múltiples aspectos de la sociedad. En la misma línea, se valoran la descentralización de sistemas y redes, por considerarse, de esa forma, más resistentes a la censura y al control, y la autosuficiencia con actitud autodidacta, que anima a tomar el control de la propia tecnología para mejorar la seguridad y la funcionalidad (Levy, 1984). Lo antedicho contrasta con los valores de la cultura dominante, que suele hacer hincapié en el control de la información, y esto es parte de lo que se promueve en la industria, la cual busca el beneficio propio, incluso en detrimento del resto de actores.

En cuanto a la legalidad y cuestiones éticas, si bien se trata de aspectos diferentes, por simplicidad, aquí son analizados en conjunto, aunque a riesgo de perder precisión. Dichos aspectos han sido estudiados de manera formal, y en varias ocasiones, con abordaje integral para la ciberseguridad (Christen et al., 2020). La academia contempla cuestiones éticas estrictas, como evitar conflicto de intereses, compartir la propiedad intelectual, mantener una postura crítica ante la influencia externa y garantizar el beneficio a la sociedad. La industria contrasta con cada uno de estos planteamientos porque opera según intereses financieros, busca la protección de la propiedad intelectual para su beneficio, es permeable a las influencias externas de accionistas, inversores y grupos de poder y a veces limita su responsabilidad social a cumplir regulaciones y leyes. En cuanto a la comunidad, algunas actividades pueden lindar los márgenes de la ilegalidad, lo cual es su principal punto de crítica, y promulga la llamada ética *hacker*, basada en sus principios y valores y alineada con lo antedicho para la academia.

El último de los grupos es el de las variables relacionadas con los objetivos y las implicaciones sociales. En la academia, los *objetivos* son el avance del conocimiento y el servicio a la sociedad. Mientras tanto, la industria persigue la producción y comercialización

de bienes y servicios; en ciberseguridad, se enfoca en la protección frente a las ciberamenazas y la mitigación de sus efectos, además, está impulsada por la necesidad de anticipar y prevenir ataques cibercriminales a redes, sistemas y datos. También, llega a mostrar interés en cuestiones empíricas y en satisfacer necesidades de clientes, más que en investigación fundamental, de modo que busca probar lo conveniente para dar relevancia a sus productos o servicios, sin interés genuino en el conocimiento. Y esto limita su validez formal. En cuanto a la comunidad, la demostración de habilidades es un objetivo primordial, y pese a carecer de foco comercial, la investigación suele tener impacto en el mercado, ya que los productos sobre los que esta se realiza son desarrollados por empresas que perciben, directa o indirectamente, los beneficios por la atención que generan. Así, la investigación se vincula a la realidad del mercado y sus temas de cada momento, e implica el análisis de sistemas y tecnologías existentes para identificar vulnerabilidades, o el desarrollo y prueba de nuevas tecnologías y *software*. Adicionalmente, puede ver el mero hecho de crear como un fin en sí mismo, lo que le da un sentido por momentos artístico, que no busca ser productivo.

En cuanto a las partes interesadas y público objetivo, por lo común la investigación académica está destinada a otros investigadores y científicos, aunque, en última instancia, el beneficio debería redundar en la sociedad. En la comunidad, en cambio, aquellos suelen ser otros miembros y grupos específicos de profesionales, aunque las grandes corporaciones son parte indirecta. En el caso de la industria, tanto otras empresas y organizaciones como los propios accionistas y socios conforman el conjunto de partes interesadas.

En general, aunque hay cierto solapamiento entre ámbitos, existen puntos que marcan diferencias diametrales. En la tabla 2 se presenta un resumen con los puntos identificados relativos a la ciberseguridad, como diferencias cualitativas entre partes.

Tabla 2. Síntesis comparativa de enfoques sobre ciberseguridad

	Academia	**Comunidad**	**Industria**
Tiempos de investigación	Mayormente prolongados. Asociados al nivel.	Variables según complejidad.	Internos de la organización.
Tiempos de publicación	Mayormente prolongados. Asociados al nivel.	Variables según grado de formalidad y nivel.	Variables según la empresa. Estacionales y periódicos.
Dificultad de publicación	Asociada a la calidad editorial.	Asociada a calidad del medio.	Asociada a la empresa.
Validación de la calidad	Revisión de pares.	Opiniones de expertos.	Opiniones de expertos. Opiniones de clientes.
Financiación	Gobiernos. Universidades. Centros de investigación.	Fondos personales. Mecenazgo.	Fondos propios. Organizaciones interesadas.
Métodos	Método científico. Estudios controlados.	Métodos informales. Enfoques desestructurados.	Creación de prototipos. Pruebas e implementación.
Reputación profesional	Publicaciones formales. Citas de publicaciones.	Opiniones de pares. Resultados prácticos.	Roles en empresas. Certificaciones profesionales.
Motivación	Generación de conocimiento. Impacto social. Reputación y reconocimiento.	Reputación y reconocimiento. Desafiar límites. Curiosidad.	Compensación económica. Adelantar a la competencia.
Valores	Replicabilidad. Objetividad. Transparencia.	Libertad de información. Derecho a la privacidad. Autosuficiencia.	Variables según la organización.
Ética y legalidad	Evitar conflictos de intereses. Propiedad intelectual compartida. Beneficio a la sociedad.	Ética propia. Legalidad a veces marginal.	Ética limitada por intereses económicos. Legalidad necesaria.
Objetivos	Avance del conocimiento. Beneficios para la sociedad. Comprensión del campo.	Demostración de habilidades. Democratización de saberes. Actos meramente creativos.	Desarrollo de productos. Beneficios económicos. Agenda comercial.
Partes interesadas	Sociedad. Comunidad científica.	Miembros de la comunidad. Grandes corporaciones.	Empresas y organizaciones. Accionistas y socios.

Fuente: elaboración propia.

- **Propuestas para acotar la divergencia**

Existen múltiples maneras de trazar puentes duraderos que permitan hacer avanzar a la ciberseguridad de una forma más integral y sustentable. Para esto, cada actor debe realizar un esfuerzo de distinto tipo y magnitud, que requiere el abandono de su consolidada comodidad, para dirigirse hacia terrenos menos conocidos, algunos ya transitados por disciplinas que debieron trazar sus propios puentes.

En principio, son necesarios la construcción de un lenguaje común y un conjunto de conceptos sobre los que se pueda desarrollar un entendimiento compartido, más una serie de protocolos experimentales consensuados, para facilitar la comprobación de hipótesis y la validación de criterios. Ignorar esto conlleva el riesgo de continuar expandiendo cierto oscurantismo digital, que perjudica al saber.

A partir de la consideración de que los riesgos de ciberseguridad se caracterizan por una incertidumbre fundamental que plantea un gran desafío para su gobernanza y exige nuevas formas de organizar las políticas, las asociaciones público-privadas se consideran una respuesta plausible, al mejorar la flexibilidad y solidez mediante el intercambio de conocimientos (Christensen y Petersen, 2017). Desde el punto de vista de la academia, es posible establecer asociaciones y colaboraciones formales con los profesionales y la comunidad, en diseños de investigación controlada, estudios longitudinales, series temporales, e investigación de campo, siguiendo el ejemplo de otras áreas.

Las universidades y centros de investigación pueden trabajar con empresas y grupos de la comunidad, para proporcionar recursos y conocimientos que ayuden a afrontar los retos en común. Además, es fundamental transmitir la teoría y práctica de la escritura científica y técnica, habilidad indispensable para redactar propuestas de investigación, comunicación de resultados y transferencia de conocimientos, lo cual puede hacerse a través de seminarios y talleres (Behles, 2019). Asimismo, la academia puede proveer a la industria de consultoría y asesoramiento en proyectos concretos o en cuestiones generales, aportando perspectivas y conocimientos formales a cambio de poder conocer los retos y necesidades del mercado. La creación de bibliotecas con revisiones de expertos sobre estudios de temas específicos puede ser también de gran ayuda, como ocurre en medicina. Es necesario mantener un abordaje constructivo desde la humildad intelectual, evitando establecerse puramente en el lugar del conocimiento teórico, que en la práctica profesional es insuficiente.

Por su parte, tanto la comunidad técnica como los profesionales y practicantes de la industria deberían aprender a realizar aproximaciones más estructuradas al conocimiento, a la vez de redactar sus hallazgos y describir sus procesos. También, pueden aprender sobre investigación básica y aplicada y colaborar con investigadores académicos, para ampliar conocimientos y trabajar en proyectos reales con estándares científicos. Lograr mayor proximidad a entornos externos a la propia comunidad técnica es un desafío en sí mismo,

debido a los resquemores creados en el pasado, que hoy tienen poco sentido.

En cuanto a la industria, por su posición privilegiada en el motor de la economía, su responsabilidad y marco de acción son aún mayores. Pese a algunas diferencias insoslayables, la industria y la comunidad han estrechado lazos históricamente. Esta cercanía aparente surge del mero hecho de que los individuos necesitan trabajar para vivir en el contexto de una sociedad de predominancia capitalista, donde las reglas obligan a elegir de forma taxativa las propuestas del sistema. Así, muchos miembros de la comunidad son atraídos por empresas que les garantizan un mejor nivel socioeconómico que el que podrían lograr si se obstinaran en una moral idealista. Más allá de dicho acercamiento, y a fin de reforzar los vínculos, las empresas cuentan con diferentes estrategias posibles.

Una maniobra cada vez más común son los programas de recompensas (*bug bounty programs*), establecidos por las empresas para permitir que especialistas descubran vulnerabilidades en sus productos a cambio de dinero y ayuden a corregirlas antes de sean explotadas por ciberdelincuentes. Esto, a su vez, posibilita el reconocimiento de la comunidad (Malladi y Subramanian, 2019) y se vincula a la práctica de la divulgación responsable, la cual promueve el informe de fallos de seguridad, a fin de que las empresas dispongan de un plazo determinado para solucionarlos y evitar que sean públicos (Cavusoglu et al., 2007). Otra estrategia es patrocinar y organizar conferencias, eventos y encuentros para compartir información y debatir sobre tendencias y desafíos. También, pueden promover competencias del tipo “hackatones” y *Capture The Flag* (CTF), en las que se ponen a prueba habilidades y se demuestran capacidades individuales o grupales, en un contexto realista con características lúdicas. Más allá de tomarlos como terrenos productivos, los hackathones se consideran ideológicamente significativos en la cultura *hacker* (Richterich, 2019). Por último, las empresas pueden fomentar la investigación e innovación abierta y crear programas colaborativos para compartir información y adelantarse a los peligros incipientes. Estas iniciativas pueden beneficiar también a empresas emergentes (*startups*), con procesos más flexibles y fluidos y más tendencia a la innovación (Kantis et al., 2023).

Las anteriores estrategias permiten que las empresas identifiquen talentos contratables, por lo que, si bien las acciones producen conexiones reales, en última instancia pueden servir a sus intereses. En cualquier caso, aquellas pueden ser más proactivas, contratando a graduados universitarios de programas y carreras de ciberseguridad, así como a miembros destacados de la comunidad.

En cuanto a su relación con el mundo académico, la industria puede colaborar en proyectos de investigación, compartiendo recursos, conocimientos e instalaciones, ayudando a incorporar sus perspectivas y necesidades a la investigación y proporcionando acceso a las últimas tecnologías. También, puede ofrecer prácticas y programas cooperativos a investigadores, para proporcionarles experiencia y ayudarles a establecer contactos con posibles empleadores. Además, los líderes pueden actuar como mentores e incluir a

estudiantes en prácticas profesionalizantes, para intercambiar experiencia por perspectivas.

Como última mención, es conveniente potenciar la creación de centros interdisciplinarios, por medio de grupos de expertos que conecten los entornos con puntos de encuentro en los que los actores compartan información y aprendan unos de otros, mejorando la comunicación y facilitando la difusión de ideas y conocimientos. Esto podría complementarse mediante la alineación de programas educativos del ámbito público y privado a los recientes marcos regionales o nacionales de educación en ciberseguridad orientada a la industria, como los existentes en Estados Unidos (Newhouse et al., 2017) y, de forma más reciente, en la Unión Europea. Finalmente, vale observar con detenimiento el caso de España, donde estructuras público-privadas resultaron idóneas, al agrupar la inteligencia colectiva, necesidades y voluntades de todos los agentes para conseguir objetivos comunes con base en la coinversión (González, 2021).

- # Conclusiones

Tanto la academia como la comunidad y la industria desempeñan un papel propiamente ineludible en el campo de la ciberseguridad y su gobernanza, por lo tanto, es de vital importancia encontrar maneras de salvaguardar las distancias y tender puentes que ayuden a crear asociaciones de mutuo beneficio, así como facilitar la transferencia de conocimiento entre sectores. Ese camino comienza al reconocer la importancia de los demás actores en el ecosistema y los riesgos de transformarse en víctimas silenciosas de sus propios sesgos.

Cada actor tiene sus propias fortalezas y debilidades con sus enfoques y valores correspondientes, que influyen en la producción y difusión de conocimiento. Este análisis resalta la necesidad de colaborar para impulsar la creación de información, innovación y progreso, en una sociedad con dependencia creciente de la tecnología y riesgos en aumento.

La búsqueda de una integración sostenible conlleva nuevas preguntas, que deben ser abordadas para formalizar cualquier tipo de análisis, incluyendo la identificación de casos de éxito en la colaboración intersectorial que reflejen los beneficios de dichos esfuerzos. Además, este estudio deja planteada la conveniencia de determinar un conjunto de indicadores descriptivos confiables, que sean transversales y puedan generalizarse para su aplicación en otros alcances geográficos. Para concluir, queda de manifiesto que es menester contar con una metodología de análisis más completa y que permita limitar los sesgos aparejados al campo de experiencia de los investigadores.

Referencias

Alexei, L. A., & Alexei, A. (2022). The difference between cyber security vs information security. *Journal of Engineering Sciences*, (4), 72-83.

Arora, A., Krishnan, R., Telang, R., & Yang, Y. (2010). An empirical analysis of software vendors' patch release behavior: impact of vulnerability disclosure. *Information Systems Research*, *21*(1), 115-132.

Behles, J. E. (2019). *Required skills for technical communicators in cybersecurity* [doctoral dissertation]. University of Wisconsin-Stout.

Benzel, T. (2020). Cybersecurity research for the future. *Communications of the ACM*, *64*(1), 26-28.

Blankenship, L. (1986). The Conscience of a Hacker. *Phrack Magazine*, *1*(7), file 3.

Bradshaw, S., DeNardis, L., Hampson, F. O., Jardine, E., & Raymond, M. (2015). The emergence of contention in global Internet governance. *Global Commission on Internet Governance Paper Series*, (17).

Bustos Frati, G., y Aguerre, C. (2022). *Marco analítico para el análisis de políticas públicas sobre ciberseguridad en los países latinoamericanos*. Centro LATAM Digital.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2007). Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge. *IEEE Transactions on Software Engineering*, *33*(3), 171-185.

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*, 100167.

Christen, M., Gordijn, B., & Loi, M. (Eds.). (2020). *The Ethics of Cybersecurity*. Springer Nature.

Christensen, K. K., & Petersen, K. L. (2017). Public–private partnerships on cyber security: a practice of loyalty. *International Affairs*, *93*(6), 1435-1452.

Couture, S. (2020). Free and Open Source Software. In M. O'Neil, C. Pentzold, & S. Toupin (Eds.), *The Handbook of Peer Production* (pp. 153-168). John Wiley & Sons.

Davis, A. (2019). The Role of Cybersecurity Certifications. In S. Furnell & I. Vasileiou (Eds.), *Cybersecurity Education for Awareness and Compliance* (pp. 222-248). IGI Global.

De Grande, H., De Boyser, K., Vandevelde, K., & Van Rossem, R. (2014). From academia to industry: are doctorate holders ready? *Journal of the Knowledge Economy*, *5*(3), 538-561.

Dunbar-Hester, C. (2019). *Hacking Diversity. The Politics of Inclusion in Open Technology Cultures*. Princeton University Press.

Edwards, B. J. (2016). *Evidence-based cybersecurity: Data-driven and abstract models*. The University of New Mexico.

Fisk, N., Kelly, N. M., & Liebrock, L. (2023). Cybersecurity Communities of Practice:

Strategies for Creating Gateways to Participation. *Computers & Security*, *132*, 103188.

Gehring, V. (Ed.). (2004). *The Internet in Public Life*. Rowman & Littlefield Publishers.

Gernhardt, D., & Groš, S. (2022, May). Use of a non-peer reviewed sources in cyber-security scientific research. In *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 1057-1062). IEEE.

González, J. D. (2021). La importancia de la colaboración Público Privada en ciberseguridad. *Revista SIC: Ciberseguridad, Seguridad de la Información y Privacidad*, *30*(145), 95-97.

Graham, P. (2005). Great hackers. In J. Spolsky (Ed.), *The Best Software Writing I* (pp. 95-109). Apress.

Himanen, P. (2001). *The Hacker Ethic and the Spirit of the Information Age*. Secker & Warburg.

Holt, T. J. (2020). Computer hacking and the hacker subculture. In T. Holt, & A. M. Bosler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 725-742). Palgrave Macmillan.

Hurel, L. M. (2016). *Cybersecurity and internet governance: Two competing fields?* (publicación núm. 3036855) [tesis de licenciatura, Pontificia Universidade Católica de Rio de Janeiro]. SSRN.

Kantis, H., Menendez, C., Álvarez-Martínez, P., & Federico, J. (2023). Colaboración entre grandes empresas y startups: una nueva forma de innovación abierta. *Tec Empresarial*, *17*(1), 70-93.

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity Awareness Framework for Academia. *Information*, *12*(10), 417.

Malladi, S. S., & Subramanian, H. C. (2019). Bug bounty programs for cybersecurity: Practices, issues, and recommendations. *IEEE Software*, *37*(1), 31-39.

Maxion, R., Longstaff, T., & McHugh, J. (2010, September 21-23). *Why Is There No Science in Cyber Science* [panel discussion]. NSPW'10, 2010, Concord, MA, United States.

Lee, I. (2014). Publish or perish: The myth and reality of academic publishing. *Language Teaching*, *47*(2), 250-261.

Levy, S. (1984). *Hackers: Heroes of the computer revolution*. Anchor Press/Doubleday.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (special publication, 800-181). National Institute of Standards and Technology.

Novella, R., Repetto, A., Robino, C., & Rucci, G. (Eds.). (2018). *Millennials en América*

Latina y el Caribe:¿trabajar o estudiar? Banco Interamericano de Desarrollo.

Raymond, E. (1999). The cathedral and the bazaar. *Knowledge, Technology & Policy*, *12*(3), 23-49.

Richterich, A. (2019). Hacking events: Project development practices and technology use at hackathons. *Convergence*, *25*(5-6), 1000-1026.

Urgessa, W. G. (2020). Multilateral cybersecurity governance: Divergent conceptualizations and its origin. *Computer Law & Security Review*, *36*, 105368.

Biografía del autor

Especialista en Ciberseguridad, con formación en ingeniería electrónica. Cuenta con 20 años de experiencia docente, y dicta clases en la Universidad Tecnológica Nacional (UTN) y en la Universidad Nacional de Quilmes (UNQ). Lleva publicados 4 libros y diversos trabajos de investigación, y posee destacadas certificaciones internacionales relacionadas con seguridad de la información. Además, ha trabajado para diferentes gobiernos y empresas multinacionales, incluyendo roles de alcance regional. Actualmente se desempeña como R+D+i Manager en BASE4 Security.