TESIS DE POSGRADO

ESPECIALIZACIÓN EN CIBERCRIMEN

UNIVERSIDAD EMPRESARIAL SIGLO 21 (UES21)

La ciberseguridad más allá de lo técnico: la ciberseguridad como política de seguridad ciudadana. (F.04)

AUTORA: JAQUELINA TALERICO

AÑO 2025

TÍTULO:

Ciberseguridad como política de seguridad ciudadana en Argentina:
Protección de infraestructuras críticas y ciudadanos.

ÍNDICE

Resumen

La presente tesis analiza la ciberseguridad como política pública en la Argentina contemporánea. A partir de un enfoque interdisciplinario, se abordan los principales desafíos institucionales, normativos, culturales y sociales que enfrenta el Estado en la protección de los entornos digitales, las infraestructuras críticas y los derechos ciudadanos. El estudio incluye un análisis comparado con los casos de México y Brasil, así como una revisión de incidentes emblemáticos en Argentina que exponen sus vulnerabilidades. A partir de este diagnóstico, se propone un modelo de gobernanza colaborativa que articule al sector público, privado, académico y a la ciudadanía, con el objetivo de fortalecer las capacidades estatales y construir un entorno digital seguro, inclusivo y resiliente.

Abstract

This thesis analyzes cybersecurity as a public policy issue in contemporary Argentina. Using an interdisciplinary approach, it explores the main institutional, regulatory, cultural, and social challenges the State faces in protecting digital environments, critical infrastructure, and citizens' rights. The study includes a comparative analysis with Mexico and Brazil, as well as a review of emblematic cyber incidents in Argentina that highlight systemic vulnerabilities. Based on this diagnosis, the thesis proposes a collaborative governance model involving public, private, academic, and civil society actors to enhance state capacities and promote a secure, inclusive, and resilient digital environment.

Palabras clave

ciberseguridad, política pública, seguridad ciudadana, infraestructura crítica, gobernanza colaborativa.

Keywords

cybersecurity, public policy, citizen security, critical infrastructure, collaborative governance.

Introducción

En las últimas décadas, el desarrollo de las tecnologías de la información y la comunicación ha transformado profundamente la vida social, política, económica e institucional. La digitalización de procesos estatales, el avance del comercio electrónico, la educación virtual, los servicios financieros online y la comunicación interpersonal han ampliado exponencialmente las oportunidades, pero también han generado nuevas formas de riesgo que afectan tanto a las personas como a las estructuras críticas de los Estados. En este contexto, la ciberseguridad se ha convertido en una condición necesaria para el ejercicio de derechos, la integridad de las infraestructuras y la estabilidad democrática.

La expansión del delito en entornos digitales, el uso malicioso de la tecnología, la explotación de vulnerabilidades y las amenazas a infraestructuras estratégicas colocan a la ciberseguridad en el centro del debate sobre la seguridad contemporánea. Ya no se trata únicamente de una problemática técnica, reservada a especialistas informáticos, sino de un fenómeno social, político y jurídico que exige abordajes integrales. La protección de los entornos digitales impacta directamente en la vida cotidiana de las personas y en la capacidad de los Estados para garantizar derechos fundamentales como la privacidad, la identidad, la libertad de expresión y el acceso a servicios esenciales.

En América Latina, y en particular en Argentina, el tratamiento de la ciberseguridad como política pública ha avanzado en forma desigual y fragmentada.

Si bien existen normativas, instituciones y programas que abordan el tema, todavía persisten importantes desafíos vinculados con la falta de estrategias sostenidas, la debilidad de los marcos normativos, la escasa articulación entre actores, la subestimación del problema y la ausencia de una cultura preventiva consolidada. Estos vacíos generan brechas de protección, limitan la capacidad de respuesta estatal y colocan en situación de vulnerabilidad tanto a ciudadanos como a sectores estratégicos como la salud, la energía o las telecomunicaciones.

Este trabajo propone abordar la ciberseguridad desde una perspectiva de política pública, entendida como un campo de intervención estatal que debe articular múltiples niveles y actores para garantizar entornos digitales seguros y resilientes.

La investigación se centra en el análisis del caso argentino, con énfasis en el abordaje estatal de la ciberseguridad, la protección de infraestructuras críticas y la seguridad ciudadana en el entorno digital. Asimismo, se realiza un análisis comparado con los casos de México, y Brasil, con el propósito de identificar buenas prácticas, obstáculos comunes y posibles líneas de mejora. El enfoque elegido es interdisciplinario, integrando herramientas del derecho, la sociología, la ciencia política y la tecnología.

Asimismo, se consideran casos emblemáticos de ciberataques ocurridos en Argentina en los últimos años, como los incidentes que afectaron a la Dirección Nacional de Migraciones, el PAMI y empresas privadas como Telecom, que exponen con crudeza la vulnerabilidad de infraestructuras críticas. Estos hechos refuerzan la necesidad de una política pública integral que trascienda la lógica reactiva y apueste por una cultura preventiva y participativa.

En este marco, la tesis propone un modelo de gobernanza colaborativa que incorpore al sector público, privado, académico y a la ciudadanía, entendiendo que solo a través de una acción conjunta será posible construir entornos digitales resilientes y seguros.

PLANTEAMIENTO DEL PROBLEMA

La aceleración de la digitalización en los ámbitos social, institucional y productivo ha introducido riesgos que van más allá de lo técnico, afectando directamente la seguridad ciudadana. En este contexto, la ciberseguridad ha trascendido su rol técnico, emergiendo como un pilar estratégico para la seguridad pública, la protección de infraestructuras críticas y la gobernanza democrática.

A pesar de los avances normativos e institucionales, Argentina enfrenta desafíos significativos para consolidar una política integral de ciberseguridad. La fragmentación de estrategias a nivel federal, la limitada coordinación entre sectores público, privado y académico, y la baja tasa de denuncia de incidentes —con solo el 39.7% de los 591 casos reportados en 2021, según CERT.ar (2023)— reflejan una respuesta estatal predominantemente reactiva. Este enfoque quedó en evidencia con el ciberataque al Renaper en 2024, que expuso vulnerabilidades en la gestión de datos sensibles, debilitando la prevención y dejando sectores como salud y telecomunicaciones expuestos.

La creciente dependencia de infraestructuras tecnológicas ha intensificado la vulnerabilidad a ciberataques que comprometen servicios esenciales, subrayando la necesidad de integrarla como prioridad en las políticas públicas para resguardar tanto infraestructuras críticas como a los ciudadanos.

Este trabajo aborda la ciberseguridad como una política de seguridad ciudadana, promoviendo un enfoque preventivo y transversal. El problema investigado no se limita a los aspectos técnicos del delito informático, sino que abarca las condiciones estructurales, normativas e institucionales que restringen la capacidad estatal para garantizar entornos seguros digitales e inclusivos.

1. Justificación

La transformación digital de Argentina ha acelerado la dependencia de infraestructuras críticas que sustentan el funcionamiento de sectores vitales como energía, salud, telecomunicaciones y sistemas financieros, situando la ciberseguridad como una prioridad estratégica para la seguridad nacional y el desarrollo económico.

En un mundo cada vez más interconectado, donde las operaciones esenciales dependen de sistemas digitales complejos, la protección frente a ciberataques no solo constituye una cuestión técnica, sino un desafío político, social y jurídico.

La Comisión Económica para América Latina y el Caribe (CEPAL) ya advertía al respecto que:

"*En un mundo cada vez más digital y conectado, con tecnologías disruptivas y tiempos de implementaciones muy exigentes, la exposición a recibir un ciberataque es solo una cuestión de tiempo. El esfuerzo debe realizarse entonces para reducir las posibilidades de ocurrencia, mediante un plan de gestión de ciberseguridad, que contemple medidas efectivas sobre los procesos, la tecnología y las personas, independientemente del tamaño de la organización, y al mismo tiempo, prepararse de la mejor manera posible para atender una incidencia*" (CEPAL, 2020, p. 16).

Esta afirmación refuerza la necesidad de que las políticas públicas en ciberseguridad superen una visión meramente técnica para incorporar estrategias integrales de anticipación, mitigación y resiliencia. La comprensión y análisis detallado de esta compleja problemática se abordará en profundidad en el desarrollo de este trabajo.

La progresiva sofisticación de los ataques digitales y la multiplicidad de vectores de amenaza, desde el ransomware hasta la manipulación de datos críticos, exigen que las políticas públicas incorporen no solo la dimensión tecnológica sino también la jurídica y social.

La interdependencia de los sectores económicos y la globalización de los flujos digitales hacen imprescindible que Argentina fortalezca sus capacidades nacionales

en sintonía con estándares internacionales, para no quedar rezagada en un contexto donde la ciberseguridad es un factor clave de competitividad y seguridad.

A nivel regional, América Latina se ha convertido en una de las regiones de mayor crecimiento en incidentes cibernéticos, con un aumento exponencial de ataques que afectan infraestructuras críticas y sistemas de información, generando un impacto económico cuantificable y riesgos que trascienden las fronteras digitales para influir en ámbitos políticos, sociales y culturales. Argentina no es ajena a esta realidad; casos emblemáticos de filtraciones masivas de datos, ataques de *ransomware* y campañas de *phishing* (ver glosario), han puesto en evidencia la urgente necesidad de fortalecer sus capacidades de ciberseguridad (CERT.ar, 2023; Fortinet, 2023). Esta coyuntura requiere un abordaje multidimensional que integre elementos técnicos, jurídicos, organizacionales y sociales, como se desarrollará más adelante.

Este fenómeno, lejos de ser exclusivo de la región, es reflejo de una tendencia global donde los actores maliciosos aprovechan las debilidades institucionales y las brechas tecnológicas para causar impactos significativos. En este escenario, resulta crucial analizar cómo las limitaciones estructurales pueden ser subsanadas mediante modelos de cooperación público-privada y el desarrollo de una cultura digital resiliente.

No obstante, a pesar de los esfuerzos realizados, la respuesta estatal argentina enfrenta obstáculos estructurales significativos. Entre ellos, destaca la fragmentación institucional y la falta de una coordinación efectiva entre los distintos organismos públicos, así como la débil cooperación con el sector privado y la académico.

Estos factores limitan la capacidad del país para implementar medidas preventivas y reaccionar con agilidad ante incidentes, dejando a sectores críticos vulnerables y ampliando el riesgo nacional. Además, persiste una insuficiente inversión en infraestructura tecnológica y en la formación técnica especializada, lo que dificulta el desarrollo de una capacidad sostenida y resiliente. En este sentido, avanzar hacia un modelo colaborativo de gobernanza en ciberseguridad que

promueva la corresponsabilidad, la integración de actores y una gestión coordinada es una necesidad impostergable.

El entramado institucional fragmentado y la ausencia de un liderazgo claro dificultan la creación de estrategias integradas y sostenibles. Esto no solo afecta la capacidad de reacción ante incidentes, sino también la prevención y la gestión del riesgo en escenarios complejos y dinámicos. En consecuencia, la coordinación entre organismos públicos, sector privado y sociedad civil debe transformarse en una prioridad política, orientada a establecer un marco normativo claro, mecanismos de intercambio de información seguros y procesos de formación continua.

Esta perspectiva invita a plantear interrogantes esenciales para el diseño de políticas públicas efectivas: ¿Cómo puede el Estado facilitar y asegurar una cooperación eficaz entre los sectores público y privado? ¿Qué mecanismos regulatorios y técnicos son necesarios para garantizar la confianza y la protección jurídica en el intercambio de información sensible? ¿De qué modo puede integrarse la academia y la sociedad civil para potenciar la innovación y la educación en ciberseguridad? Estas preguntas orientan el análisis y proponen un camino hacia la construcción de un sistema nacional robusto y adaptable.

En este contexto, la construcción de una política pública eficaz exige la incorporación de perspectivas multidisciplinarias que integren el conocimiento técnico, jurídico y sociocultural. La pregunta por cómo diseñar e implementar estas políticas sin vulnerar derechos fundamentales, y garantizando la equidad en el acceso y protección digital, es un desafío central que orienta el análisis crítico de esta tesis.

En paralelo, la prevención eficaz del cibercrimen no puede reducirse únicamente a la aplicación del derecho penal ni al despliegue de tecnología avanzada.

Es imprescindible fomentar una cultura digital que potencie la alfabetización crítica y promueva una ciudadanía consciente de sus derechos, responsabilidades y riesgos en el entorno digital. Esto incluye la formación en buenas prácticas, el conocimiento de los mecanismos legales para la protección de datos personales, y la disponibilidad de canales accesibles para la denuncia y reparación ante incidentes

digitales. La reducción de brechas digitales y la inclusión social son condiciones indispensables para que esta cultura sea genuina y efectiva, las cuales serán abordadas en detalle en esta tesis.

El fortalecimiento de una ciudadanía digital activa y consciente no solo minimiza el impacto de los ataques, sino que también fomenta la participación en la co-construcción de políticas y estrategias. La alfabetización digital crítica debe ser concebida como un derecho social, y su promoción, una responsabilidad compartida entre Estado, instituciones educativas y sector privado. Solo a través de esta sinergia se podrá cerrar la brecha entre desarrollo tecnológico y protección ciudadana.

El impacto económico del cibercrimen representa una amenaza tangible para el desarrollo sostenible y la competitividad del país en un mercado global cada vez más digitalizado. Las pérdidas derivadas de ataques informáticos, fraudes electrónicos y vulneraciones de datos afectan no solo a las organizaciones directamente involucradas, sino también a la confianza de consumidores, inversores y ciudadanos. Sin políticas públicas robustas que articulen prevención, detección, respuesta y recuperación, y que garanticen el respeto irrestricto a los derechos fundamentales —como la privacidad, la libertad de expresión y el debido proceso—, la vulnerabilidad estructural persistirá, limitando el progreso tecnológico y afectando la cohesión social.

El cibercrimen afecta de forma directa a la economía formal e informal, creando un efecto multiplicador en la pérdida de productividad y confianza. Este impacto trasciende el ámbito digital para incidir en la calidad de vida de la población, la generación de empleo y la innovación tecnológica. La ausencia de políticas integrales y coordinadas en esta materia representa un obstáculo para el crecimiento inclusivo y sostenible del país, lo que demanda una reflexión profunda y la definición de prioridades estratégicas.

Adicionalmente, la experiencia comparada con países de la región, como Brasil y México, ofrece valiosas lecciones sobre la adopción de estrategias nacionales unificadas y la implementación de modelos efectivos de cooperación público-privada, que han demostrado mejorar la capacidad de respuesta y la resiliencia frente a

amenazas cibernéticas. El análisis de estos ejemplos, así como la evaluación de índices internacionales como el Global Cybersecurity Index, proveen un marco de referencia relevante para la adaptación de políticas al contexto argentino.

La experiencia regional y global muestra que las soluciones efectivas combinan la adopción de normativas actualizadas con la capacitación constante de recursos humanos especializados, la inversión en infraestructura tecnológica y la promoción de una cultura organizacional de seguridad.

Argentina tiene la oportunidad de aprender de estas experiencias para diseñar un modelo propio, adaptado a su realidad, que fomente la innovación tecnológica y garantice la protección ciudadana en el entorno digital.

La presente investigación se propone contribuir a la comprensión de estos desafíos y al diseño de un modelo integral y adaptado a la realidad argentina, que integre aspectos técnicos, legales y sociales. A través de una mirada interdisciplinaria, se busca aportar una propuesta de política pública que fortalezca las capacidades institucionales, promueva una ciudadanía digital activa y garantice la protección de los derechos fundamentales en el entorno digital.

Este trabajo no solo aspira a diagnosticar el estado actual y los desafíos existentes, sino también a aportar una propuesta de política pública integral en materia de ciberseguridad, basada en la evidencia empírica, el análisis comparado y el marco normativo vigente. A través de una mirada interdisciplinaria, se busca contribuir al diseño de una estrategia nacional que fortalezca las capacidades institucionales, promueva una ciudadanía digital activa y garantice la protección de los derechos fundamentales en el entorno digital.

OBJETIVOS

1. Objetivo General

- Integrar la ciberseguridad en las políticas públicas de seguridad ciudadana en Argentina, con el fin de mejorar la respuesta coordinada y eficaz ante las amenazas cibernéticas, fortaleciendo la protección de las infraestructuras críticas.

2. Objetivos Específicos

1. Analizar el estado actual de la ciberseguridad en las políticas públicas argentinas y su impacto en la protección de infraestructuras críticas.

2. Comparar las políticas de ciberseguridad de Argentina con las de otros países de la región, como Brasil y México, para identificar prácticas exitosas que puedan aplicarse en el contexto argentino.

3. Proponer un modelo de integración de ciberseguridad en las políticas públicas de Argentina que responda a los desafíos identificados y promueva una cultura de seguridad digital.

MARCO METODOLÓGICO

La investigación adopta un paradigma cualitativo-descriptivo, definido por Hernández Sampieri, Fernández Collado y Baptista Lucio (1991) como “aquella que busca especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice. Describe tendencias de un grupo o población” (p. 80). Mediante la técnica de análisis documental, se examinan fuentes relevantes para comprender la ciberseguridad como política de seguridad ciudadana en Argentina, analizando los desafíos en la protección de infraestructuras críticas y los derechos ciudadanos, así como el impacto de las políticas públicas en un marco normativo resiliente.

La metodología se basa en el análisis de documentos oficiales, normativas nacionales e internacionales, informes de organismos multilaterales y literatura académica sobre ciberseguridad. Esto permite estudiar la evolución de la ciberseguridad en Argentina,

comparándola con modelos de Brasil y México, para identificar buenas prácticas y desafíos en la protección de infraestructuras críticas y ciudadanos.

1. Hipótesis

La integración de la ciberseguridad como componente clave de las políticas de seguridad ciudadana fortalecerá la capacidad de Argentina para prevenir y responder a amenazas cibernéticas, promoviendo entornos digitales más seguros y resilientes para las infraestructuras críticas y la población.

MARCO TEÓRICO

El marco teórico de esta tesis se desarrolla a lo largo de los once capítulos que componen el cuerpo del trabajo, integrando un enfoque interdisciplinario que articula conceptos del derecho, la ciencia política, la sociología, los estudios en tecnología y la gestión pública. La investigación aborda la ciberseguridad no solo como un desafío técnico, sino como una política pública estratégica, orientada a proteger infraestructuras críticas y garantizar derechos fundamentales en el entorno digital.

En el Capítulo I, se sientan las bases conceptuales de la ciberseguridad en el contexto argentino y latinoamericano, identificando los principales enfoques teóricos, la evolución del concepto y su relación con la seguridad ciudadana. El Capítulo II traza un recorrido por la evolución institucional y normativa en la región, analizando cómo distintos países han construido sus estrategias nacionales en esta materia.

El Capítulo III presenta un diagnóstico integral de la situación argentina, evidenciando debilidades estructurales en materia de prevención, articulación interinstitucional y cultura digital, a partir del análisis de datos, índices e informes especializados. El Capítulo IV profundiza el tratamiento de la ciberseguridad como política pública, analizando su incorporación progresiva en las agendas estatales, su marco normativo y los desafíos de su institucionalización.

Los Capítulos V y VI abordan dos pilares estratégicos: por un lado, la necesidad de una gobernanza colaborativa que articule al sector público, privado, académico y a la sociedad civil; y por otro, la construcción de una cultura de la

ciberseguridad y una ciudadanía digital consciente, como condición para una protección efectiva en entornos digitales.

El Capítulo VII analiza la influencia del Convenio de Budapest y de los instrumentos internacionales en la adaptación del marco legal argentino, mientras que el Capítulo VIII amplía la mirada hacia otras normativas globales y regionales que condicionan o inspiran las políticas locales.

En el Capítulo IX, se examinan diversas iniciativas educativas y campañas de concientización en el país, reconociendo su impacto limitado y proponiendo su articulación en una estrategia nacional. El Capítulo X incorpora evidencia empírica a través del análisis de casos emblemáticos de ciberataques en organismos públicos y privados, destacando vulnerabilidades comunes y la falta de respuesta estructurada.

Finalmente, el Capítulo XI presenta una propuesta de política pública integral basada en un modelo de integración de la ciberseguridad en la estructura estatal, incluyendo acciones concretas en cinco dimensiones: gobernanza, marco normativo, formación, cultura y evaluación. Este marco conceptual y aplicado sostiene la hipótesis central de la tesis: que la ciberseguridad debe ser concebida como una política pública de seguridad ciudadana, preventiva, transversal y corresponsable.

Capítulo I. Fundamentos de la ciberseguridad en Argentina y América Latina

A finales del siglo XX, la expansión de internet y la digitalización de sectores clave, como la banca y las telecomunicaciones, transformaron la seguridad global, exponiendo a gobiernos y ciudadanos a nuevas formas de delitos digitales. En América Latina, esta transición fue más lenta, pero igualmente crítica, ya que los países comenzaron a enfrentar amenazas como el robo de datos y el sabotaje informático. Los primeros intentos por regular estos riesgos surgieron en la década de 2000, cuando la interconexión de sistemas evidenció la necesidad de marcos normativos y cooperación regional. En Argentina, la falta de infraestructura tecnológica y conciencia digital limitó los avances iniciales, dejando al país vulnerable frente a un panorama de amenazas en constante evolución (BID & OEA, 2020). Este escenario global y regional marcó el punto de partida para las políticas de ciberseguridad en la región.

En América Latina, la ciberseguridad ha evolucionado de manera gradual, impulsada por la digitalización de sectores estratégicos y el aumento de ciberataques. Históricamente, Argentina ha adoptado un enfoque limitado y fragmentado en términos de ciberseguridad, centrado más en la reacción ante incidentes que en una planificación preventiva o en el desarrollo de una infraestructura robusta. La creciente sofisticación de los ataques, sumada a la interdependencia digital entre sectores económicos, sociales y gubernamentales, exige una política de ciberseguridad más amplia, estructurada y coordinada.

Antes de la pandemia, Argentina enfrentaba ciberataques que revelaban la fragilidad de sus sistemas digitales. En la década de 2010, los fraudes bancarios mediante phishing, se multiplicaron, con delincuentes enviando correos electrónicos falsos que engañaban a los usuarios para obtener sus credenciales bancarias. Estos ataques, cada vez más sofisticados, usaban técnicas de ingeniería social y sitios web fraudulentos para explotar la confianza de los ciudadanos y las debilidades de las plataformas financieras (Saín, 2018). Aunque menos resonantes que los incidentes posteriores, estos fraudes evidenciaron la necesidad de normativas como la Ley 26.388, que buscó tipificar los delitos informáticos. Las vulnerabilidades expuestas

por estos casos anticiparon los desafíos que se intensificaron con la digitalización acelerada durante el COVID-19.

Durante la pandemia de COVID-19, el incremento de incidentes cibernéticos en América Latina puso en evidencia las debilidades estructurales del ecosistema digital regional, especialmente en sectores críticos como salud, energía y educación (CEPAL, 2020). La región, en general, ha adoptado medidas reactivas ante amenazas inmediatas, sin un marco de continuidad o una estrategia a largo plazo. Según CEPAL (2022), uno de los principales obstáculos es la falta de inversión sostenida y políticas públicas consistentes, lo que lleva a que los esfuerzos se diluyan con los cambios de gestión y que se actúe principalmente en contextos de crisis.

En este marco, organismos como la OEA y el BID (2020) han señalado que los modelos de gobernanza colaborativa —basados en la articulación entre el sector público, privado y académico— son fundamentales para incrementar la resiliencia frente a ciberamenazas. La implementación de estos modelos en América Latina permitiría avanzar hacia estándares similares a los de regiones más maduras en la materia. Esta perspectiva ha comenzado a permear en los debates nacionales sobre seguridad digital, aunque con avances desiguales.

En cuanto al plano normativo, Argentina ha mostrado ciertos avances. La sanción de la Ley 26.388 en 2008, que incorporó delitos informáticos al Código Penal, marcó un primer paso relevante. Esta norma introdujo figuras como el acceso ilegítimo a sistemas, el daño informático y la violación de datos personales (Argentina. Congreso de la Nación, 2008). Posteriormente, la Ley 26.904 de 2013 tipificó el grooming, visibilizando riesgos específicos que afectan a niños, niñas y adolescentes en entornos digitales (Argentina. Congreso de la Nación, 2013).

Sin embargo, expertos citados por el Ministerio Público Fiscal de Salta (2021), como Marcos Salt, han advertido que estos avances normativos resultan insuficientes frente a desafíos como la persecución de delitos transnacionales, la responsabilidad de los intermediarios tecnológicos, y la obtención de evidencia digital en entornos que requieren garantías constitucionales. En este sentido, también se destaca la creación de organismos como el CSIRT.AR en 2015, que si bien ha permitido avances en la

detección y respuesta a incidentes, continúa operando en un contexto de escasa articulación con otras áreas del Estado, y sin una estrategia nacional de ciberseguridad plenamente operativa.

Capítulo II. Evolución de la ciberseguridad en Argentina y América Latina

La evolución de la ciberseguridad en América Latina presenta desafíos persistentes en materia de preparación, articulación institucional y cultura organizacional. En el informe de la CEPAL (2022), se señala que una porción significativa de los responsables logísticos considera que recién después de sufrir un incidente cibernético incrementaría su inversión en ciberseguridad. Además, se identifica que muchas pequeñas y medianas empresas desconocen los mecanismos para reportar ataques, y que la visibilidad del fenómeno se ve afectada por la baja tasa de denuncia, ya que las organizaciones tienden a resolver los incidentes de forma privada, sin informar a las autoridades.

Por su parte, el informe del BID y la OEA (2020) indica que hasta principios de ese año, solo siete países de América Latina y el Caribe contaban con un plan de protección para sus infraestructuras críticas. Además, se reporta que 20 países habían creado algún tipo de equipo de respuesta a incidentes (CERT o CSIRT), doce habían aprobado una estrategia nacional de ciberseguridad y apenas diez tenían un organismo estatal específico a cargo de esta área. Estos datos permiten observar que la región todavía presentaba un bajo nivel de desarrollo institucional en términos de ciberseguridad estratégica.

En el caso argentino, Saín, Carnaghi y Wierzbinsky (2021) advierten que muchas empresas afectadas por ciberdelitos no realizan la denuncia correspondiente, ya sea por desconocimiento del circuito institucional o por temor al impacto reputacional. Esta práctica, según los autores, contribuye a una cifra oculta que impide dimensionar con precisión la magnitud de los delitos digitales. También se señala que, ante este contexto, el Estado muchas veces interviene de manera tardía o reactiva, lo que limita su capacidad de implementar políticas eficaces en la materia.

En la última década, Argentina ha impulsado medidas específicas para fortalecer su infraestructura de ciberseguridad, aunque de forma dispersa. En comparación con otros países de la región como Brasil o México, el desarrollo local ha carecido de una estrategia integral y de largo plazo. Un ejemplo de avance parcial es la Decisión Administrativa 641/2021, que estableció puntos focales en organismos

clave para monitorear incidentes. Si bien representa una mejora institucional, su impacto se ve limitado por la ausencia de un marco unificado de gobernanza digital.

En contraste, países como México han consolidado estructuras interinstitucionales que integran a actores públicos y privados bajo estrategias nacionales coherentes. Este modelo permite una mejor respuesta preventiva y una mayor resiliencia sistémica. De acuerdo con el Global Cybersecurity Index (GCI) 2024, estas estructuras han contribuido no solo a una mejor defensa de infraestructuras críticas, sino también a fortalecer el posicionamiento internacional de esos países en términos de confianza e inversión en economía digital.

El caso de Brasil también es ilustrativo: su Estrategia Nacional de Ciberseguridad ha permitido una coordinación transversal de esfuerzos entre fuerzas de seguridad, agencias técnicas y empresas del sector privado. En este marco, se articulan capacidades tecnológicas con políticas públicas sostenidas. En cambio, en Argentina la falta de continuidad y de liderazgo centralizado ha provocado avances fragmentados que se diluyen con el tiempo (CEPAL, 2022).

El Informe Anual de Incidentes de Seguridad 2023 de CERT.ar confirma un aumento sostenido de ataques dirigidos a instituciones públicas, organismos descentralizados y empresas estratégicas. Este escenario demanda una transformación urgente del modelo nacional de ciberseguridad, que integre prevención, respuesta, capacitación y evaluación permanente. Las políticas implementadas hasta el momento han mostrado resultados acotados, en parte por la falta de mecanismos efectivos de cooperación interinstitucional, y en parte por la escasa inversión presupuestaria destinada a estos fines.

Por último, el desajuste entre la rapidez de evolución de las amenazas digitales y la lentitud normativa e institucional para responder a ellas configura una vulnerabilidad estructural. El desarrollo de una estrategia nacional integral, con liderazgo político, participación federal y compromiso del sector privado, resulta indispensable para revertir esta tendencia.

Capítulo III. Diagnóstico de la ciberseguridad en Argentina y América Latina

Actualmente, Argentina enfrenta desafíos importantes en su capacidad para proteger sus infraestructuras críticas y responder a ciberataques. La clasificación en el **Global Cybersecurity Index (GCI) 2024** como país "*Evolutivo*" indica que, si bien existen algunos avances, el país aún tiene limitaciones en términos de coordinación interinstitucional y capacidades técnicas especializadas (Barclay, 2024).

Al comparar la situación con países como Brasil y México, que ocupan niveles de "Rol Modelador" y "Avanzado" en el índice, queda claro que la integración de la ciberseguridad en las políticas de seguridad pública es fundamental para mejorar la resiliencia ante amenazas cibernéticas.

La situación actual pone de relieve una fragmentación en los esfuerzos de ciberseguridad, donde diferentes organismos y sectores gestionan sus riesgos de manera independiente, sin un marco nacional que permita una respuesta coordinada.

En este sentido, los esfuerzos aislados de ciberseguridad han creado una situación en la que cada sector maneja sus propios riesgos de forma autónoma, lo cual impide una defensa unificada. La colaboración interinstitucional y el establecimiento de un centro de ciberseguridad unificado se presentan como alternativas necesarias para mejorar la resiliencia del país frente a las ciberamenazas.

A pesar de los avances institucionales, persiste una asignación presupuestaria limitada a la ciberseguridad: solo el 4% del gasto tecnológico estatal se destina a este rubro, frente al 10% en Brasil o el 8% en México. Asimismo, menos del 10% de los organismos públicos y solo el 20% del sector privado nacional han implementado certificaciones internacionales como la ISO/IEC 27001, lo cual profundiza la vulnerabilidad estructural del país frente a amenazas cibernéticas (Actualidad Esquina, 2024).

A este escenario se suma un bajo índice de denuncia de los delitos informáticos, que contribuye a una amplia cifra oculta. Muchas veces, los incidentes son resueltos directamente por las propias víctimas —como empresas privadas— que evitan exponer públicamente sus vulnerabilidades por temor al daño reputacional, o

que confían en soluciones administrativas o técnicas sin intervención judicial. Esta falta de intervención del Estado limita el conocimiento real sobre la magnitud del problema y debilita su capacidad de respuesta institucional (Saín, Carnaghi & Wierzbinsky, 2021).

La falta de colaboración entre el sector público y privado es un problema estructural que limita la efectividad de las políticas de ciberseguridad. El informe de la **OEA y BID (2020)** subraya que América Latina necesita avanzar hacia modelos de gobernanza en ciberseguridad que involucren a todos los actores en un esfuerzo conjunto, una necesidad que es especialmente crítica en el caso de Argentina. La falta de coordinación centralizada no solo limita la capacidad de respuesta, sino que también genera duplicidad de esfuerzos, dificultando la optimización de los recursos disponibles.

Desde una perspectiva interpretativa, el estado actual de la ciberseguridad en Argentina revela la importancia de un cambio de mentalidad hacia la ciberseguridad como parte integral de la seguridad nacional.

La adopción de un enfoque preventivo que incluya la colaboración entre sectores, la capacitación y la creación de una cultura de seguridad digital permitiría a Argentina reducir sus vulnerabilidades y avanzar hacia un entorno digital más seguro y resiliente. La implementación de un modelo integral podría no solo mejorar la seguridad ciudadana, sino también fortalecer la posición de Argentina en el entorno digital global.

Capítulo IV. Ciberseguridad como política pública en Argentina y América Latina

La ciberseguridad es hoy una dimensión estratégica de las políticas públicas. Su transversalidad exige la articulación entre protección técnica, derechos fundamentales y gobernanza institucional. En este sentido, la elaboración de una política pública en ciberseguridad debe considerar no solo la prevención del delito, sino también la defensa de garantías constitucionales como la privacidad, la libertad de expresión y el debido proceso.

A diferencia de otras áreas tradicionales de la seguridad pública, el campo digital impone desafíos inéditos: delitos sin fronteras, evidencia volátil, actores privados involucrados en la infraestructura crítica. Por ello, se vuelve necesario que el Estado no solo legisle, sino que desarrolle una capacidad institucional especializada. Esto implica equipos técnicos, formación permanente y la creación de protocolos de actuación frente a incidentes digitales.

De acuerdo a Saín, (Saín, 2018, p. 15-16) la fragilidad de la evidencia digital constituye uno de los principales desafíos en las investigaciones penales vinculadas a delitos informáticos. Este tipo de prueba se caracteriza por su volatilidad —ya que puede perderse simplemente al apagar un dispositivo—, su facilidad de modificación u ocultamiento en dispositivos externos o entornos virtuales, y su anonimato, que dificulta la atribución directa de las acciones a sus responsables. Estas particularidades obligan a desarrollar marcos técnicos y jurídicos que permitan preservar, identificar y validar la prueba digital de manera eficiente y conforme al debido proceso.

Además, debe tenerse en cuenta que la inseguridad digital afecta especialmente a los sectores más vulnerables. La carencia de educación digital, la falta de acceso a herramientas seguras y la limitada capacidad para reconocer amenazas hacen que ciertas poblaciones estén más expuestas. Por tanto, una política pública en ciberseguridad no debe ser elitista ni tecnocrática, sino profundamente inclusiva, con perspectiva de derechos humanos y equidad territorial.

La aprobación de la Segunda Estrategia Nacional de Ciberseguridad de Argentina en 2023, formalizada mediante la Resolución 44/2023, representó un avance significativo en la consolidación de la ciberseguridad como una política pública estructural. Este documento, elaborado por el Comité Nacional de Ciberseguridad, establece ocho principios rectores —incluyendo la protección de derechos humanos, la equidad de género, la paz en el ciberespacio y el fortalecimiento federal— y se articula en 42 medidas organizadas en torno a objetivos estratégicos como la protección de infraestructuras críticas, la promoción de la concientización ciudadana, el desarrollo normativo, la soberanía digital y el fomento de una industria nacional de ciberseguridad (Lara, 2024).

Su enfoque trasciende la dimensión técnica, promoviendo una cultura de seguridad digital inclusiva que abarca a todos los sectores sociales. Entre sus disposiciones, destaca la creación de una unidad de articulación y seguimiento, encargada de monitorear resultados, coordinar entre organismos e incorporar contenidos de ciberseguridad en las currículas educativas, reflejando una visión integral que supera las perspectivas meramente policiales o tecnológicas.

En un contexto regional, Argentina se alinea con países como Brasil y México, que también han desarrollado estrategias nacionales de ciberseguridad con enfoques multisectoriales. La Estrategia Nacional de Ciberseguridad de Brasil (E-Ciber), formalizada en 2020 mediante el Decreto Nº 10.222 y prorrogada hasta 2024, persigue tres grandes metas: fortalecer la resiliencia nacional, posicionar al país como referente internacional y promover la prosperidad digital. Sus acciones incluyen la capacitación técnica, la concientización ciudadana, la investigación tecnológica y la participación activa en foros globales, construidas con la colaboración de actores públicos y privados (Lara, 2024).

Por su parte, México publicó en 2017 su Estrategia Nacional de Ciberseguridad (ENCS), con apoyo de la Organización de los Estados Americanos, centrada en cinco objetivos: proteger los derechos ciudadanos, garantizar la seguridad nacional, fomentar la cooperación internacional, impulsar la prosperidad económica y consolidar la confianza en el gobierno digital. Aunque ha avanzado en la promoción

de una cultura de ciberseguridad y en la capacitación técnica, su implementación enfrenta desafíos por la falta de armonización institucional (Lara, 2024).

A pesar de los avances en estos países, la región muestra un panorama heterogéneo. Naciones como Chile, Colombia y Costa Rica cuentan con estrategias formales, mientras que otras, como Perú o Uruguay, están en fases de desarrollo, y países como El Salvador o Venezuela aún carecen de documentos oficializados (Lara, 2024). En el caso argentino, la Segunda Estrategia enfrenta obstáculos estructurales que podrían limitar su impacto: la ausencia de recursos presupuestarios adicionales, una débil cultura de evaluación en políticas digitales y una articulación interjurisdiccional insuficiente. La clave para su éxito radica en la capacidad del Estado para institucionalizar esta hoja de ruta de manera transversal y sostenida, transformándola en una política pública efectiva y no en un conjunto de intenciones. La participación activa del sector privado, la sociedad civil y el sistema educativo será fundamental para consolidar un modelo de gobernanza colaborativa que fomente la equidad, la resiliencia y la soberanía tecnológica en el entorno digital.

Capítulo V. Gobernanza colaborativa en ciberseguridad

Uno de los pilares para enfrentar eficazmente el ciberdelito es la gobernanza colaborativa. Las amenazas actuales exceden ampliamente la capacidad de un solo actor estatal: requieren la participación de empresas tecnológicas, proveedores de servicios de internet, centros académicos y organizaciones de la sociedad civil. Esta lógica de corresponsabilidad es central para la eficacia de cualquier estrategia nacional.

La cooperación público-privada no puede limitarse al intercambio de alertas o firmas digitales. Debe incluir procesos de construcción conjunta de normativas técnicas, canales para compartir evidencia bajo garantías de legalidad y mecanismos de confianza mutua. El modelo propuesto en el Convenio de Budapest —y profundizado en su Segundo Protocolo Adicional— representa un avance en esta dirección, habilitando incluso solicitudes transfronterizas de datos a proveedores privados (Conde, 2023).

En Argentina, los marcos normativos aún presentan debilidades para aprovechar esta cooperación. Marcos Salt, citado por el Ministerio Público Fiscal de Salta (2021), advierte que los tiempos procesales, la falta de fiscales especializados y la ausencia de infraestructura digital interoperable dificultan la obtención de pruebas en causas penales.

Esta situación, tal como se describe en ese documento institucional, exige reformas legislativas, inversión estatal y la creación de unidades judiciales capacitadas en delitos informáticos.

Además, existen ejemplos concretos de intentos de cooperación público-privada en el país, aunque todavía limitados en alcance y sistematicidad. La creación de la Red Nacional de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRTs), impulsada desde la Dirección Nacional de Ciberseguridad, promueve un marco de colaboración entre organismos públicos y entidades privadas con capacidad técnica en la detección de amenazas. Si bien su funcionamiento aún enfrenta desafíos

de coordinación, representa un modelo embrionario de trabajo conjunto que podría fortalecerse con mayores recursos y liderazgo político.

Otro ejemplo es la articulación que se ha dado, en contextos de crisis, entre entes reguladores como el ENACOM y empresas proveedoras de servicios de internet (ISPs), especialmente ante incidentes masivos de *denegación de servicio* (ver glosario) o fugas de datos. Sin embargo, estos esfuerzos suelen carecer de continuidad institucional, dado que responden a lógicas ad hoc y no a un protocolo establecido de acción conjunta. Como señala la OEA y el BID (2020), la sostenibilidad de la gobernanza en ciberseguridad requiere que la cooperación sea parte de un marco formal, con roles definidos, incentivos claros y objetivos estratégicos compartidos.

Es fundamental que universidades nacionales promuevan convenios con organismos del Estado y empresas del sector privado para formar profesionales en ciberseguridad, impulsar la investigación y desarrollar herramientas innovadoras de detección temprana, fomentando un modelo colaborativo articulado dentro de políticas públicas estructuradas (Ministerio de Seguridad, 2023; Gobierno de Argentina, 2023, p.5) .

Por otra parte, la gobernanza en ciberseguridad debe trascender las respuestas reactivas para convertirse en un sistema adaptativo que integre a todos los actores de manera sostenible. La experiencia regional muestra que países como México y Brasil han avanzado en la institucionalización de espacios de diálogo y coordinación permanentes, donde se comparten no solo información sobre amenazas sino también recursos, capacidades y experiencias (BID y OEA, 2020). Estas mesas de trabajo han permitido un monitoreo continuo y la implementación conjunta de planes de contingencia, favoreciendo la resiliencia de sus ecosistemas digitales.

En este sentido, la creación de marcos legales claros que regulen la cooperación público-privada es crucial. El establecimiento de incentivos para que el sector privado participe activamente —por ejemplo, mediante beneficios fiscales o certificaciones de seguridad— podría fomentar una mayor transparencia y compromiso. Asimismo, la confianza y protección jurídica para el intercambio de

información sensible debe ser garantizada para evitar temores sobre responsabilidad legal o vulneración de privacidad (BID y OEA, 2020).

Desde la perspectiva sociocultural, la construcción de una cultura organizacional de ciberseguridad en empresas y organismos públicos resulta esencial para que la colaboración no sea solo formal sino operativa. Esto implica no solo protocolos técnicos sino también capacitación, sensibilización y políticas internas que promuevan la gestión compartida del riesgo.

Además de los aspectos normativos y estructurales, la cooperación público-privada debe contemplar un enfoque territorial y federal, reconociendo que las capacidades técnicas y los riesgos cibernéticos varían según las regiones del país. Las provincias y municipios también enfrentan amenazas digitales —por ejemplo, ransomware o hackeos a sitios oficiales—, pero muchas veces carecen de unidades técnicas propias o de protocolos de respuesta. Esto plantea la necesidad de incluir a los gobiernos locales en las estrategias nacionales y establecer redes de colaboración que no se limiten al nivel central.

Otro elemento clave es la incorporación de criterios de transparencia y responsabilidad compartida en las alianzas público-privadas en materia de ciberseguridad. La Segunda Estrategia Nacional de Ciberseguridad (Gobierno de Argentina, 2023) destaca estos valores como principios rectores, fundamentales para fortalecer la confianza entre actores estatales y privados. En este marco, los esquemas de cooperación deberían promover entornos seguros para el intercambio de información, respetando los derechos humanos y fomentando la corresponsabilidad en la protección de los datos y los sistemas críticos.

Finalmente, en un escenario global atravesado por conflictos geopolíticos, espionaje digital y ciberinteligencia ofensiva, la soberanía tecnológica emerge como un eje estratégico en las discusiones sobre gobernanza. La dependencia de tecnologías extranjeras, tanto para infraestructura crítica como para soluciones de ciberdefensa, limita la autonomía estatal y expone a los países a riesgos externos difíciles de gestionar.

Por ello, fomentar una industria local de ciberseguridad —mediante cooperación con universidades, pymes tecnológicas y agencias estatales— no solo es una cuestión de desarrollo económico, sino también de seguridad nacional.

Capítulo VI. Cultura de la ciberseguridad y ciudadanía digital

La prevención eficaz del ciberdelito no puede lograrse solo desde el castigo penal ni desde la tecnología: necesita una cultura de la ciberseguridad. Esto implica que tanto los usuarios como las instituciones adquieran hábitos, conocimientos y actitudes que reduzcan su exposición a riesgos digitales. La alfabetización digital crítica es tan importante como el software de protección.

El informe elaborado por Saín, Carnaghi y Wierzbinsky (2021) durante la pandemia mostró que muchas víctimas de fraudes digitales no sabían distinguir un correo oficial de un intento de phishing, ni tenían recursos para denunciar correctamente lo ocurrido. Esto revela una brecha estructural en materia de educación digital, tanto en lo formal como en lo informal. La falta de protocolos de denuncia claros y accesibles también agrava la desprotección.

Además, promover una ciudadanía digital implica que los usuarios conozcan sus derechos en línea: cómo reclamar por uso indebido de datos, cómo protegerse del acoso digital, qué hacer ante la pérdida de identidad digital. Las campañas estatales deben ir más allá de “no compartas tu contraseña” y abordar la dimensión ética, legal y social de la vida conectada.

Si bien el avance de las políticas públicas en materia de ciberseguridad en Argentina ha estado enfocado mayormente en el plano técnico y normativo, la dimensión cultural y educativa sigue siendo un desafío estructural. Desarrollar una verdadera cultura de la ciberseguridad requiere no solo capacitar técnicamente a ciertos sectores estratégicos, sino también generar conciencia colectiva, promoviendo hábitos digitales seguros y una ciudadanía crítica frente a los riesgos del entorno virtual.

La ciudadanía digital debe entenderse como el ejercicio pleno de derechos y responsabilidades en entornos digitales. Esto incluye, entre otros aspectos, la capacidad de proteger la propia privacidad, identificar contenidos maliciosos, ejercer el derecho a la información y participar activamente en la creación de una comunidad digital segura. La cultura de la ciberseguridad, por tanto, no puede limitarse a la

transmisión de normas técnicas: debe abordar también los aspectos éticos, legales y sociales del uso de la tecnología (Saín et al., 2021).

En este contexto, las brechas digitales representan un obstáculo concreto para la inclusión efectiva en una cultura de seguridad digital. Según el Banco Interamericano de Desarrollo (2020), una proporción significativa de la población latinoamericana carece de acceso regular a internet o utiliza dispositivos obsoletos, lo que no solo dificulta la alfabetización digital sino que aumenta la exposición a ciberamenazas, especialmente en sectores vulnerables como adultos mayores, niños y habitantes de zonas rurales.

Por otra parte, las campañas estatales de concientización en ciberseguridad, si bien se han multiplicado en los últimos años, tienden a ser fragmentadas, episódicas y con escaso alcance territorial. Esto genera un enfoque reactivo en lugar de preventivo. La falta de continuidad, articulación con el sistema educativo y participación de actores sociales impide que dichas campañas se transformen en verdaderas políticas públicas sostenidas en el tiempo.

Un ejemplo de política orientada en la dirección correcta es el Programa Nacional de Concientización en Ciberseguridad lanzado en 2023, que busca generar capacidades en el ámbito educativo y laboral. No obstante, su implementación aún es incipiente y no alcanza a constituir una estrategia integral, la educación digital en ciberseguridad debería ser entendida como un derecho ciudadano y no como una medida técnica circunstancial.

La formación en ciberseguridad debe comenzar desde edades tempranas y ser incorporada en todos los niveles educativos, desde la primaria hasta la universidad. Pero también debe estar presente en entornos laborales, comunitarios y estatales, a través de planes de capacitación periódicos. La alfabetización digital no se limita al uso técnico de dispositivos, sino que abarca el pensamiento crítico, la gestión de la identidad digital, la ética en el uso de información y el conocimiento de los derechos digitales.

Además, resulta necesario fortalecer las instancias de denuncia, asistencia y reparación para víctimas de delitos informáticos.

El diseño de portales accesibles, campañas multilingües e instancias de mediación en línea permitiría acercar el sistema de protección a la ciudadanía. Como bien señalan Saín et al. (2021), gran parte del daño que provocan los ciberdelitos deriva no solo del hecho delictivo, sino de la sensación de indefensión y aislamiento que experimentan las víctimas al no saber cómo actuar frente a estas situaciones.

En síntesis, una cultura de la ciberseguridad y una ciudadanía digital activa son componentes esenciales para fortalecer la resiliencia social frente a las amenazas digitales. La acción estatal debe enfocarse no solo en proteger, sino también en empoderar a los usuarios con herramientas concretas para reconocer riesgos, ejercer sus derechos y participar activamente en la construcción de un entorno digital ético, seguro e inclusivo.

Capítulo VII. La Convención de Budapest y su aplicación en Argentina

El Convenio sobre Ciberdelincuencia, conocido como el Convenio de Budapest y firmado en 2001 (Organización de los Estados Americanos, 2003), es considerado el instrumento internacional más completo en la regulación del cibercrimen. Actúa como marco para que los países adapten sus normativas en relación con los ciberdelitos, abarcando la tipificación de conductas criminales como ataques a la seguridad de los sistemas, fraudes electrónicos y delitos relacionados con el abuso y la explotación infantil, además de establecer procedimientos para la obtención de evidencia y la cooperación internacional.

El Convenio de Budapest representa un punto de inflexión en la lucha jurídica internacional contra el cibercrimen. No solo establece delitos, sino que propone una arquitectura de cooperación jurídica que permite avanzar en investigaciones a pesar de las fronteras físicas. Su enfoque es mixto: normativo, procesal y de cooperación judicial. En Argentina, la adhesión implicó revisar el Código Penal, capacitar a operadores judiciales y actualizar los canales de asistencia mutua. Uno de los principales aportes del tratado ha sido la creación de puntos de contacto 24/7, que permiten preservar evidencia digital crítica incluso antes de que se formalice un pedido internacional (Ministerio de Justicia y Derechos Humanos de la Nación, 2019). Esto ha sido especialmente relevante en delitos como pornografía infantil, grooming y fraudes bancarios.

El Segundo Protocolo Adicional (2023) refuerza esta cooperación transfronteriza al permitir solicitudes directas de información a empresas extranjeras bajo estrictas salvaguardas legales (OCEDIC, 2022). Para Argentina, este instrumento representa una oportunidad para fortalecer su capacidad de investigación de ciberdelitos complejos, aunque exige una supervisión rigurosa para proteger derechos fundamentales como la privacidad y el debido proceso, asegurando un equilibrio entre seguridad y libertades digitales.

Capítulo VIII. Marco legal internacional y su influencia en Argentina

El fenómeno del cibercrimen ha impulsado, en las últimas décadas, el desarrollo de instrumentos jurídicos internacionales destinados a armonizar normas penales sustantivas y procesales, así como a fortalecer la cooperación entre países en la investigación de delitos informáticos. Entre ellos, el más relevante y pionero es el Convenio sobre Ciberdelincuencia del Consejo de Europa, conocido como Convenio de Budapest, adoptado en 2001 y en vigor desde 2004. Este tratado ha sido ratificado por más de 60 países, incluyendo a varios de América Latina, y constituye el marco jurídico global más robusto en la materia (OCEDIC, 2022).

Argentina adhirió al Convenio de Budapest a través de la Ley 27.411 en 2017, lo cual implicó un compromiso formal de adecuación legislativa y procedimental. Este instrumento establece una lista mínima de delitos informáticos que los Estados firmantes deben tipificar, entre ellos el acceso ilegal a sistemas informáticos, la interferencia en datos, el fraude informático, el abuso sexual infantil en línea y la falsificación informática. Pero su aporte más significativo es el Título III, dedicado a la cooperación internacional, que habilita a las autoridades nacionales a solicitar datos transfronterizos, realizar medidas urgentes de preservación de evidencia digital y coordinar operativos en tiempo real con otros Estados Parte (Conde, 2023).

La influencia del Convenio de Budapest en la legislación argentina ha sido parcial. Si bien la Ley 26.388 de 2008 ya contemplaba algunos de los delitos exigidos por el tratado, la ratificación posterior del convenio generó presión para adaptar mecanismos procesales a las exigencias de cooperación internacional. En este sentido, se han producido avances como la designación del punto de contacto 24/7 en el ámbito del Ministerio Público Fiscal, que permite coordinar rápidamente con otros países la conservación de evidencia digital antes de que desaparezca o sea alterada (Ministerio de Justicia, 2019). No obstante, especialistas del ámbito jurídico y técnico han señalado que la implementación efectiva del convenio aún enfrenta obstáculos estructurales, como la falta de uniformidad normativa en las provincias y la ausencia de protocolos nacionales específicos para operar con la urgencia que requieren estos delitos (Saín et al., 2021).

El Segundo Protocolo Adicional al Convenio, adoptado en 2022, representa una evolución del marco original, centrada en el acceso directo a información de proveedores de servicios privados. Este instrumento permite a las autoridades judiciales de un Estado parte solicitar datos a empresas extranjeras —*como plataformas digitales o proveedores de correo electrónico*—, sin pasar por el engorroso proceso tradicional de asistencia jurídica mutua, aunque con salvaguardas importantes en materia de protección de datos y debido proceso (OCEDIC, 2022).

Argentina firmó este Segundo Protocolo el 16 de febrero de 2023 en Estrasburgo; sin embargo, para que sus disposiciones sean plenamente vinculantes, es necesario que el Congreso Nacional lo ratifique. Hasta la fecha, no se ha confirmado públicamente dicha ratificación. Esta situación refleja uno de los desafíos más frecuentes en la adopción de instrumentos internacionales: la brecha entre la firma simbólica y la implementación efectiva de sus disposiciones.

En términos prácticos, la armonización con estándares internacionales sigue siendo una deuda pendiente en el país. Tal como señala la OEA (2020), en América Latina, muchos Estados han suscripto convenios internacionales sin realizar las reformas internas necesarias para garantizar su aplicabilidad. En Argentina, esto se traduce en la coexistencia de normas nacionales con instrumentos internacionales que no siempre se articulan eficazmente, generando inseguridad jurídica o dilaciones en procesos clave como la obtención de evidencia digital alojada en servidores extranjeros.

Desde una perspectiva más amplia, el impacto del derecho internacional en la lucha contra el cibercrimen no se limita a lo normativo. La construcción de confianza entre Estados y entre actores públicos y privados también se ve influenciada por el grado de compromiso con instrumentos como el Convenio de Budapest. La capacidad de un país para proteger sus infraestructuras críticas, perseguir delitos complejos y colaborar en operativos globales depende, en parte, de su reputación jurídica y su integración en redes de cooperación internacional formalizadas.

Capítulo IX. Educación y concientización en ciberseguridad en Argentina

La creciente digitalización de la sociedad argentina ha puesto en evidencia la necesidad de fortalecer la educación y concientización en ciberseguridad como pilares fundamentales para la prevención de delitos informáticos y la protección de los derechos digitales. Diversos actores, tanto del sector público como privado y de la sociedad civil, han implementado iniciativas para abordar esta problemática desde múltiples enfoques.

9.1. Iniciativas gubernamentales

El Estado argentino ha desarrollado programas y campañas orientados a sensibilizar a la población sobre los riesgos en el ciberespacio. Una de las más destacadas es la campaña federal “Pará, Pensá, Conectate”, impulsada por el Ministerio de Seguridad, que busca reforzar la concientización en ciberseguridad y brindar estrategias para profundizar la seguridad en el uso de tecnologías e Internet (Ministerio de Seguridad, 2023).

En el ámbito de las pequeñas y medianas empresas (PyMEs), se ha implementado una Ruta de Aprendizaje en Ciberseguridad, que incluye capacitaciones sobre seguridad de la información, protección de datos y arquitectura de ciberseguridad, con el objetivo de fortalecer las capacidades de este sector frente a las amenazas digitales (Ministerio de Desarrollo Productivo, 2023).

Asimismo, la Resolución 44/2023 establece la creación de un plan programático de concientización de alcance nacional sobre la seguridad en el ciberespacio, abarcando a toda la sociedad y promoviendo la inclusión de la ciberseguridad en las currículas educativas (Ministerio de Seguridad, 2023).

9.2. Organizaciones de la sociedad civil y sector privado

La organización Argentina Cibersegura ha desarrollado diversas campañas y actividades para promover el uso responsable de Internet y la tecnología. Entre ellas, la campaña #EnVosEs se enfoca en concientizar a los jóvenes sobre la privacidad y

la huella digital, brindando herramientas y consejos para cuidar la información personal en línea (Argentina Cibersegura, 2023).

Por su parte, la plataforma SMARTFENSE ofrece soluciones de concientización en ciberseguridad mediante módulos interactivos, simulaciones de ataques y herramientas de gamificación, orientadas a generar un cambio de comportamiento real y permanente en los usuarios (SMARTFENSE, 2023).

La Fundación Dr. Manuel Sadosky, a través de su programa Program.AR, busca impulsar el aprendizaje y la enseñanza de las Ciencias de la Computación en las escuelas, promoviendo la inclusión de contenidos de ciberseguridad en la educación formal (Fundación Sadosky, 2023).

9.3. Movimientos comunitarios y culturales

El movimiento “Cybercirujas”, surgido en 2020 en la Universidad Nacional de Córdoba, se dedica a recuperar tecnología en desuso para reducir la brecha digital y combatir la obsolescencia programada. Organizan eventos como “reparatones” y “ollas populares de hardware”, donde enseñan a la comunidad a reparar dispositivos y promueven el uso de software libre, fomentando la autonomía tecnológica y la concientización sobre el consumo responsable (El País, 2024).

Estas iniciativas reflejan un enfoque integral y multisectorial en la promoción de la educación y concientización en ciberseguridad en Argentina, reconociendo la importancia de empoderar a la ciudadanía para enfrentar los desafíos del entorno digital.

No obstante estos avances, los esfuerzos en educación y concientización en ciberseguridad en Argentina aún presentan desafíos importantes. La mayoría de las iniciativas carecen de articulación entre sí, no se encuentran integradas en una estrategia nacional sostenida y suelen tener un alcance limitado en términos geográficos y demográficos. Persiste una fuerte brecha entre sectores urbanos y rurales, y entre niveles socioeconómicos, en relación con el acceso a formación digital crítica. Para lograr un impacto estructural, se requiere institucionalizar la enseñanza de la ciberseguridad en todos los niveles del sistema educativo, garantizar campañas

permanentes y federales orientadas a distintos públicos, y fortalecer la cooperación entre el Estado, la sociedad civil y el sector privado. De lo contrario, el componente humano seguirá siendo el eslabón más débil de la cadena de seguridad digital.

Capítulo X. Casos emblemáticos de ciberdelitos en Argentina

10.1. Tendencias generales y contexto

En los últimos años, Argentina ha experimentado un crecimiento exponencial en la cantidad y sofisticación de ciberataques, dirigidos tanto a instituciones públicas como a empresas del sector privado. Según Fortinet, en 2022 se registraron más de 10.000 millones de intentos de ciberataques en el país, lo que representa un incremento del 200% respecto al año anterior (Fortinet, 2023).

Por su parte, el informe anual del CERT.ar señaló que durante 2021 se reportaron 591 incidentes de seguridad informática, lo que implicó un aumento del 161% en comparación con 2020. Del total, el 39,7% de los ataques afectaron a sitios del Estado, posicionando al sector público como el más comprometido (CERT.ar, 2021). La pandemia de COVID-19 intensificó esta tendencia, al generar una mayor dependencia de los entornos digitales y, por tanto, una mayor superficie de exposición. En ese contexto, proliferaron los ataques de phishing, ransomware y denegación de servicios, dirigidos especialmente a áreas críticas como salud, migraciones y telecomunicaciones (LV12, 2020).

10.2. Casos destacados en organismos públicos

Uno de los ataques más significativos ocurrió en agosto de 2020, cuando la Dirección Nacional de Migraciones fue blanco de un ransomware "*netwalker"* (ver glosario) que obligó a suspender el tránsito fronterizo por varias horas. Los ciberdelincuentes cifraron información y exigieron el pago de un rescate para restablecer los sistemas comprometidos. Un mes después, la Agencia Nacional de Seguridad Vial también fue víctima de un ataque que expuso datos sensibles de ciudadanos, generando alarma sobre la protección de la información que manejan los organismos estatales (LV12, 2020; Infobae, 2020).

En junio de 2023, la Comisión Nacional de Valores fue atacada por el grupo *Medusa* (ver glosario), que cifró archivos y robó documentación interna. Si bien el incidente fue contenido, las plataformas digitales del organismo quedaron fuera de servicio durante varios días (Ámbito, 2025).

Otro incidente grave ocurrió en agosto de 2023, cuando el PAMI fue atacado por el grupo Rhysida. La organización no accedió al pago del rescate, por lo que miles de datos de beneficiarios y proveedores fueron publicados en la dark web (RePro Digital, 2024).

Otro caso relevante ocurrió en junio de 2024, cuando el Ministerio de Salud fue afectado por un ataque de ransomware que paralizó temporalmente los sistemas administrativos. Los atacantes solicitaron un rescate en criptomonedas y accedieron a registros sensibles vinculados a la gestión hospitalaria (Innovación Digital 360, 2025).

En octubre de ese mismo año, el Registro Nacional de las Personas (ReNaPer) también fue vulnerado por el atacante “gov.eth”, quien filtró información personal de ciudadanos argentinos. Este caso evidenció fallas en los protocolos de seguridad y la necesidad urgente de reforzar la protección de bases de datos estatales (Innovación Digital 360, 2025).

Más recientemente, el 25 de diciembre de 2024, el sistema Mi Argentina y la plataforma SUBE fueron blanco de un ciberataque de alto impacto que expuso información sensible de millones de usuarios y paralizó funciones críticas del ecosistema digital gubernamental.

Este incidente no solo tuvo consecuencias operativas inmediatas, sino que también reveló graves falencias estructurales, entre ellas, la ausencia de protocolos de respuesta efectivos y la falta de implementación de estándares internacionales como la certificación ISO/IEC 27001 en organismos estatales clave (Actualidad Esquina, 2024).

El Hospital Churruca, perteneciente a la Policía Federal, fue blanco de un ataque en diciembre de 2024. Se vieron afectadas tanto las prestaciones médicas como la distribución de medicamentos, debido a la falta de sistemas de respaldo eficientes (Innovación Digital 360, 2025).

10.3. Casos destacados en el sector privado

En julio de 2024, Telecom Argentina fue víctima de un ataque de ransomware ejecutado por el grupo *REvil* (ver glosario), que exigió un rescate de 7,5 millones de dólares. La brecha de seguridad se produjo a través de una vulnerabilidad *Zero-Day* en Citrix, lo que permitió que el *malware* se distribuyera a más de 18.000 dispositivos internos (Telecom Argentina, 2024; Innovación Digital 360, 2025).

En noviembre de 2024, el Grupo Rossi, compuesto por los centros médicos Rossi, Stamboulian y Laboratorio Hidalgo, sufrió un grave ataque que inhabilitó sus sistemas informáticos durante más de 20 días, interrumpiendo la atención médica y la realización de estudios de diagnóstico.

Este incidente, que afectó a los tres centros médicos, consistió en un ciberataque con ransomware que expuso la falta de inversión en ciberseguridad en el sector salud. Dicho ataque, que incluyó el cifrado de datos y la posible exfiltración de información, interrumpió las operaciones y afectó la atención a pacientes. Expertos señalan la creciente amenaza del ransomware como servicio (RaaS) y la vulnerabilidad del factor humano como factores clave en este tipo de incidentes.

La recuperación se complicó debido a la dificultad para descifrar los datos sin pagar el rescate, lo cual provocó retrasos en diagnósticos y tratamientos. Esto evidencia la necesidad de invertir en actualizaciones de seguridad, sistemas avanzados de protección, capacitación del personal y concientización sobre las mejores prácticas para evitar este tipo de ciberataques. (Innovación Digital 360, 2025; Forbes Argentina, 2024)

10.4. Análisis y consideraciones

Los casos detallados evidencian la magnitud del desafío que representa el cibercrimen en Argentina, especialmente para los sectores críticos del Estado y los servicios esenciales. La variedad de actores afectados: organismos gubernamentales, prestadores de salud, empresas de telecomunicaciones, demuestra que el riesgo es transversal y creciente.

La experiencia argentina refuerza la necesidad de fortalecer las capacidades institucionales para prevenir y responder ante incidentes cibernéticos. Esto requiere no solo infraestructura técnica, sino también protocolos normativos claros, capacitación continua y marcos de cooperación interinstitucional.

Además, se vuelve imperativo establecer canales efectivos de coordinación entre el sector público y privado, con mecanismos de intercambio seguro de información, y políticas públicas que integren una visión integral de la ciberseguridad nacional.

Capítulo XI. Propuesta de Modelo de Integración de la Ciberseguridad en las Políticas Públicas de Argentina

11.1. Introducción

Argentina ha avanzado en la construcción de un andamiaje institucional y normativo en materia de ciberseguridad. No obstante, este desarrollo se caracteriza por una notable dispersión normativa, una implementación desigual y dificultades persistentes en la articulación entre actores clave. Frente a un escenario de amenazas crecientes, dinámicas y transnacionales, la necesidad de fortalecer el enfoque estratégico, preventivo y transversal en la política pública de ciberseguridad resulta impostergable.

Este capítulo propone un modelo de integración que parte de los avances existentes, pero plantea mejoras concretas para consolidar un enfoque coordinado, eficaz y centrado en la ciudadanía digital, que responda de manera ágil a los desafíos tecnológicos emergentes y que incorpore una perspectiva multidimensional, incluyendo la protección de derechos digitales y la cooperación internacional.

11.2. Gobernanza: Fortalecimiento y ampliación del Comité Nacional de Ciberseguridad

Desde el año 2017, Argentina cuenta con el Comité Nacional de Ciberseguridad, creado por el Decreto N.º 577/2017. Este órgano fue concebido como instancia de coordinación para la elaboración y seguimiento de la Estrategia Nacional de Ciberseguridad. Sin embargo, su integración actual se limita a organismos estatales, sin participación formal de actores del sector privado, académico o de la sociedad civil.

Se propone ampliar su composición, incorporando representantes de estos sectores estratégicos, y establecer subcomités temáticos que operen con criterios técnicos y autonomía operativa. Además, se recomienda definir mandatos claros y roles específicos dentro del Comité para mejorar la eficiencia de la toma de decisiones.

Asimismo, sería valioso implementar mecanismos de rendición de cuentas y transparencia pública sobre sus decisiones, informes y líneas de acción, para generar confianza en su funcionamiento y fortalecer la legitimidad institucional (Gobierno de Argentina, 2017; Gobierno de Argentina, 2023).

Para asegurar un seguimiento efectivo, se sugiere establecer reuniones periódicas obligatorias y un calendario anual de trabajo, acompañado de reportes públicos semestrales que informen sobre avances y desafíos. La incorporación de una plataforma digital de comunicación y gestión colaborativa entre miembros podría optimizar la coordinación y el flujo de información.

Finalmente, para incentivar la participación activa y el compromiso multisectorial, es recomendable diseñar mecanismos de incentivos para el sector privado y académico, tales como reconocimiento público, beneficios fiscales o participación en programas conjuntos de investigación y desarrollo.

11.3. Marco normativo: Integración, actualización y enfoque transversal

El marco normativo argentino en materia de ciberseguridad presenta un desarrollo progresivo pero disperso. Existen normas relevantes como la Ley 25.326 de Protección de Datos Personales, la Ley 26.388 sobre delitos informáticos, la Ley 26.904 que penaliza el grooming, y la Ley 27.411 que aprueba el Convenio de Budapest sobre ciberdelito. También se destacan resoluciones administrativas como la 641/2021, que establece requisitos mínimos de seguridad de la información en organismos públicos, y la 1291/2019 que crea la Unidad 24/7 para delitos informáticos.

Aunque estos instrumentos representan avances significativos, se propone avanzar hacia un marco normativo integral y dinámico que unifique criterios, incorpore nuevas figuras delictivas emergentes (como ransomware, deepfakes o ataques a infraestructuras críticas), y contemple herramientas de prevención, respuesta y reparación.

Además, debería contemplar obligaciones claras para la cooperación público-privada, así como mecanismos ágiles de actualización normativa frente a los cambios

tecnológicos constantes (Congreso de la Nación Argentina, 2008; Congreso de la Nación Argentina, 2013; Boletín Oficial de la República Argentina, 2017; Argentina. Jefatura de Gabinete de Ministros, 2021; Ministerio de Justicia y Derechos Humanos de la Nación, 2019).

Para ello, se recomienda la creación de una comisión permanente de revisión normativa que pueda proponer modificaciones legislativas o reglamentarias con celeridad, asegurando la adaptación a nuevas amenazas y tecnologías.

Asimismo, se propone incorporar de forma explícita en la normativa nacional los estándares internacionales ISO/IEC 27001, que establece requisitos para los sistemas de gestión de la seguridad de la información (SGSI), y su extensión ISO/IEC 27701, orientada a la gestión de la privacidad de la información. La implementación de estos estándares permite establecer procesos estructurados, medibles y auditables que fortalecen la protección de los activos de información, facilitan la interoperabilidad con sistemas internacionales, y aumentan la confianza de los ciudadanos y actores privados en los sistemas institucionales.

Su adopción puede promoverse mediante programas de certificación, incentivos regulatorios, asistencia técnica y la exigencia de su aplicación progresiva en organismos públicos y sectores críticos (ISO/IEC, 2022).

Además, se sugiere incluir cláusulas específicas sobre la protección de los derechos humanos digitales, en línea con los estándares internacionales en privacidad, acceso a la información y libertad de expresión en entornos digitales.

Tal como se desarrolló en capítulos anteriores, la limitada adopción de estándares internacionales como ISO/IEC 27001 en organismos estatales ha tenido consecuencias concretas en términos de vulnerabilidad institucional. Casos recientes, como el ataque al sistema Mi Argentina, evidencian la necesidad de avanzar hacia una política normativa integral que promueva la estandarización, la auditoría de procesos y la gestión proactiva del riesgo digital en todo el aparato estatal (Actualidad Esquina, 2024).

11.4. Cultura y capacitación: Propuesta de una Estrategia Nacional de Formación en Seguridad Digital

En Argentina existen iniciativas valiosas en materia de formación y concientización digital, aunque de manera fragmentada y no siempre articulada entre sí. La Fundación Dr. Manuel Sadosky, por ejemplo, desarrolla el programa Program.AR, que introduce contenidos sobre seguridad digital básica en contextos educativos formales y no formales (Fundación Dr. Manuel Sadosky, 2023). Por su parte, organizaciones de la sociedad civil como Argentina Cibersegura llevan adelante campañas dirigidas a adolescentes y jóvenes con recursos didácticos y actividades de sensibilización (Argentina Cibersegura, 2023). A nivel estatal, el Ministerio de Seguridad ha impulsado acciones como “Pará, pensá, conectate”, orientadas a la concientización general (Ministerio de Seguridad de la Nación, 2023).

Si bien estas experiencias resultan fundamentales, su alcance es limitado, carecen de continuidad en el tiempo y no están integradas bajo una estrategia nacional común. Por ello, este trabajo propone diseñar e implementar una Estrategia Nacional de Capacitación y Cultura en Ciberseguridad, entendida como una política pública transversal, sostenida y multisectorial.

Esta estrategia debería contemplar la incorporación progresiva de contenidos de ciberseguridad en los distintos niveles del sistema educativo formal, el desarrollo de programas de formación continua para trabajadores del sector público, campañas de concientización dirigidas a diversos sectores sociales, y el establecimiento de alianzas entre el Estado, las universidades, el sector privado y organizaciones de la sociedad civil.

Se recomienda establecer metas concretas para la implementación, por ejemplo: inclusión curricular en educación formal en un plazo de 3 años, programas regulares de actualización para funcionarios públicos a partir del primer año, y campañas masivas anuales con evaluación de impacto.

La propuesta se orienta a construir una cultura digital preventiva y democrática, fortaleciendo las capacidades ciudadanas para convivir en entornos digitales seguros,

y fomentando una ética de responsabilidad compartida entre usuarios, instituciones y empresas.

Además, es esencial promover la inclusión digital, asegurando que los contenidos y acciones estén adaptados a diversos niveles socioeconómicos y regiones geográficas, evitando la ampliación de brechas digitales.

11.5. Seguimiento y evaluación: Creación de un Observatorio Nacional de Ciberseguridad

Un aspecto crítico de la política de ciberseguridad en Argentina es la escasa evaluación sistemática de sus resultados. Si bien se publican informes sobre incidentes a través del CERT.ar y existen diagnósticos puntuales, no hay una entidad con mandato específico para monitorear el cumplimiento de los objetivos estratégicos ni para evaluar su impacto.

Se propone la creación de un Observatorio Nacional de Ciberseguridad, de carácter multisectorial, que produzca información pública, sistemática y accesible sobre amenazas, brechas, avances normativos, recursos humanos capacitados y niveles de cultura digital. Este organismo permitiría orientar decisiones, identificar prioridades y mejorar la transparencia de las acciones estatales.

El Observatorio deberá contar con indicadores claros y estandarizados para medir el desempeño de la política pública en ciberseguridad, tales como:

- Número y tipo de incidentes reportados y mitigados.
- Nivel de cumplimiento normativo en organismos públicos y privados.
- Porcentaje de la población con formación básica en ciberseguridad.
- Tiempo promedio de respuesta ante incidentes críticos.
- Grado de articulación multisectorial y participación ciudadana.
- Avances en actualización normativa y tecnológica.

Se recomienda fijar un calendario anual de publicación de informes públicos y sesiones de consulta abiertas con la sociedad civil y actores privados.

Asimismo, el Observatorio podría facilitar espacios de capacitación y talleres de actualización para distintos sectores, además de ser un puente para la cooperación internacional en ciberseguridad.

Finalmente, se sugiere que su constitución incluya una fase piloto de implementación dentro del primer año, con evaluación de resultados al término del segundo año para realizar ajustes y consolidar su rol estratégico.

CONCLUSIONES

Esta investigación ha analizado la ciberseguridad como un pilar de la seguridad ciudadana en Argentina, explorando su complejidad como un campo que trasciende lo técnico para convertirse en un desafío político, normativo y social.

Los hallazgos revelan que, a pesar de avances significativos, como la Ley 26.388 y la Segunda Estrategia Nacional de Ciberseguridad (2023), persisten obstáculos estructurales: la fragmentación institucional entre ministerios y organismos, la escasez de recursos humanos y tecnológicos, y la falta de una visión integral que conecte la seguridad digital con los derechos de los ciudadanos. Este diagnóstico pone en evidencia una desconexión entre las iniciativas estatales —a menudo reactivas y sectoriales— y la necesidad de un proyecto colectivo que posicione a la ciberseguridad como un componente esencial de la democracia digital.

En respuesta a estos desafíos, se propone la creación de un Observatorio Nacional de Ciberseguridad, un modelo diseñado para articular esfuerzos interinstitucionales, promover la alfabetización digital y fortalecer la cooperación público-privada y regional. Este enfoque no busca blindar sistemas, sino construir vínculos entre actores, visibilizar riesgos y anticipar amenazas, entendiendo los ciberdelitos—, acciones ilícitas en el ciberespacio —como expresiones de desigualdades estructurales que requieren soluciones integrales. La comparación con Brasil y México refuerza esta perspectiva, al mostrar que las debilidades argentinas son parte de una problemática regional, pero también que existen oportunidades para aprendizajes cruzados y estrategias situadas. La relevancia de esta propuesta radica en su capacidad para transformar la ciberseguridad en un proceso colectivo, inclusivo y orientado a la equidad.

Como reflexión final, este trabajo no pretende clausurar el debate, sino abrirlo a nuevos interrogantes. La ciberseguridad, como política pública, debe superar su carácter tecnocrático para convertirse en un espacio de deliberación pública, donde la tecnología se encuentre al servicio de una sociedad más justa y democrática. Para ello, se requiere una acción sostenida: inversión en formación, infraestructura y campañas de concientización, así como una vigilancia permanente para adaptar las

políticas a un entorno digital en constante cambio. Esta tesis, desde su perspectiva autoral, aspira a contribuir a ese proceso, con la convicción de que un entorno digital seguro es inseparable de un proyecto de país que prioriza la inclusión, la participación y los derechos de sus ciudadanos.

Finalmente, se destaca que la propuesta de modelo integral presentada en esta tesis —basada en el fortalecimiento del Comité Nacional de Ciberseguridad, un marco normativo actualizado, una estrategia nacional de formación y un Observatorio de Ciberseguridad— constituye un punto de partida viable y adaptable. Este modelo busca superar la fragmentación actual mediante una estructura coordinada, transparente y participativa, que promueva la corresponsabilidad entre el Estado, el sector privado, la academia y la sociedad civil. Sólo a través de esta sinergia será posible garantizar la soberanía tecnológica, proteger los derechos fundamentales y consolidar una ciudadanía digital activa y resiliente.

A este contexto debe sumarse el impacto económico que tienen los incidentes cibernéticos. En América Latina, el costo promedio de una filtración de datos supera los 3.5 millones de dólares, y más del 70% de las empresas argentinas no cuenta con protocolos eficaces de respuesta ante incidentes. Este escenario expone la urgencia de adoptar estándares internacionales como la norma ISO/IEC 27001, no simplemente como un estándar técnico, sino como una estrategia nacional para proteger la infraestructura crítica, garantizar derechos digitales y reforzar la confianza institucional (Actualidad Esquina, 2024).

REFERENCIAS BIBLIOGRÁFICAS

- Actualidad Esquina. (2024, diciembre 26). *Ciberseguridad en crisis: el hackeo a Mi Argentina expone las falencias del país y la necesidad de estándares internacionales*. https://actualidadesquina.com.ar/ciberseguridad-en-crisis-el-hackeo-a-mi-argentina-expone-las-falencias-del-pais-y-la-necesidad-de-estandares-internacionales/

- Ámbito. (2025). *Bajó el nivel de peligro de ciberataques en Argentina*. https://www.ambito.com/tecnologia/aumento-el-nivel-peligro-ciberataques-argentina-n5981756

- Argentina. Dirección Nacional de Ciberseguridad. (2021). *Disposición 7/2021 - Dirección Nacional de Ciberseguridad*. https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-7-2021-353181/texto

- Argentina. Jefatura de Gabinete de Ministros. (2021). *Decisión Administrativa 641/2021 - Requisitos mínimos de seguridad de la información para organismos*. https://servicios.infoleg.gob.ar/infolegInternet/anexos/350000-354999/351345/norma.htm

- Argentina. Congreso de la Nación. (2013). *Ley 26.904. Modificación del Código Penal sobre delitos contra la integridad sexual (Grooming)*. https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=223586

- Argentina. Congreso de la Nación. (2008). *Ley 26.388. Delitos informáticos*. https://servicios.infoleg.gob.ar/infolegInternet/verNorma.do?id=141790

- Argentina Cibersegura. (2023). *#EnVosEs: Campaña para adolescentes y jóvenes*. https://www.argentinacibersegura.org/en-vos-es

- Avast. (s.f.). *¿Qué es el ransomware Sodinokibi?* Avast. https://www.avast.com/es-ar/business/resources/what-is-sodinokibi-ransomware#pc

- Barclay, S. (2024). *An analysis of the Global Cybersecurity Index (GCI) 2024: Progress, challenges, and opportunities for cybersecurity*. International Telecommunications Union. https://www.researchgate.net/publication/385417927_An_Analysis_of_the_Global_Cybersecurity_Index_GCI_2024_Progress_Challenges_and_Opportunities_for_Cybersecurity_in_the_Caribbean

- Banco Mundial. (2024). *De la ficción a la realidad: cómo América Latina se convirtió en el campo de batalla cibernético más crítico del mundo*. https://blogs.worldbank.org/es/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe?

- Banco Interamericano de Desarrollo (BID) & Organización de los Estados Americanos (OEA). (2020). *Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe*. https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

- Boletín Oficial de la República Argentina. (2017). *Ley 27.411. Convenio sobre ciberdelito*. https://www.boletinoficial.gob.ar/detalleAviso/primera/176168/20171215

- CEPAL. (2020). *La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad (Boletín 382)*. https://repositorio.cepal.org/server/api/core/bitstreams/6727e17b-6ebc-4544-b8cf-5f859a45fa28/content

- CEPAL. (2022). *Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe*. https://www.cepal.org/es/publicaciones/48065-ciberseguridad-cadenas-suministros-inteligentes-america-latina-caribe

- CERT.ar. (2023). *Incidentes informáticos - Informe Anual de Incidentes de Seguridad registrados en el 2023*. https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/informes-de-la-direccion-7

- Conde, M. (2023, 17 de febrero). *Nuevas herramientas contra el ciberdelito*. ANCCOM. https://anccom.sociales.uba.ar/2023/02/17/nuevas-herramientas-contra-el-ciberdelito/

- Consejo de Europa. (2023, febrero 16). *Argentina firma el Segundo Protocolo Adicional sobre obtención de pruebas electrónicas*. https://www.coe.int/es/web/portal/-/convenio-sobre-ciberdelincuencia-argentina-firma-el-protocolo-sobre-divulgaci%C3%B3n-de-pruebas-electr%C3%B3nicas

- El País. (2024, 2 de septiembre). *Los cybercirujas: el movimiento que desafía el usar y tirar de la tecnología en Argentina*. https://elpais.com/america-futura/2024-09-02/los-cybercirujas-el-movimiento-que-desafia-el-usar-y-tirar-de-la-tecnologia-en-argentina.html

- Forbes Argentina. (2024). *Tras hackeos a centros médicos Grupo Rossi, especialistas alertan falta de inversión en ciberseguridad del sector salud*. Forbes Argentina. https://www.forbesargentina.com/innovacion/tras-hackeos-centros-medicos-grupo-rossi-especialistas-alertan-falta-inversion-ciberseguridad-sector-salud-n63802: https://www.forbesargentina.com/innovacion/tras-hackeos-centros-medicos-grupo-rossi-especialistas-alertan-falta-inversion-ciberseguridad-sector-salud-n63802

- Fortinet. (2023). *Argentina fue el objetivo de más de 10.000 millones de intentos de ciberataques en 2022*. CanalAR. https://www.canal-ar.com.ar/30830-Fortinet-Argentina-fue-el-objetivo-de-mas-de-10-000-millones-de-intentos-de-ciberataques-en-2022.html

- Fundación Dr. Manuel Sadosky. (2023). *Program.AR: Introducción a la computación y la seguridad digital*. https://fundacionsadosky.org.ar

- Gobierno de Argentina. (2017). *Decreto N° 577/2017 - Creación del Comité Nacional de Ciberseguridad*. Boletín Oficial de la República Argentina. https://www.boletinoficial.gob.ar/detalleAviso/primera/168225/20230923

- Gobierno de Argentina. (2018). *Ley N° 27.444 - Simplificación y Desburocratización*. Boletín Oficial de la República Argentina. https://www.argentina.gob.ar/normativa/nacional/ley-27444-2018-311587

- Gobierno de Argentina. (2023, septiembre 28). *Se aprobó la Segunda Estrategia Nacional de Ciberseguridad*. https://www.argentina.gob.ar/noticias/se-aprobo-la-segunda-estrategia-nacional-de-ciberseguridad

- Gobierno de Argentina. (2023). *Segunda Estrategia Nacional de Ciberseguridad*. https://www.argentina.gob.ar/sites/default/files/2023/06/consulta_publica_segunda_estrategia.pdf

- Harán, J. M. (2023, 12 de junio). *Ransomware Medusa ataca a la Comisión Nacional de Valores de Argentina*. WeLiveSecurity. https://www.welivesecurity.com/la-es/2023/06/12/ransomware-medusa-ataca-comision-nacional-valores-argentina/

- INCIBE. (2021). *Glosario de Ciberseguridad.* https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

- Infobae. (2020, 5 de septiembre). *Quiénes están detrás del hackeo a Migraciones y cómo funciona NetWalker, el software malicioso utilizado.* Infobae. https://www.infobae.com/tecno/2020/09/05/quienes-estan-detras-del-hackeo-a-migraciones-y-como-funciona-netwalker-el-software-malicioso-utilizado

- Infoleg. (2000). *Ley N° 25.326 - Protección de Datos Personales*. https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

- Innovación Digital 360. (2025). *Ciberseguridad en Argentina: actualidad, leyes y delitos*. https://www.innovaciondigital360.com/cyber-security/ciberseguridad-en-argentina-actualidad-leyes-y-delitos/

- ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* International Organization for Standardization. https://www.iso.org/standard/27001

- ISO/IEC. (2019). *ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.* International Organization for Standardization. https://www.iso.org/standard/71670.html

- Lara, J. C. (2024). *Ciberseguridad en América Latina: Estrategias nacionales en 2024*. Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/DD_CYRILLA_ESP_2024.pdf

- LV12. (2020). *El 2020 será recordado como el año de los ciberataques*. https://www.lv12.com.ar/ciberataques/el-2020-sera-recordado-como-el-ano-los-ciberataques-n85599

- Ministerio de Desarrollo Productivo. (2023). *Ciberseguridad para PyMEs*. https://www.argentina.gob.ar/ciberseguridad-para-pymes

- Ministerio de Justicia y Derechos Humanos de la Nación. (2019). *Resolución 1291/2019: Creación de la Unidad 24/7 de Delitos Informáticos y Evidencia Digital*. https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-1291-2019-332246

- Ministerio de Seguridad de la Nación. (2023). *Pará, pensá, conectate. Campaña federal de concientización en ciberseguridad*. https://www.argentina.gob.ar/seguridad/ciberdelito/para-pensa-conectate-argentina

- Ministerio de Seguridad de la Nación. (2023). *Resolución 44/2023: Programa nacional de concientización en ciberseguridad*. https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-44-2023-389245

- Ministerio Público Fiscal de Salta. (2021, 29 de marzo). *Ciberdelitos: La evidencia digital como cambio de paradigma en la investigación*. https://www.fiscalespenalesalta.gob.ar/ciberdelitos-la-evidencia-digital-como-cambio-de-paradigma-en-la-investigacion/

- NordVPN. (s.f.). *¿Qué es NetWalker? Definición del ransomware NetWalker.* NordVPN. https://nordvpn.com/es/cybersecurity/glossary/netwalker-ransomware

- NordVPN. (s.f.). ¿Qué es Zero Day*? Definición del ataque de día cer*o. NordVPN. https://nordvpn.com/es/cybersecurity/glossary/zero-day

- OCEDIC. (2022). *Segundo Protocolo Adicional de la Convención de Budapest*. https://ocedic.com/segundo-protocolo-adicional-de-la-convencion-de-budapest/

- RePro Digital. (2024). *Argentina, sede de ciberataques: Recomendaciones sobre cómo prevenirlos*. https://reprodigital.com.ar/nota/902/argentina_sede_de_ciberataques_recomendaciones_sobre_como_prevenirlos

- Saín, G. (2018). La informática jurídica, el derecho informático y el cibercrimen. En R. Parada & J. D. Errecaborde (Comps.), *Cibercrimen y delitos informáticos*. Buenos Aires, Erreius. https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

- Saín, G., Carnaghi, C., & Wierzbinsky, K. (2021). *Ciberdelitos durante la pandemia del COVID-19 en Argentina: Informe de denuncias judiciales y modalidades frecuentes 2020–2021*. Dirección Nacional de Política Criminal.

https://www.argentina.gob.ar/sites/default/files/2020/11/informe_sobre_ciberdelitos_en_pandemia_en_argentina_2020-2021.pdf

- SMARTFENSE. (2023). *Plataforma de concientización en ciberseguridad*. https://smartfense.com/es-ar/plataforma-para-la-concientizacion-en-ciberseguridad

- Telecom Argentina. (2024). *Información de Telecom sobre situación de ciberseguridad.* https://institucional.telecom.com.ar/prensa/noticias/nota/informacion-de-telecom-sobre-situacion-de-ciberseguridad/415

- TEDIC. (s.f.). *Declaración sobre ciberseguridad en América Latina*. https://www.tedic.org/declaracion-sobre-ciberseguridad-en-america-latina/

BIBLIOGRAFÍA METODOLÓGICA

- Giró, Juan. (2022). *Guía para la Elaboración de una Tesis*. Editorial Líbryco, 2ª Edición.

- Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (1991). *Metodología de la investigación*. México: Ed. McGraw.

- Sabino, C. (1998). *Cómo hacer una tesis* (Ed. ampliada). Editorial Lumen.

- Universidad Siglo 21. (2024). *Taller de metodología para el trabajo final: Material de clase*. Especialización en Cibercrimen.

GLOSARIO DE TÉRMINOS

Denegación de Servicio (DoS): Ataque dirigido a un sistema, aplicación o dispositivo con el fin de dejarlo fuera de servicio mediante la saturación de peticiones, impidiendo el acceso legítimo a los recursos del sistema (INCIBE, 2021).

Malware: Programa malicioso cuya funcionalidad es secuestrar un dispositivo o la información contenida en él. En sus inicios afectaba al equipo completo, pero actualmente suele centrarse en la información, cifrándola y exigiendo un rescate para su liberación (INCIBE, 2021).

Medusa: Grupo de ransomware cuya actividad se intensificó en 2023. Se caracteriza por extorsionar a sus víctimas mediante la publicación de información robada en su sitio en la red Tor. Opera cifrando archivos en los sistemas comprometidos —cambiando sus extensiones por *.MEDUSA*— y dejando una nota de rescate bajo el nombre "!!!READ_ME_MEDUSA!!!.txt". Exige pagos para recuperar los datos y evitar su divulgación pública, con opciones adicionales como extender el plazo o eliminar los datos robados. Ha afectado organismos públicos y privados de diversos sectores en Argentina, Bolivia, Brasil, Chile, Colombia y República Dominicana (Harán, 2023).

Netwalker: Ransomware que cifra los datos de las víctimas, exigiendo un pago a cambio de la clave de descifrado. Se dirige a empresas y organizaciones, explotando vulnerabilidades de acceso remoto o utilizando correos electrónicos de phishing. Puede propagarse por la red interna, cifrando unidades locales y compartidas (NordVPN, s.f.).

Phishing: Técnica de ingeniería social en la que un atacante suplanta una entidad legítima mediante correos electrónicos o mensajes para engañar a la víctima y obtener credenciales, información personal o financiera. Suele incluir enlaces a sitios falsificados que imitan a los originales (INCIBE, 2021).

REvil (Sodinokibi) : Ransomware que funciona bajo el modelo *Ransomware as a Service* (RaaS), distribuido principalmente a través de phishing. Afecta a grandes organizaciones y figuras públicas, buscando tanto el cobro de rescates como el

daño reputacional. El modelo RaaS facilita su expansión mediante la colaboración entre desarrolladores y afiliados (Avast, s.f.).

Zero-Day (0-day o día cero): Vulnerabilidad no descubierta por los desarrolladores y, por lo tanto, no corregida. Los cibercriminales aprovechan estas fallas antes de que se implementen parches de seguridad. Casos emblemáticos son el gusano *Stuxnet* y el ataque a Sony en 2014 (NordVPN, s.f.).