Paakat
Revista de tecnología y sociedad

PAAKAT: Revista de Tecnología y Sociedad
e-ISSN: 2007-3607
Centro Universitario de Guadalajara

Universidad de Guadalajara
México
paakat@cugdl.udg.mx

Año 15, número 28, marzo – agosto 2025

¿Qué necesita una ley de ciberseguridad? Análisis de las propuestas legislativas en México (2019-2023)

Legislative proposals on cybersecurity in Mexico (2019-2023)

Juan Manuel Aguilar Antonio*
https://orcid.org/0000-0002-4686-685X
Centro de Investigaciones sobre América del Norte (CISAN), UNAM

Kate Quechol Maciel**
https://orcid.org/0009-0008-9072-4905
Universidad Autónoma de las Américas de Puebla (UDLAP)

[Recibido: 12/08/2024 - Aceptado para su publicación: 13/01/2025]

DOI: http://dx.doi.org/10.32870/Pk.a15n28.892

Resumen

La investigación analiza las propuestas legislativas en materia de ciberseguridad en México entre 2019 y 2023, partiendo de la hipótesis de que estas iniciativas tienen un enfoque estado-centrista basado en la seguridad nacional y pública, evadiendo principios clave como los derechos humanos, las asociaciones público-privadas, la protección de infraestructuras críticas nacionales, la cooperación en niveles institucional, regional e internacional, y el avance de las tecnologías emergentes. Se identifican y evalúan dieciocho iniciativas, utilizando una metodología cualitativa basada en marcos teóricos de Riza Azmi Tibben, Than Win, Jeff Kossef y Aguilar-Antonio, etc. Además, se utiliza una metodología de minería de texto para analizar el contenido de las propuestas. Los resultados confirman la hipótesis y destacan la necesidad de una legislación holística y coordinada que abarque todos los aspectos de la ciberseguridad.

Palabras clave:
Legislación,
Seguridad Cibernética,
Seguridad Nacional,
Derechos Humanos.

Abstract

The research analyzes legislative proposals on cybersecurity in Mexico from 2019 to 2023, based on the hypothesis that these initiatives have a state-centered approach focused on national and public security, evading key principles such as human rights, public-private partnerships, the protection of national critical infrastructures, cooperation at the institutional, regional, and international levels, and the advancement of emerging technologies. Eighteen initiatives are identified and evaluated using a qualitative methodology based on theoretical frameworks by Riza Azmi Tibben, Than Win, Jeff Kossef, and Juan Manuel Aguilar-Antonio, etc. Additionally, they used a Text Mining methodology is employed to analyze the content of the proposals. The results confirm the hypothesis and highlight the need for holistic and coordinated legislation encompassing all aspects of cybersecurity.

Keywords:
Legislation, Cybersecurity, National Security, Human Rights.

Introducción

La ciberseguridad se ha convertido en un tema de creciente importancia a nivel global, impulsado por el rápido avance de las tecnologías de la información y la comunicación (TIC) y la creciente dependencia de las infraestructuras digitales en todos los ámbitos de la sociedad. México no ha sido ajeno a esta tendencia, y el país ha experimentado un aumento significativo en la cantidad y sofisticación de las amenazas cibernéticas. Estas van desde ataques a infraestructuras críticas hasta incidentes de violación de datos personales y ciberdelincuencia. En respuesta a estos desafíos, el Congreso de la República presentó un total de 18 iniciativas legislativas a nivel federal en la materia entre 2019 y 2023.

La investigación tiene como objetivo analizar las propuestas legislativas en materia de ciberseguridad, partiendo de la hipótesis de que la gran mayoría de iniciativas presentadas tienen un enfoque estado-centrista basado en la seguridad nacional y seguridad pública. Esta perspectiva, aunque crucial, tiende a evadir principios clave necesarios para una legislación, política, estrategia o estándar de ciberseguridad más integral. Los principios incluyen la consideración de los derechos humanos, la promoción de asociaciones público-privadas, la protección de infraestructuras críticas nacionales, la cooperación tanto a nivel institucional, regional e internacional como la adaptación a los avances de las tecnologías emergentes.

El análisis se centra en las dieciocho iniciativas identificadas y evaluadas a través de una metodología cualitativa divida en dos partes. En la primera se hace un análisis de marcos teóricos propuestos por expertos como Riza Azmi Tibben, Than Win, Jeff Kossef y Aguilar-Antonio, entre otros. En la segunda se emplea una metodología de minería de texto para analizar el contenido de las propuestas que tienen el perfil de ley de ciberseguridad, lo cual permite una evaluación más detallada y objetiva de los temas abordados en cada una.

En las conclusiones, la investigación busca demostrar que las iniciativas legislativas en materia de ciberseguridad en México, aunque bien intencionadas, deben evolucionar

hacia un enfoque más holístico e inclusivo. Solo así se podrá garantizar una ciberseguridad robusta y sostenible que proteja no solo la seguridad nacional, sino también los derechos y las libertades de los ciudadanos y la integridad de las infraestructuras críticas del país.

Discusión teórica en torno a una ley de ciberseguridad

Existen múltiples enfoques para la creación de un marco legal en materia de ciberseguridad. Las preguntas centrales que guían la discusión teórica de esta investigación son: ¿qué necesita una ley de ciberseguridad? ¿Qué aspectos hay que tomar en consideración a la hora de redactar una iniciativa legislativa holística que contemple a las partes interesadas para implementar una política nacional de ciberseguridad?

Un primer punto de partida, para responder estas interrogantes, se da a través de métricas internacionales en la materia como el Global Cybersecurity Index (GCI) y el National Cybersecurity Index (NCSI) que ofrecen aportes clave y complementarios para la construcción de una ley o política nacional de ciberseguridad, destacando dimensiones y subindicadores clave que guían estos marcos. En este punto es importante mencionar que es necesario diferenciar la política del marco legislativo. Si bien, ambos conceptos están interrelacionados es necesario indicar que los autores citados en esta sección no necesariamente se centran solo en un concepto, sino que presentan propuestas analíticas que relacionan el marco legislativo con la política nacional de ciberseguridad.

De esta forma el GCI, a través de su dimensión de *Legal Framework*, evalúa la existencia de componentes fundamentales como leyes contra el cibercrimen, normativas de protección de datos y privacidad, legislación para la seguridad de infraestructuras críticas y la regulación de tecnologías emergentes (ITU, 2024). Estos elementos legales son imprescindibles para proporcionar una base jurídica sólida que sustente las políticas de ciberseguridad, permitiendo el cumplimiento efectivo y la protección de ciudadanos e instituciones frente a las amenazas digitales. La legislación no solo responde a los desafíos actuales, sino que establece un marco proactivo para regular el desarrollo tecnológico futuro, otorgando legitimidad y efectividad a cualquier estrategia nacional de ciberseguridad (ITU, 2024).

Por su parte, el NCSI refuerza este enfoque al centrarse en su subindicador de *Cybersecurity Policy*, el cual evalúa aspectos como la existencia de una estrategia nacional de ciberseguridad, la claridad de los objetivos estratégicos, la definición de roles y responsabilidades institucionales y la articulación de medidas específicas para implementar y supervisar la estrategia (e-GAF, 2024). Este subindicador subraya la importancia de contar con una política integral que opere como hoja de ruta para traducir las disposiciones legales en acciones concretas y coordinadas.

Al integrar estas dimensiones, el GCI y el NCSI demuestran cómo las leyes y las políticas no son esfuerzos aislados, sino componentes interdependientes que, cuando se alinean correctamente permiten a los países construir marcos normativos y estratégicos capaces de responder a los complejos desafíos del ciberespacio, asegurando una mayor resiliencia y seguridad cibernética.

En ese sentido, se realizó una revisión de la literatura que incluyó marcos legales (*legal framework*), marcos de trabajo (*frameworks*) y la revisión de iniciativas en materia de ciberseguridad alrededor del mundo. La primera propuesta de interés identificada fue la de Riza Azmi, Tibben y Than Win (2018), quienes analizaron 26 documentos sobre marcos de ciberseguridad que proporcionan, a funcionarios gubernamentales, herramientas para crear leyes o iniciativas legislativas en torno al tema.

Entre sus hallazgos existen siete temas a considerar, que contribuyen en la creación de una iniciativa o ley de ciberseguridad, los cuales son: 1) crear confianza en línea; 2) crear coordinación, cooperación y colaboración entre las partes interesadas o los *stakeholders*; 3) perfilar la política de planeación cibernética del Estado; 4) promover la asimilación e integración de todos los estratos de la sociedad; 5) revisar, adecuar y crear métodos de evaluación de la política de ciberseguridad; 6) establecer un entorno jurídico o marco legal (framework); y 7) crear normas complementarias en la materia.

Los autores identificaron cinco pilares principales que construyen la ciberseguridad en general: 1) el factor humano; 2) el organizativo; 3) la infraestructura crítica; 4) la tecnología; y por último 5) la legislación y reglamentación. Ahora bien, cada contexto requiere un marco de trabajo específico, por ello Riza Azmi, Tibben & Than Win (2018) identificaron diferentes contextos a considerar, los cuales se pueden observar en la Tabla 1.

Tabla 1. Dimensiones de contexto a considerar en la creación de un marco legal o ley de ciberseguridad

Tipo	División	¿En qué consiste?
Acción Promovida	Acción colaborativa	• Estrategia enfocada en el exterior. • Basada en interdependencia positiva. • Promueve la cooperación entre entidades del ciberespacio. • ***Idea central:*** la ciberseguridad es una responsabilidad compartida dados los nuevos retos.

	Acción estratégica	• Estrategia enfocada en lo interno. • Promueve el fortalecimiento interno de la organización mediante la creación de cibercapacidades de las instituciones de gobierno.
El Conductor	Centrado en el riesgo	• La estrategia de ciberseguridad tiene como objetivo minimizar los riesgos causados por las amenazas cibernéticas. • Se debe identificar, evaluar y gestionar los riesgos.
	Centrado en el valor	• La creación de la estrategia de ciberseguridad está impulsada o enmarcada por un determinado valor (o el compromiso/enfoque del país). • El crear una política cibernética significa considerar el ciberespacio no solo como un ámbito aislado, sino también como un ámbito que implica la seguridad política y la estrategia nacional.
Nivel	Nivel organizativo	• Alcance limitado en el ámbito interno de la organización. • Pretende fortalecer la capacidad cibernética de la organización o la infraestructura de información crítica. • El marco puede utilizarse como complemento de un marco de nivel superior. • ***Ejemplo de frameworks*:** Marco NIST y CMM.
	Nivel regional	• Persigue una interdependencia positiva entre el país y sus homólogos regionales. • Suele crearse para responder a las necesidades específicas de los países miembros de una región que comparten valores institucionales similares. • ***Ejemplo*:** Unión Europea (UE) y Organización de los Estados Americanos (OEA)
	Nivel internacional	• Apuntar también a la interdependencia positiva entre el país y el mundo. • Hace hincapié en la cooperación y colaboración con cualquier organismo internacional que tenga los mismos intereses en materia de ciberseguridad.
Audiencia	Público específico	• Principalmente está dedicado y dirigido a organismos e instituciones específicas que comparten valores semejantes a la política cibernética.
	Público general	• Aplicabilidad general en cuanto a la ciudadanía y población. • Centrado en ayudar a las organizaciones a aumentar su capacidad para reducir las ciberamenazas.

		• Puede ser utilizado por cualquier organización pública o privada. • ***Ejemplo:*** ISO/_ Microsoft y BSA

Fuente: elaboración propia con base en Riza Azmi, Tibben & Than Win (2018).

Jeff Kossef (2020) analizó y criticó las constantes dentro de las leyes y *frameworks* de ciberseguridad en Estados Unidos de América. En relación con lo anterior presentó principios rectores, los cuales se advierten en la Tabla 2, los cuales a su criterio permiten crear leyes de ciberseguridad más equipadas para afrontar la naturaleza compleja y cambiante del ciberespacio. Además, se asevera que el influir en las prácticas de ciberseguridad del sector privado es una meta a la que toda estrategia nacional de ciberseguridad debe aspirar, ya sea por medio de educación y asistencia tecnológica, o bien por medio de legislación que regule sus prácticas.

En términos de amenazas específicas en México, Quezada (2022) en el documento *Ciberseguridad, desafío para México y trabajo legislativo* destaca varios aspectos de interés. Por ejemplo, señala que una de las amenazas más prominentes en el país es la falta de protección adecuada de la información. Menciona que en ocasiones la protección de datos se subestima en comparación con la protección del software, creando una brecha que los atacantes pueden explotar en la gestión de datos en un incidente cibernético. Alude a que el GCI resalta la creciente brecha de capacidades cibernéticas entre los países desarrollados y en desarrollo. Por ello, subraya la necesidad de mejorar las habilidades y la infraestructura digital en México para aminorar la brecha y fortalecer la ciberseguridad. También habla de la falta de leyes armoniosas en el ámbito de la ciberseguridad, siendo una preocupación.

La mayoría de los ataques de ciberseguridad se dirigen a las pequeñas y medianas empresas (PyMEs), lo cual pone de manifiesto la necesidad de una regulación efectiva que proteja a estas organizaciones. Aborda cómo la ciberseguridad tiene un impacto en diversos derechos humanos, como el derecho a la vida, la libertad de prensa y la protección de datos personales. Con aquello que señala que la ciberseguridad en México es un desafío multidimensional que requiere una respuesta coordinada de actores gubernamentales, empresariales y la sociedad civil. El fortalecimiento de la infraestructura digital, la promoción de buenas prácticas y la formación de expertos en ciberseguridad son pasos cruciales hacia un entorno cibernético más seguro.

Tabla 2. Principios para la creación de una ley y/o marco legal de ciberseguridad

Principios que cumplir	Implicaciones
Principio de Información	***Objetivo:*** los legisladores deben debatir y promulgar leyes de ciberseguridad respaldadas por la ciencia y redactadas por personas que entiendan las cuestiones políticas y tecnológicas subyacentes. ***Opciones:*** el Congreso podría reactivar la Oficina de Evaluación Tecnológica (OTA), la cual es una unidad dentro del poder legislativo que empleaba a científicos para dotar al Congreso de medios nuevos y eficaces para obtener información competente e imparcial. El Congreso podría crear un nuevo comité permanente sobre ciberseguridad, contratando más personal dentro de ese comité para que aporte su experiencia. Convocar más audiencias para escuchar a expertos en la materia.
Principio de Claridad	***Objetivo:*** existe una necesidad de claridad y especificidad escritas y transmitidas a los legisladores y a la población en los requisitos legales por parte del Estado a empresas privadas, oficinas estatales y a la ciudadanía. ***Fines:*** aumentar la probabilidad de que una empresa invierta en el cumplimiento de las normas. Que las empresas desarrollen políticas y procedimientos detallados de ciberseguridad y formen a su personal. Las leyes de ciberseguridad deben poder adaptarse a las nuevas tecnologías y a las normas del sector en materia de seguridad de los datos.
Principio de Adaptabilidad	***Objetivo:*** la legislación sobre ciberseguridad debe ser capaz de cambiar al mismo ritmo que las amenazas y las medidas defensivas. ***Opciones:*** el Congreso debería promulgar una ley general de seguridad de datos y notificación de violaciones, delegando la autoridad normativa en una agencia experta. Esa agencia tendría autoridad normativa para promulgar requisitos específicos en materia de ciberseguridad. ***Razón:*** no es realista esperar que los legisladores aborden explícitamente tecnologías concretas. Al delegar la autoridad normativa en materia de ciberseguridad el Congreso permitiría la promulgación de normativas que se adapten a las nuevas tecnologías.
Principio de Comprensión	***Objetivo:*** la ciberseguridad debe abordar y cumplir principios de seguridad de la información como la "tríada de la CIA", acrónimo de confidencialidad, integridad y disponibilidad. Para que una ley sea comprensiva debe abordar los tres puntos. ***Tipos de ataques*** ***Confidencialidad:*** incluyen el ataque de información personal, información gubernamental clasificada y secretos comerciales corporativos, etc. ***Integridad:*** implica que no se permitan cambios no autorizados en los datos. ***Disponibilidad:*** se producen cuando los datos o sistemas no están accesibles a los usuarios autorizados cuando se supone que deben.

	Problemas para abordar: en ocasiones las violaciones a la confidencialidad suelen ser necesarias para activar acción por parte de las autoridades, usualmente poniendo en segundo plano la integridad y disponibilidad. La legislación actual se centra en daños financieros, descuidando la protección de secretos comerciales, sitios web públicos, información personal no financiera, pornografía por venganza, *ransomware, deepfakes*, ataques a la democracia y noticias falsas.
Principio de Cohesión	***Objetivo:*** la ley de ciberseguridad debe ser cohesiva en todo el territorio nacional. ***Razón:*** la interconectividad del internet hace complicado cumplir con diferentes regulaciones estatales. Un sitio web con sede en Nueva York, que procesa datos de residentes de todos los estados, debería seguir múltiples leyes de ciberseguridad y privacidad, lo cual resalta la necesidad de regulaciones federales uniformes. ***Meta:*** crear un régimen regulador nacional de la ciberseguridad que garantice exigir responsabilidades a las empresas por incidentes de ciberseguridad.
Principio de Globalidad	***Objetivo:*** Estados Unidos no puede limitarse a confiar en la red existente de leyes contra la ciberdelincuencia como la CFAA, sino que debe utilizar la diplomacia y las alianzas internacionales para presionar a los ciber adversarios para que cesen o reduzcan su comportamiento malicioso. ***Implicaciones:*** colaborar con otros actores regionales e internacionales para la seguridad del ciberespacio.
Principio de Colaboración	***Objetivo:*** la ciberseguridad usualmente está dividida en muchos organismos con diferentes líderes y programas que se encargan de dar forma a la política o estrategia nacional y su aplicación. Sin embargo, siempre que sea posible, las funciones de ciberseguridad deben concentrarse en una agencia para permitir una mejor alineación, tanto entre la normativa como en la cooperación interinstitucional. ***Posible problema:*** las preocupaciones logísticas y pragmáticas pueden impedir la centralización de la ciberseguridad en un único departamento federal, principalmente dado que la información de seguridad nacional debe ser tratada de forma más cuidadosa. ***Opciones:*** los responsables políticos deben procurar coordinar mejor los esfuerzos de ciberseguridad en todo el gobierno. Un modelo para considerar es el equivalente en ciberseguridad del Director de Inteligencia Nacional, una persona encargada de asegurar la cooperación entre instituciones. Se puede promover la gobernanza policéntrica, que es un sistema de gobernanza donde las autoridades de jurisdicciones superpuestas interactúan para determinar las condiciones en las que estas autoridades, así como los ciudadanos sujetos a estas unidades jurisdiccionales, están autorizados a actuar, así como las limitaciones impuestas a sus actividades para fines públicos.

Fuente: elaboración propia con base en Kossef (2020).

Finalmente, Aguilar-Antonio (2020a) destaca la importancia de establecer estándares claros para evaluar los niveles de riesgo cibernético, basados en la Directiva de Política Presidencial de los Estados Unidos de América. Estos niveles de riesgo varían desde la amenaza inminente y de gran escala (Nivel 5), la cual afecta a la infraestructura crítica hasta situaciones con un impacto mínimo en la seguridad pública, la seguridad nacional y la confianza pública (Nivel 1).

Enfatiza que el impacto de los ciberataques se relaciona más con su efecto en áreas críticas como la infraestructura y las libertades civiles que con los medios usados. De esta forma, identifica siete pilares que comparten las estrategias nacionales de ciberseguridad de los miembros y aliados de la Organización del Tratado del Atlántico Norte (OTAN), países de vanguardia en la materia, los cuales son:

1. Considerar el ciberespacio como un componente del poder nacional.
2. Promover el multilateralismo y la cooperación.
3. Utilizar el ciberespacio como instrumento de proyección internacional.
4. Reconocer que la ciberseguridad tiene diferentes dimensiones: civil, militar y estatal.
5. Fomentar la colaboración entre actores estatales y no estatales o privados.
6. Comprender y diferenciar la parte física y virtual del ciberespacio.
7. Reconocer la trascendencia comercial y económica del ciberespacio.

Estos pilares pueden servir como guía para la creación de propuestas legislativas efectivas en ciberseguridad en América Latina. Cabe mencionar que dentro de los artículos existen puntos de coincidencia, en consecuencia, los elementos esenciales identificados para la creación de una de ley de ciberseguridad mucho más completa y consciente de los retos existentes en el ciberespacio son los siguientes cinco puntos:

1. Adopción de una lógica centrada en riesgos.
2. Cohesión legislativa y requerimientos legales específicos dentro del territorio.
3. Coordinación activa entre actores e instituciones que manejan temas de ciberseguridad.
4. Dinamismo que permita no rezagarse ante la evolución de las actividades cibercriminales y el avance de las tecnologías emergentes.
5. Colaboración y regulación del estado con el sector privado, proporcionando estándares mínimos de responsabilidad cibernética.

Es importante mencionar que, hasta este punto de la revisión teórica en torno a iniciativas legislativas o políticas, los artículos revisados no han tratado a profundidad los temas de derechos humanos como un componente trascendental para la elaboración de una ley o política nacional de ciberseguridad. Con lo cual se puede considerar que una fuerte cantidad de la literatura sobre esta temática tiene una perspectiva centrada en la seguridad nacional y en los delitos cibernéticos.

Deibert (2018) expresa que el paradigma de ciberseguridad más comúnmente adoptado es el centrado en el Estado (definido como "Estado céntrico"), el cual prioriza la seguridad nacional por encima de los derechos humanos de los ciudadanos. En contraste, el autor propone un enfoque centrado en el ser humano ("humano céntrico") que aboga por la creación de una arquitectura política de seguridad distribuida, que incorpore mecanismos institucionales de separación de poderes para prevenir abusos a la ciudadanía bajo la justificación de proteger la seguridad nacional.

Esto puede relacionarse al hecho de que la protección del ciberespacio resulta imperativa ante la cantidad de ataques cibernéticos experimentados a nivel mundial por los gobiernos. Ello hace que los creadores de políticas de ciberseguridad prioricen la temática de la seguridad nacional o los delitos cibernéticos. Sin embargo, a la par es importante considerar que esta protección no debe interferir o coartar los derechos humanos de los ciudadanos.

Por lo anterior, fue necesario hacer una búsqueda adicional de literatura en torno a la creación de leyes o políticas nacionales de ciberseguridad que se centraran en la relación entre ciberseguridad y protección de derechos humanos. El primer autor de importancia identificado fue Deibert (2018, quien indica que este enfoque busca salvaguardar a los ciudadanos que conforman la nación en lugar de priorizar la seguridad de la nación en sí misma.

Con esto, estaría por encima la seguridad humana y el resguardo de los derechos de la ciudadanía sobre la seguridad nacional. Bajo este enfoque, el Estado debe ser considerado como una entidad al servicio de la protección de los derechos humanos, incluyendo la seguridad en redes, la censura en internet, la protección de datos personales, la privacidad de los usuarios y la libertad de expresión.

Este argumento se emparenta con el desarrollo de obras teóricas que buscan analizar las relaciones de poder en el internet, donde se da prevalencia en primera instancia a los intereses de los gobiernos y de las corporaciones, delegando la salvaguarda de los derechos de la ciudadanía. Por ejemplo, Rodríguez Prieto y Martínez Cabezudo (2016) expresan que el internet no es una tecnología neutral, sino un espacio donde los gobiernos y corporaciones buscan influir en las personas. De esta forma, consideran necesario construir nuevos marcos conceptuales para transformar las dinámicas de poder y ampliar la participación ciudadana y la democracia en la red.

En concordancia, McChesney (2015) expresa que marcos legales reconocidos a nivel global como la ley SOPA (Stop Online Piracy Act) y CISPA (Cyber Intelligence Sharing and Protection Act) reducen los derechos de los ciudadanos y amplían las incumplibles prerrogativas de la seguridad nacional. Esto se relaciona con lo expresado por Mosco (2017), quien señala necesario transformar los equilibrios de poder en el internet, inclinando la balanza hacía la ciudadanía a razón de que nuevas tecnologías

como el Internet de las Cosas, el Big Data y el Cloud Computing multiplicarán la cantidad de información sensible disponible sobre los ciudadanos en el futuro cercano, con lo cual es necesario reforzar leyes que pongan al centro a los individuos por encima de los gobiernos y de las empresas.

En relación con la vigilancia de los derechos humanos en línea, Pavlova (2020) sugiere asignar mayores recursos económicos para establecer organismos independientes o comisionados con la autoridad para investigar y sancionar a individuos, empresas o entidades gubernamentales que hagan un uso indebido de herramientas en línea y afecten derechos humanos de terceros. Además, aboga porque las empresas privadas pueden desempeñar un papel crucial al informar a sus usuarios sobre posibles ataques y compartir herramientas de higiene digital con la población.

Al reforzar estos argumentos, Shackelford (2017) promueve conceptos como "ciber paz" (*cyber peace*) y la adopción de una gobernanza policéntrica en el ciberespacio. La ciber paz se concibe como un régimen multinivel que persigue la ciberseguridad global al establecer normas que todos los actores del ciberespacio deben seguir, con el fin de reducir conflictos y delitos en este dominio.

Por otro lado, la gobernanza policéntrica se presenta como una alternativa para abordar problemas colectivos por medio del diálogo entre todos los actores afectados. Esto a través de estructuras de gobernanza existentes o creando nuevas como medio para implementar soluciones colectivas. La meta, según el autor, consiste en lograr la cooperación de la mayor cantidad de actores posibles, asegurando así sus sistemas y creando un ecosistema cibernético más seguro para todos. Al abonar a la importancia de la integración y colaboración entre distintos actores, Aguilar Antonio (2022) recalca la necesidad de un "enfoque multistakeholder" en temas de ciberseguridad.

Con base en la revisión de Shackelford (2017), Deibert (2018) y Pavlova (2020) se identificaron que los principales derechos humanos que deberían ser salvaguardados en una propuesta legislativa o una política nacional en materia de ciberseguridad son: 1) La seguridad de las redes; 2) Censura en Internet; 3) Custodia de datos y privacidad; y 4) Libertad de expresión.

Materiales y métodos de investigación

Con la finalidad de identificar el total de iniciativas legislativas en materia de ciberseguridad en el Congreso de México, tanto en la Cámara de Diputados como en la de Senadores, se procedió a realizar una búsqueda en la Gaceta Parlamentaria de ambas cámaras. Se utilizaron técnicas de Dorking[1] en el buscador Google para

identificar los textos de las iniciativas. Del total de iniciativas identificadas se encontraron dieciocho que se pueden observar en la Tabla 3.

Tabla 3. Iniciativas legislativas en materia de ciberseguridad

Nombre del Legislador	Grupo Parlamentario	Nombre de la Propuesta	Año
Alejandra Lagunes Soto Ruíz	Partido Verde Ecologista	Decreto para reformar y adicionar diversas disposiciones del código penal federal en materia de ciberseguridad.	2018
Alejandra Lagunes Soto Ruíz	Partido Verde Ecologista	Proposición para la adhesión de México al convenio sobre la ciberdelincuencia, o convenio de Budapest.	2019
Alejandra Lagunes Soto Ruíz	Partido Verde Ecologista	Iniciativa con proyecto de decreto que declara el mes de octubre como "El mes nacional de la ciberseguridad".	2019
José Salvador Rosas Quintanilla	Partido Acción Nacional	Decreto por el que se reforma el artículo 211 Bis 1 del Código Penal Federal.	2019
Javier Salinas Narváez	Morena	Decreto de reforma constitucional para facultar al congreso de la unión para legislar en materia de ciberseguridad.	2019
María Eugenia Hernández Pérez	Morena	Iniciativa con proyecto de decreto por el que se declara el día 23 de noviembre como “Día Nacional de Ciberseguridad”.	2020
Miguel Ángel Mancera Espinosa	Partido de la Revolución Democrática	Ley General de Ciberseguridad	2020
José Ramón Enríquez Herrera	Morena	Iniciativa con Proyecto de Decreto por el que se adiciona la fracción XIV al Artículo 5 de la Ley de Seguridad Nacional.	2020
Jesús Lucía Trasviña Waldenrath	Morena	Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Ciberseguridad y se derogan diversas disposiciones del Código Penal Federal.	2021
Jesús Lucía Trasviña Waldenrath	Morena	Iniciativa con Proyecto de Decreto para reformar diversos artículos de la Ley General del Sistema Nacional de Seguridad Pública en	2021

		materia de creación de la Comisión Nacional de Ciberseguridad.	
Lidia García Anaya	Morena	Iniciativa con proyecto de decreto por el que se reforma y adiciona una fracción IX al artículo 11 y una fracción VIII al artículo 13 de la Ley de la Fiscalía General de la República en materia de ciberseguridad.	2021
Juanita Guerra Mena	Morena	Adiciona la fracción XXIII del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos en materia de ciberdelincuencia.	2021
Juanita Guerra Mena	Morena	Iniciativa con proyecto de decreto por el que se expide la ley general de ciberseguridad.	2022
María del Rocío Corona Nakamura	Partido Verde Ecologista	Iniciativa con proyecto de decreto por el que se reforma y adiciona el artículo 5 de la ley de seguridad nacional.	2022
María Eugenia Hernández Pérez	Morena	Iniciativa con proyecto de decreto por el que se adiciona la fracción XIV al artículo 5, una fracción VII al artículo 6 y se reforma el artículo 13 de la Ley de Seguridad Nacional.	2022
Caro Cabrera Salvador	Movimiento Ciudadano	Iniciativa con proyecto de decreto por el que se reforman las fracciones XXX y XXXI y se adiciona la fracción XXXII al artículo 73 de la constitución.	2022
Javier López Casarín	Partido Verde Ecologista	Iniciativa con proyecto de decreto por el que se expide la ley federal de ciberseguridad.	2023
Alejandra Lagunes Soto Ruíz, *et al*.	Partido Verde Ecologista	Iniciativa con proyecto de decreto por el que se reforma la fracción XVII, al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos en materia de inteligencia artificial, ciberseguridad y neuroderechos.	2023

Fuente: elaboración propia.

En el ejercicio de identificación de las iniciativas por partido político se encontró que el que presentó más propuestas en la materia fue el Movimiento de Regeneración Nacional (Morena) con un total de nueve, en segunda posición se encontró el Partido Verde Ecologista de México (PVEM) con un total de seis. Por último, partidos como Movimiento Ciudadano (MC), el Partido de la Revolución Democrática (PRD) y el Partido Acción Nacional (PAN) tenían un total de una.

Una segunda labor clave en el análisis de las iniciativas fue el clasificar cuál era la naturaleza de cada proyecto en materia legislativa. Se identificaron al menos cuatro tipos diferentes que a continuación se explican con base en la terminología legislativa (Cámara de Diputados, s.f.):

- Ley: en el régimen constitucional es una disposición votada por el pleno y sancionada por el Ejecutivo, la cual debe ser: justa, bilateral, general, obligatoria y coercitiva.
- Reforma: es el documento mediante el cual se solicita dar un cambio para mejorar, modificar y/o enmendar una ley, un reglamento, un proyecto de ley o un artículo de la Constitución, de una ley o de un reglamento.
- Adición a artículo: es el procedimiento por el que se agrega un texto a una ley, a un reglamento, a un proyecto de ley o a la Constitución Política de los Estados Unidos Mexicanos. En la sesión que se vote en definitiva una proposición o un proyecto de ley se presentarán de manera escrita las propuestas de adición.
- Proyecto de ley: propuesta presentada al pleno para la creación de un nuevo ordenamiento, o modificaciones, reformas, abrogaciones y derogaciones en una ley existente.
- Proposiciones: propuesta con punto de acuerdo en el que se solicita algo en un asunto específico.

A continuación, en la Tabla 4 se presenta la clasificación de las iniciativas de ley según su naturaleza. Destaca que solo que se identificaron cuatro iniciativas concretas para la creación de una ley específica en materia de ciberseguridad, las cuales corresponden a las propuestas de los senadores Lucía Trasviña y Miguel Ángel Mancera y de los diputados Javier López Casarín y Juanita Guerra Mena. En contraste la clasificación que más iniciativas presentó, fue la de reformas con un total de ocho propuestas. Por último, se indica que adición a artículos y proyectos y proposiciones tuvieron un total de seis iniciativas.

Una vez identificadas las fuentes de información se dividió la estrategia de análisis de las iniciativas a través de dos diferentes fases. La primera corresponde a un análisis comparativo de carácter cualitativo a través de las propuestas de Riza Azmi, Tibben y Than Win (2018), Kossef (2020) y Aguilar-Antonio (2020a). Se identificaron los indicadores o elementos que debe contener una ley o estrategia nacional de ciberseguridad y se contrastaron con cada una de las iniciativas.

La segunda correspondió a utilizar la metodología de *Text Mining*, la cual es una rama de la ciencia de datos y procesamiento de lenguaje natural que se enfoca en extraer información valiosa y conocimiento significativo a partir de documentos de texto. El objetivo principal del método fue analizar grandes cantidades de texto para descubrir patrones, tendencias, relaciones y conocimiento en su contenido, lo cual se realizó a través del lenguaje de programación R Studio.

Tabla 4. Clasificación de las iniciativas según su naturaleza

Tipo	Iniciativas
Ley	Miguel Ángel Mancera Espinosa (MME 2020)
	Jesús Lucía Trasviña Waldenrath (LTW 2021)
	Juanita Guerra Mena (JGM 2022)
	Javier López Casarín (JLC 2023)
Reformas	Alejandra Lagunes Soto Ruíz (ALS 2019)
	José Salvador Rosas Quintanilla (SRQ 2019)
	Javier Salinas Narváez (JSN 2019)
	Jesús Lucía Trasviña Waldenrath (LTW 2021)
	Lidia García Anaya (LGA 2021)
	María del Rocío Corona Nakamura (RCN 2022)
	Caro Cabrera Salvador (CCS 2022)
	María Eugenia Hernández Pérez (EHP 2020)
Adición a Artículo	Juanita Guerra Mena (JGM 2022)
	María Eugenia Hernández Pérez (EHP 2020)
	José Ramón Enríque Herrera (REH 2020)
Proyectos y Proposiciones	Alejandra Lagunes Soto Ruíz (ALS 2019)
	Alejandra Lagunes Soto Ruíz 2019 (ALS 2019)
	María Eugenia Hernández Pérez (EHP 2020)

Fuente: elaboración propia.

Análisis y discusión

1. Análisis cualitativo a través de las propuestas de Riza Azmi, Tibben y Than Win (2018), Kossef (2020) y Aguilar-Antonio (2020a)

Para el análisis específico de cada una de las iniciativas en materia legislativa se contemplaron los elementos considerados por las propuestas revisadas en el apartado teórico. Para contrastar las iniciativas con la propuesta de Riza Azmi, Tibben y Than Win (2018) se consideraron cuatro pilares a contemplar en una ley de

ciberseguridad: 1) Acción Promovida; 2) Conductor; 3) Nivel organizacional; y 4) Audiencia a la que va dirigido. A su vez, estos cuatro pilares están subdivididos en un total de nueve variables que deben considerar las iniciativas. Este análisis se presenta en la Tabla 5.

En él se observa que la gran mayoría de las propuestas se centran en la acción estratégica, un total de 14 iniciativas contemplan el fortalecimiento de las capacidades cibernéticas del Estado con un enfoque casi centrado en seguridad pública (combate a los delitos cibernéticos) y seguridad nacional. Sin embargo, esta orientación estratégica a menudo pasa por alto la importancia de la cooperación entre las partes interesadas para una gobernanza del ciberespacio. Esto implica que las legislaciones tienen un enfoque de promover la creación de capacidades cibernéticas al interior de una organización, pero no profundizan en un enfoque colaborativo entre todos los actores necesarios para la construcción de la ciberseguridad del Estado-Nación.

Este enfoque es de reciente promoción por organizaciones como la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés), la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), los cuales hablan de construir modelos de partes interesadas (stakeholders) para una buena gobernanza de la ciberseguridad.

Aguilar Antonio (2020b) ha indicado que los esfuerzos de ciberseguridad en México entre el gobierno, el sector privado y las organizaciones de la sociedad civil no tienen un eje coordinador, por lo cual presentan una situación de descoordinación y atomización de la ciberseguridad. En ese sentido, esto también se refleja en las iniciativas de ley analizadas que no presentan un modelo de coordinación o gobernanza del ciberespacio concreto.

Respecto del enfoque conductor, diez de las propuestas analizadas se centran en abordar riesgos cibernéticos, mientras que ocho se centran en el valor de la ciberseguridad. Esto refleja que están lejos de concebir al ciberespacio como una estrategia que forma parte de una dimensión más compleja como la seguridad nacional o el desarrollo económico.

Es importante mencionar que la reflexión en torno a los riesgos cibernéticos para el Estado y el gobierno se contemplan principalmente en la justificación de las iniciativas. En estas secciones es usual presentar datos concretos en torno a incidentes cibernéticos, número de delitos denunciados en instancias como Instituto Federal de Telecomunicaciones (IFT), Guardia Nacional (GN) o Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF).

Por último, cabe destacar que los marcos de trabajo predominantes se enfocan en el nivel organizacional interno, lo cual descuida la colaboración regional o internacional a través de la diplomacia[2]. Dos aspectos fundamentales para abordar

los desafíos de la ciberseguridad en un mundo interconectado. Y que en métricas como el Global Cybersecurity Index (GCI) de la ITU, o el National Cybersecuriy Index (NCSI) son considerados como indicadores clave al evaluar el aporte de un país a la ciberseguridad global; todo este análisis es visible en la Tabla 5.

Tabla 5. Análisis con base en la propuesta de Riza Azmi, Tibben & Than Win (2018)

		Acción Promovida		Conductor		Nivel Organizacional			Audiencia a la que va dirigido		
	Legisladores	Acción Colaborativa	Acción Estratégica	Centrado en el riesgo	Centrado en valor	Nivel Organizacional	Nivel Regional	Nivel Internacional	Público Específico	Público General	Total
1	ALS (2018)		X	X		X			X		4/9
2	ALS (2019)	X			X	X		X	X		5/9
3	ALS (2019)		X		X	X				X	4/9
4	SRQ (2019)		X	X		X			X		4/9
5	JSN (2019)		X	X	X	X			X		4/9
6	EHP (2020)		X		X	X				X	4/9
7	MME (2020)		X		X	X		X		X	5/9
8	REH (2020)		X	X		X			X		4/9
9	LTW (2021)	X			X	X		X		X	5/9
10	LTW (2021)		X			X	X	X	X		6/9
11	LGA (2021)	X			X	X		X	X		5/9
12	JGM (2021)		X	X		X				X	4/9
13	JGM (2021)		X	X		X				X	4/9
14	RCN (2022)		X	X		X			X		4/9
15	EHP (2022)	X		X		X		X	X		5/9
16	CCS (2022)		X		X	X				X	4/9
17	JLC (2023)		X	X		X		X		X	5/9
18	ALS (2023)		X		X	X				X	4/9
		4	14	10	8	18	1	7	9	9	

Fuente: elaboración propia.

El análisis de la propuesta de Kossef (2020) revela que ninguna propuesta cumplió con todos los principios estipulados. Entre las propuestas evaluadas se observa que el principio de información se aborda en 17, principalmente en la sección de "exposición de motivos". Sin embargo, las propuestas a menudo fallan al proporcionar datos concretos y medidas específicas como la cooperación internacional o requisitos legales para empresas privadas.

Solo nueve de las propuestas obtuvieron el principio de colaboración, lo cual resalta la tendencia en México a relegar la cooperación interinstitucional e internacional a un segundo plano en el ámbito de la ciberseguridad en la visión legislativa. Según Danelyan & Gulyaeva (2020) esta es una problemática a nivel internacional a la hora de legislar en materia de ciberseguridad. Por otra parte, los principios de claridad y comprensión son a menudo ignorados por los legisladores al crear propuestas legislativas, lo que subraya la necesidad de una mayor atención a estos aspectos para garantizar la efectividad de las medidas propuestas.

El aspecto más olvidado es el principio de adaptación, relacionado con crear una política nacional de ciberseguridad dinámica y evolutiva, capaz de mantenerse actualizada para enfrentar los desarrollos de las innovaciones de las amenazas en el ciberespacio, delitos cibernéticos, etc. Del mismo modo, el principio de adaptación se

interrelaciona al impacto de las tecnologías emergentes, tales como Inteligencia Artificial (IA), Cómputo Cuántico, Redes 5G, Internet de las Cosas (IoT) que se interrelacionan con la ciberseguridad.

Se señala que solo dos propuestas cumplieron con seis de los siete principios, la de Miguel Ángel Mancera Espinosa y la de Javier López Casarín, aunque estas no eran del todo claras en delinear o especificarlos. ¿Dónde es más notable esto? Fue en el principio de adaptación, a razón de que hablaban sobre revisar de forma constante la ley, pero no enfatizan cómo mantenerse a la vanguardia con los nuevos desafíos de la ciberseguridad o el avance de las tecnologías emergentes, con lo cual las oraciones no tienen profundidad para considerar que cumplen con este lineamiento.

Por otra parte, el principio de información fue observado en 17 de las propuestas, ello dado que en la sección "exposición de motivos" los legisladores proporcionan información pertinente sobre la importancia de la ciberseguridad en México. No obstante, fallan a la hora de crear propuestas con los datos identificados. Por ejemplo, muchos hablaban de la necesidad de cooperación internacional o de la necesidad de requerimientos legales específicos para empresas privadas. No obstante, no indican qué tipos de estándares serían óptimos para promover en dicho sector, a la par que no especificaron los tipos de instrumentos o acuerdos internacionales en materia de ciberseguridad, a los cuales podría adherirse México en aras de promover la cooperación internacional.

Solo nueve de las propuestas obtuvieron el principio de colaboración, así reforzando la hipótesis de que en México la cooperación interinstitucional e internacional es dejada en segundo plano. Se resalta que los principios de claridad, adaptación y comprensión son los más ignorados por los legisladores a la hora de la creación de una propuesta legislativa de ciberseguridad; todo esto se ve en la Tabla 6.

Tabla 6. Análisis con base en la propuesta de Kossef (2020)

	Legisladores	Información	Claridad	Adaptación	Comprensión	Cohesión	Globalidad	Colaboración	Total
1	ALS (2018)	X			X	X			3/7
2	ALS (2019)	X			X	X	X	X	5/7
3	ALS (2019)	X					X		2/7
4	SRQ (2019)					X			1/7
5	JSN (2019)	X				X	X		3/7
6	EHP (2020)	X					X		2/7
7	MME (2020)	X	X		X	X	X	X	6/7
8	REH (2020)	X				X			2/7

9	LTW (2021)	X	X		X	X	X	X	6/7
10	LTW (2021)	X	X			X	X	X	5/7
11	LGA (2021)	X				X	X		3/7
12	JGM (2021)	X				X			2/7
13	JGM (2021)	X	X			X		X	4/7
14	RCN (2022)	X				X		X	3/7
15	EHP (2022)	X				X	X	X	4/7
16	CCS (2022)	X				X		X	3/7
17	JLC (2023)	X	X		X	X	X	X	6/7
18	ALS (2023)	X				X			2/7
		17	5	0	5	16	10	9	

Fuente: elaboración propia.

En el análisis de la propuesta de Aguilar-Antonio (2020a) resaltan preocupaciones significativas en relación con la percepción y el entendimiento de los legisladores de México en torno al ciberespacio. Un aspecto inicial es que falta una percepción clara del ciberespacio como componente del poder nacional y como instrumento de proyección internacional, lo cual refleja un entendimiento limitado de la importancia del ciberpoder en las relaciones internacionales actualmente. Esto puede explicarse con el hecho de que el análisis de Aguilar-Antonio (2020a) se centra en las Estrategias Nacionales de Ciberseguridad (ENCS) de la OTAN, y México al no ser parte de este organismo no tiene una visión centrada en la seguridad o poder nacional como lo tienen los documentos de los países miembros de esta organización.

Se señala que ocho de las propuestas mencionan la diferencia entre el terreno físico y virtual del ciberespacio, mientras que el resto no abordan el tema. Esto sugiere un desconocimiento sobre cómo regular adecuadamente este entorno, a la par que presenta un tema de importancia fuertemente olvidado, y poco tratado, en varias de las iniciativas legislativas que es la protección de las Infraestructuras Críticas Nacionales (INC).

En tal respecto, se indica que principalmente las iniciativas de ley, como las de Casarín y Mancera, son las que poseen más contenido en torno al tema, sin embargo, carecen de profundidad. Por ejemplo, la iniciativa de Casarín en su Capítulo 5 "Protección de las Infraestructuras Críticas de la Información" especifica que la entidad a cargo de la INC será la Agencia Nacional de Ciberseguridad encargada de identificar y dar lineamientos de qué es una INC, evaluar cuáles deben ser incluidas en un "Catálogo Nacional de Infraestructuras

Críticas" y determinar las obligaciones de los responsables de su protección. También indica que la protección y el resguardo de las INC será un tema de seguridad nacional.

La iniciativa de Miguel Ángel Mancera, en su "Título 3. De la Infraestructura de Información Crítica" aborda el tema de las INC, proponiendo la creación de un Centro Nacional de Ciberseguridad que se coordine con el Instituto Federal de Telecomunicaciones (IFT). Ambas instituciones deberán designar que INC del país puede ser definidas como INC activa y pasiva, establecer un registro nacional y un atlas de infraestructuras críticas nacionales que debe ser actualizado cada año.

Ambas propuestas no presentan lineamientos clave de países como Estados Unidos de América con la Cybersecurity and Critical Infrastructure Agency (CISA), o Canadá con el Public Safety Department que expresan cómo identificar las INC, cuántos y qué tipos de sectores existen para clasificarlas, cómo protegerlas y cómo deben ser las asociaciones público-privadas que creen esquemas de defensa y resiliencia adecuados para su seguridad (Aguilar-Antonio, 2024). Es fundamental destacar la importancia del comercio y la economía digital, así como su impacto en la economía nacional, lo cual también debe ser considerado en una ley o política nacional de ciberseguridad. Reconocer este papel creciente es esencial para el desarrollo de políticas cibernéticas efectivas que equilibren el fortalecimiento de la seguridad pública y nacional con el crecimiento económico.

Por último, se debe mencionar que solo una propuesta hace alusión a una diferenciación de las dimensiones (como pueden ser civil, militar y estatal) de la ciberseguridad. Esto es importante, a razón de que una ley en materia de ciberseguridad debería ser holística y atender a los diferentes sectores nacionales a los cuales debe respaldar. A pesar de esto, es importante mencionar que estas tensiones no están del todo resueltas incluso en países de vanguardia en materia de ciberseguridad, principalmente en las áreas de seguridad nacional y derechos humanos que mantienen fuertes tensiones.

En última instancia se presenta un análisis centrado en los derechos humanos que debería salvaguardar una iniciativa legislativa o política nacional de ciberseguridad derivados de la revisión de los artículos de Shackelford (2017), Deibert (2018) y Pavlova (2020). El primer aspecto importante por mencionar es que el contenido vinculado a derechos humanos en las iniciativas legislativas resulta el más olvidado por los legisladores, tanto de la Cámara de Diputados como de Senadores.

Se indica que, si bien el tópico se aborda de forma conceptual, coyuntural o contextual en varias iniciativas, pocas tienen profundidad de cómo operacionalizar un marco institucional que brinde protección a los derechos humanos de la ciudadanía en el ciberespacio (Papakonstantinou, 2022). En este sentido, se destaca que solo seis propuestas abordan de forma puntual la temática, aunque el contenido no contempla los elementos de los tres autores citados.

Tabla 7. Análisis con base en la propuesta de Aguilar-Antonio (2020a)

	Legisladores	Ciberespacio como componente del poder nacional	Promoción el multilateralismo y la cooperación	Ciberespacio para la proyección internacional	Reconoce las dimensiones (civil, militar y estatal)	Colaboración entre actores estatales y privados	Diferencia entre la parte física y virtual	Trascendencia comercial y económica	Total
1	ALS (2018)						X		1/7
2	ALS (2019)		X			X	X	X	4/7
3	ALS (2019)					X		X	2/7
4	SRQ (2019)								0/7
5	JSN (2019)					X			1/7
6	EHP (2020)								0/7
7	MME (2020)		X			X	X	X	4/7
8	REH (2020)						X		1/7
9	LTW (2021)		X			X	X	X	4/7
10	LTW (2021)		X					X	2/7
11	LGA (2021)		X			X	X		3/7
12	JGM (2021)					X		X	2/7
13	JGM (2021)					X	X		2/7
14	RCN (2022)					X			1/7
15	EHP (2022)	X	X			X		X	4/7
16	CCS (2022)								0/7
17	JLC (2023)		X		X	X	X		4/7
18	ALS (2023)					X			1/7
		1	7	0	1	12	8	7	

Fuente: elaboración propia.

En la Tabla 8 se puede observar que la libertad de expresión es el principal derecho humano al cual se hace alusión en un total de cinco iniciativas legislativas.

Por su parte, respecto del derecho de custodia de datos y privacidad se indica que la mayoría de las iniciativas analizadas en este apartado abordan el tema. Sin embargo, no proveen de ninguna estrategia específica sobre cómo protegerlos y cómo las propuestas legislativas resguardaran las garantías de la ciudadanía.

Tabla 8. Análisis con base en las propuestas de Shackelford (2017), Deibert (2018) y Pavlova (2020)

Legislador	Seguridad en las Redes	Censura en Internet	Custodia de Datos y Privacidad	Libertad de Expresión	Total
SRQ (2019)			**X**		**1/4**
LGA (2021)				**X**	**1/4**
JGM (2021)			**X**		**1/4**
CCS (2022)			**X**		**1/4**
JLC (2023)			**X**	**X**	**2/4**
ALS (2023)			**X**		**¼**

Fuente: elaboración propia.

Al abordar iniciativas legislativas en concreto se podría indicar que la de Salvador Caro Cabrera, Javier López Casarín y Alejandra Lagunes son las que contienen los apartados más amplios en materia de derechos humanos. Respecto de Cabrera, Salvador se indica que el objetivo de su iniciativa es una reforma al artículo 73 de la Constitución para facultar al Congreso para expedir leyes en materia de privacidad, seguridad digital y proteger los derechos humanos en el ciberespacio. Del mismo modo, es importante mencionar que uno de los aspectos eje de esta iniciativa es crear un organismo autónomo que vele por la protección de los derechos humanos y digitales de la ciudadanía. A pesar de que no profundiza en este tópico.

La iniciativa de López Casarín hace alusión a los derechos humanos en su artículo 8, el cual indica que el Estado Mexicano deberá promover la protección de los derechos humanos al momento de la investigación de delitos cibernéticos y resguardar el debido proceso. Y en el artículo 59 expresa que los derechos humanos deben ser respetados al momento de intervención de comunicaciones. No obstante, no profundiza ni sugiere a través de qué mecanismos y qué instituciones velarán por el respeto y garantía de los derechos humanos de la ciudadanía. Con lo cual, a pesar de citar el tema, la iniciativa carece de profundidad.

En el caso de la iniciativa de Alejandra Lagunes, relaciona el avance de las tecnologías emergentes como la IA con el tema de los neuroderechos. De esta forma dedica un apartado completo de los motivos de su iniciativa para presentar y contextualizar este concepto. En él habla sobre cinco neuroderechos, los cuales son: identidad personal, libre albedrío, privacidad mental, acceso equitativo y protección contra los sesgos. Por lo cual propone una reforma al artículo 73 de la Constitución,

en su fracción XVII, donde se faculte al Congreso para legislar en materia de ciberseguridad, IA y neuroderechos.

2. Análisis de Text Mining en R Studio

Culminado el análisis cualitativo a través de las propuestas de los diferentes autores se procedió a complementar la investigación, utilizando la técnica de análisis de minería de texto (conocida en inglés como *Text Mining*). Esta es una disciplina de la minería de datos y procesamiento de lenguaje natural que se enfoca en extraer información valiosa y conocimiento significativo a partir de documentos de texto.

El objetivo principal del método es analizar documentos para descubrir patrones, tendencias, relaciones y conocimiento oculto en su contenido. Entre los principales componentes y técnicas de la minería de texto se encuentran:

- *Preprocesamiento de texto*: antes de realizar cualquier análisis, el texto debe someterse a un proceso de preprocesamiento. Esto incluye tareas como la eliminación de signos de puntuación, números y palabras comunes (*stopwords*), y la conversión del texto a minúsculas. El preprocesamiento asegura que el texto esté limpio y listo para su análisis.
- *Análisis de frecuencia de términos:* se calcula la frecuencia de aparición de cada término en el documento. Esto puede revelar qué términos son más comunes y, por lo tanto, más relevantes.
- Nube de Palabras (*Word Cloud*): se crea una representación visual que muestra las palabras más frecuentes en un documento. Las palabras se presentan en un tamaño proporcional a su frecuencia, lo que facilita la identificación de términos clave.
- Agrupamiento (*Clustering*): se agrupan términos o documentos similares en categorías o clústeres. Esto puede ayudar a identificar temas y relaciones entre los datos.
- *Análisis de Asociación:* se busca la relación y co-ocurrencia de términos en el texto, esto revela conexiones inesperadas entre conceptos.

El análisis de *Text Mining* se hizo a través de R Studio, utilizando las bibliotecas y paquetes tm, wordcloud, ggplot2, dplyr, clúster y RColorBrewer que proporcionan herramientas específicas para procesar, analizar texto y crear visualizaciones de datos como la *Word Cloud*, histogramas y dendrogramas.

En el contexto legislativo, el *Text Mining* es especialmente útil para identificar términos recurrentes en grandes volúmenes de propuestas legales, lo cual permite detectar patrones en las formulaciones legislativas y destacar los conceptos más frecuentes en las iniciativas de ley (Badenes-Olmedo, Redondo-García & Corcho, 2019). También es importante indicar que se analizó la frecuencia de palabras en cada una de las iniciativas de ley.

La *Word Cloud* ayudó a visualizar las palabras más frecuentes. Por otra parte, los dendrogramas fueron utilizados para el análisis de agrupamiento jerárquico con el método de Ward para agrupar términos relacionados en una estructura jerárquica. Esto se visualizó utilizando la función hclust que destaca los grupos utilizando rect.hclust. Además, se realizó un análisis de agrupamiento no jerárquico, utilizando el método average con la función Agnes.

Otra fortaleza del *Text Mining* en textos legislativos es su capacidad para comparar iniciativas de ley relacionadas, identificando semejanzas y diferencias entre ellas mediante algoritmos de agrupamiento y análisis de asociación (Firdhous, 2010). Además, el uso de *Text Mining* en legislaciones multilingües facilita el análisis de documentos en diferentes idiomas mediante técnicas como la creación de jerarquías de conceptos basadas en *sinsets*[3], lo cual permite trabajar con textos legales (Gómez, Blanco, García & Sánchez, 2023).

Es oportuno mencionar que el análisis de *Text Mining* se aplicó a las cuatro iniciativas de ley y a las ocho propuestas de reforma del artículo; también, a las tres de adición de artículo y tres de proyectos de proposiciones. Sin embargo, se identificó que en las categorías de iniciativas legislativas que estaban fuera de proyecto de ley, la metodología de *Text Mining* no era del todo útil a razón de que muchas de estas iniciativas legislativas solo que se concentran en pequeños cambios a fracciones de artículos de la constitución o pequeñas adiciones.

La proyección de las *Word Cloud* o dendrogramas no eran útiles para ver qué conceptos relacionados a ciberseguridad eran los más importantes en este tipo de propuestas. Por esto el análisis se concentró en las cuatro iniciativas de ley, centradas en la creación de una ley de ciberseguridad. Por último, se indica que para contrastar las carencias y áreas de oportunidad de las propuestas de ley mexicanas analizadas en esta investigación, este análisis se aplicó a dos legislaciones de América Latina: 1) la Ley de Ciberseguridad de Chile y la propuesta de Ley de Ciberseguridad de Guatemala, análisis que está en el anexo 1 de esta investigación.

De esta forma, en la Tabla 9 se presenta el filtrado de palabras que se realizó para realizar los productos del análisis de *Text Mining*.

Tabla 9. Palabras filtradas en el texto de cada una de las iniciativas

N°	Nombre del Legislador	Palabras eliminadas
1	Miguel Ángel Mancera Espinosa	"persona", "materia", "general", "conducta", "así", "título", "anterior", "uso", "artículo", "actividades", "deberá", "años", "veces", "unidad", "través", "realización", "momento", "deberán", "vigentes", "usuarias", "ello", "establecer", "sistema", "centro", "millones", "impondrán", "manera", "objeto".
2	Jesús Lucía Trasviña Waldenrath	"unidades", "acciones", "uso", "materia", "ser", "artículo", "cualquier", "mil", "persona", "general", "medio", "años", "medida", "través", "así", "forma", "comisión", "uma", "parte", "México", "personas", "mexicano", "presente", "conforme", "efecto", "sesiones", "capítulo", "tipo", "tal", "caso", "mediante", "mismo", "incluyendo", "país", "medios".
3	Juanita Guerra Mena	"capítulo", "consejo", "siguientes", "humanos", "uso", "deberán", "establecer", "así", "general", "demás", "personas", "presente", "ser", "deberá", "persona", "artículo", "México", "materia".
4	Javier López Casarín	"presente", "través", "cualquier", "veinte", "medio", "México", "mil", "así", "años", "medida", "demás", "uso", "materia", "artículo", "unidades", "establecer", "personas".

Fuente: elaboración propia.

Iniciativa del senador Miguel Ángel Mancera MME (2020)

En el caso de la iniciativa de ley del senador Miguel Ángel Mancera, después del filtrado de palabras que no se relacionaban con ciberseguridad, se identificaron las cuarenta principales palabras dentro del documento. En este se identificó que los conceptos clave son "ciberseguridad" y "nacional". Posteriormente, los demás conceptos que tuvieron mayor peso dentro del análisis fueron "infraestructura", "datos", "personas", "información" y "seguridad".

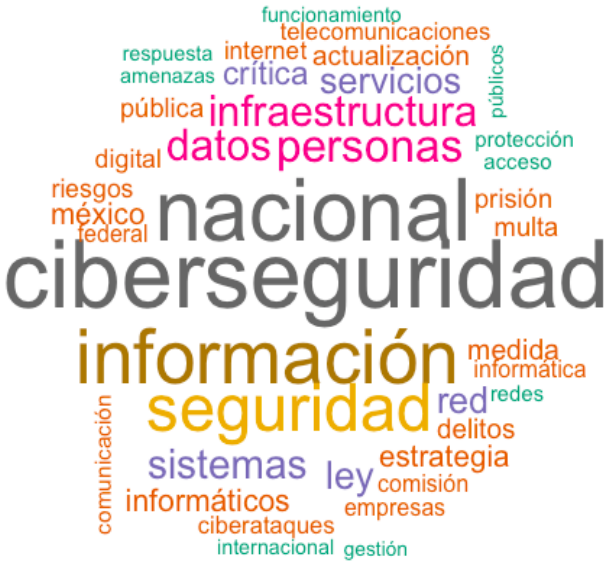
Cabe resaltar la importancia que tuvieron palabras como "prisión", "multa" "amenazas", "ciberataques", "delitos" en el marco de la *Word Cloud* que en complemento con los conceptos señalados en el párrafo anterior nos develan que la iniciativa tiene un fuerte enfoque de ciberseguridad focalizada en temas de seguridad nacional y seguridad pública.

Un aspecto de importancia de esta iniciativa es que dedica una fuerte parte de su contenido al tema de protección de INC, a razón que la palabra "infraestructura" tiene un gran peso dentro de la visualización. Por otra parte, temas como la

protección de derechos humanos y digitales, la importancia de asociaciones público-privadas y la cooperación internacional no se desarrollan a profundidad.

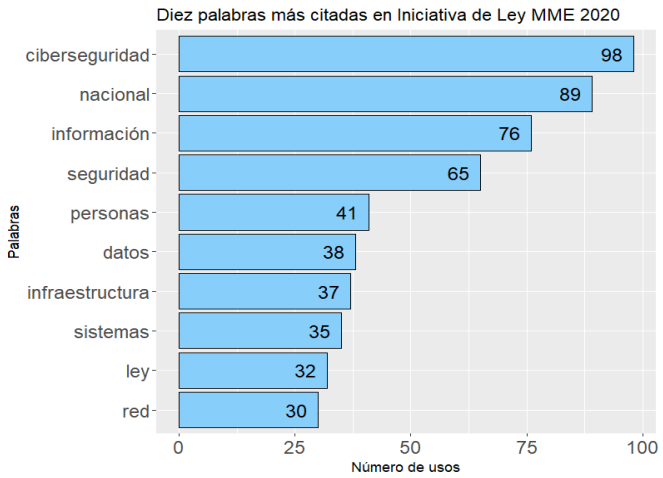
El análisis de las palabras más citadas confirma que la visión de ciberseguridad tiene como centro una noción de seguridad nacional, a razón que las palabras más citadas son "ciberseguridad" con 98 repeticiones, "nacional" con 89 e "información" con 76. A pesar de esto, resaltan conceptos como "personas" (41), "datos" (38) y "sistemas" (35).

Figura 1. *Word Cloud*. Iniciativa Miguel Ángel Mancera MME (2020)



Fuente: elaboración propia.

Figura 2. Diez palabras más citadas en Iniciativa de Ley de MME 2020

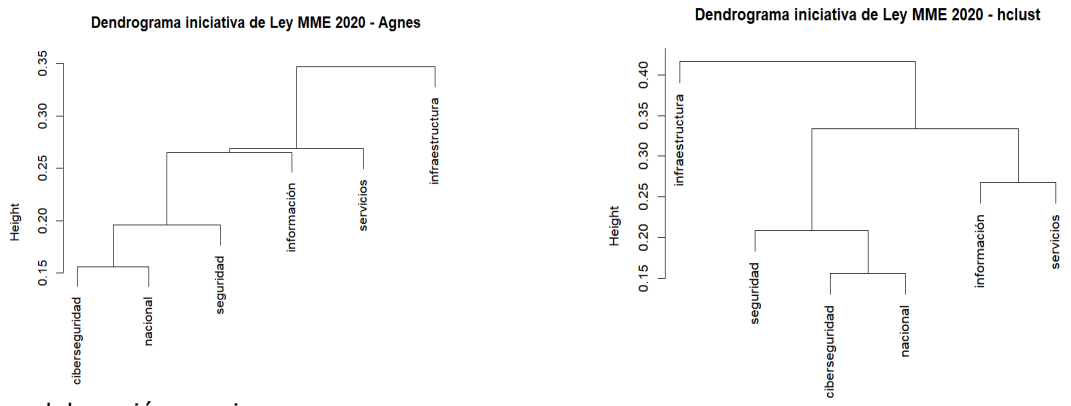


Fuente: elaboración propia.

En el análisis de dendrograma se identificaron qué conceptos se interrelacionan de una forma más estrecha. Se presentó que una de las palabras centrales en el cuerpo de la iniciativa es "infraestructura". Esto se observó, tanto en la visualización de dendrograma de hclust como de Agnes.

Se presentó que la palabra de "infraestructura" tiene una relación de .40 con palabras como "información" y "servicios", mientras que estas palabras tienen un grado de correlación del .25 al .30 con palabras como "seguridad", "ciberseguridad" y "nacional". Esto indica que los términos se fusionan a un nivel relativamente bajo de disimilitud, lo cual implica que los documentos o elementos dentro de estos clústeres son bastante similares, por lo cual estas palabras son las que presentan un mayor nivel de profundidad en el análisis de la iniciativa.

Figura 3. Dendrogramas de Agnes y hclust de la iniciativa de Ley MME 2020



Fuente: elaboración propia.

Iniciativa de la senadora Lucía Trasviña Waldenrath LTW (2021)

En el análisis de la iniciativa de ley de la senadora Lucía Trasviña Waldenrath se identificaron en la *Word Cloud* conceptos clave principalmente asociados a cuestiones de seguridad pública. Esto se observa en la Figura 4 con palabras como "prevención", "ley", "delitos", "prevenir", "conductas", "seguridad", "ciberdelitos", "protección" y "mecanismos". Esto parece indicar que el principal tema desarrollado en este proyecto de ley se focaliza en el combate a los delitos cibernéticos, con lo cual la iniciativa está más orientada a atender temas de seguridad pública. Del mismo modo, se encuentra poca evidencia para expresar una profundización en temas de derechos humanos, cooperación internacional y asociaciones público-privadas.

A pesar de esto, hay palabras como "coordinación", "cultura", "convenios" y "derechos" que permiten ver que los datos consultados en el proceso de investigación para la creación de la ley sí abordaron temas de vanguardia en la ciberseguridad y fuera de la óptica del Estado. No obstante, el hecho de que el impacto de los conceptos no sea representativo en el marco del contenido completo de la iniciativa refleja que el equipo legislativo que la redactó no atendió los temas de forma eficaz y puntual.

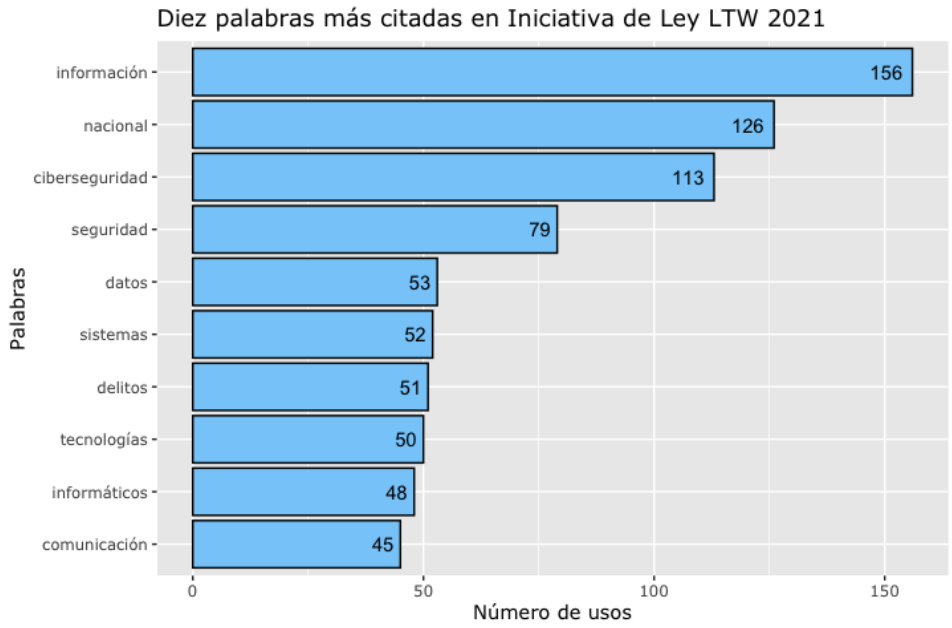
Figura 4. Lucía Trasviña Waldenrath LTW (2021)

Fuente: elaboración propia.

En el análisis de las diez palabras más citadas, la palabra "información" fue la que tuvo un mayor nivel de representación con un total de 156 repeticiones. Estuvo seguida de "nacional" con 126 y "ciberseguridad" con 113. Por otra parte, destaca la incidencia de palabras como "seguridad" (79), "datos" (53), "sistemas" (52), "delitos" (51). Lo que recalca el énfasis en los temas de seguridad pública en la iniciativa de ley. Adicionalmente, destaca la ausencia de términos relacionados con la cooperación internacional, el sector privado o los derechos humanos.

En el análisis de los dendrogramas de hclust y Agnes se encontró que la correlación existente entre los términos de la iniciativa de ley era baja, a razón de que estos solo mostraron un valor de correlación inferior al .20. En este sentido, destaca que en los dos tipos de visualizaciones los términos que se interrelacionaron fueron "información", con "seguridad" y "nacional".

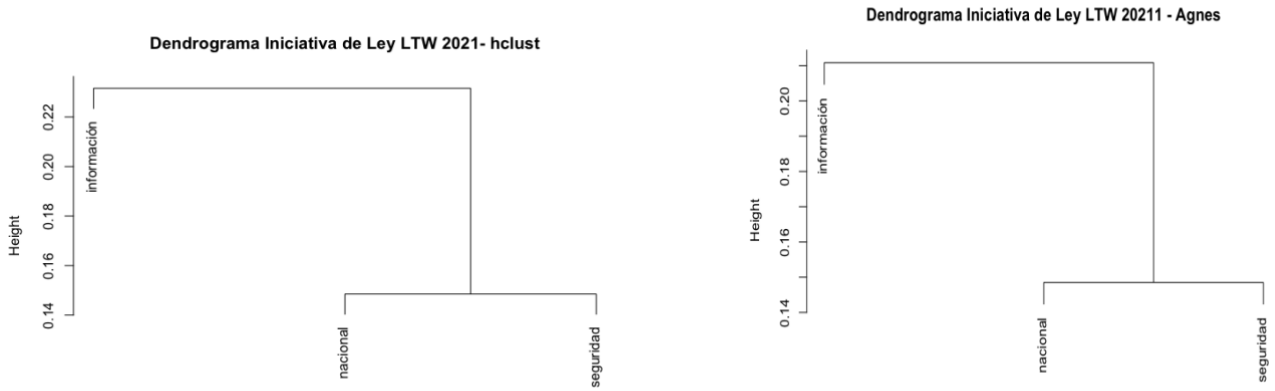
Figura 5. Diez palabras más citadas en Iniciativa de Ley de LTW 2021



Fuente: elaboración propia.

Fue un aspecto un tanto sorpresivo, porque la *Word Cloud* pareció mostrar que el concepto con mayor profundidad dentro de la iniciativa era la seguridad pública, mientras que el análisis de los dendrogramas le da mayor peso a la seguridad nacional. Sin embargo, a pesar de esta condición la iniciativa de LTW sigue siendo parte del conjunto de iniciativas que dan prevalencia a la visión estado-centrista, que a una visión holística de la ciberseguridad.

Figura 6. Dendrogramas de Agnes y hclust de la iniciativa de Ley LTW 2021



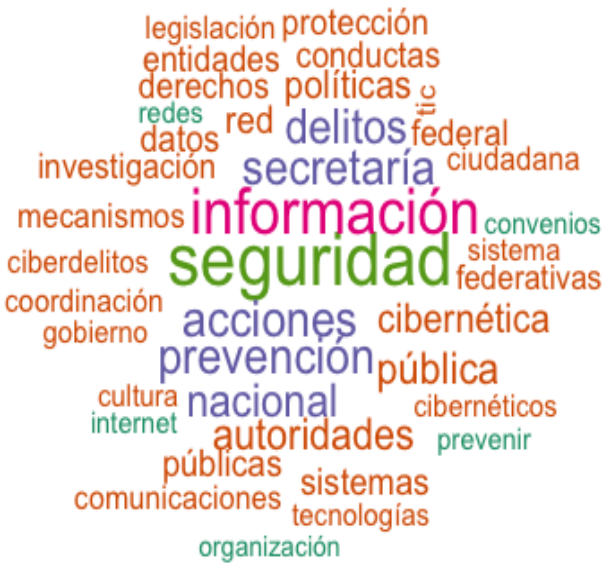
Fuente: elaboración propia.

Iniciativa de la diputada Juanita Guerra Mena JGM (2022)

En el análisis de la *Word Cloud* de JGM (2022) se identificaron conceptos claves con palabras como "seguridad", "información", "acciones", "prevención", "secretaría", "coordinación", "gobierno", "federativas", "delitos", "nacional". En este sentido, resalta que la iniciativa de ley parece dar un énfasis importante a los actores involucrados en la política nacional de ciberseguridad al tener conceptos clave como pueden ser "secretaría", "federativas" o "gobierno", que se refieren a diferentes actores de los niveles de gobierno estatal o federal. Por otra parte, las palabras "coordinación" y "convenios" refuerzan que la organización de la política nacional de ciberseguridad es un aspecto eje y clave en el marco de esta iniciativa de ley.

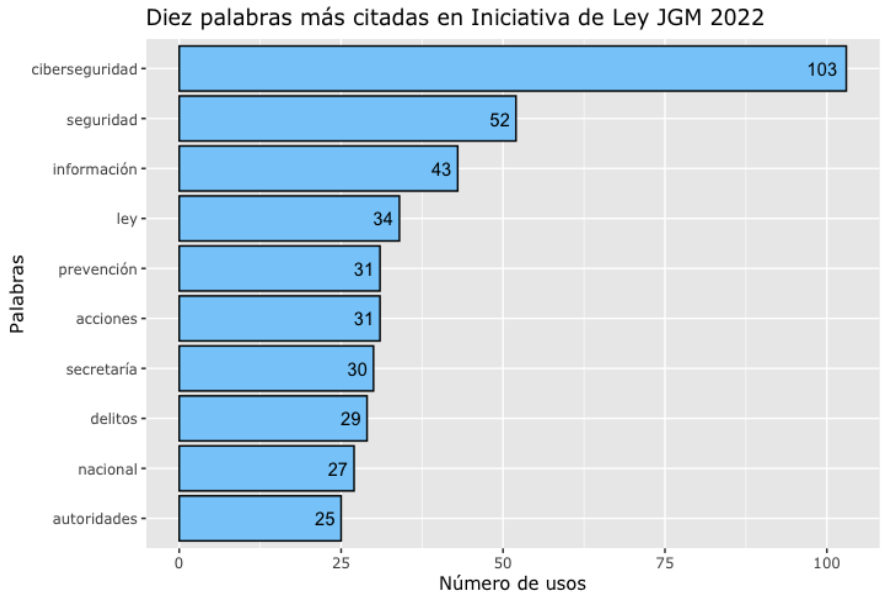
En el análisis de las palabras más citadas se identificó que estas fueron "ciberseguridad" con un total de 103 repeticiones, "seguridad" (52), "información" (43), "ley" (34) y "prevención" (31). De nueva cuenta, a pesar de que no se encuentran entre las primeras palabras con mayor número de repeticiones destacan conceptos relacionados a la coordinación de la política nacional de ciberseguridad como "acciones" (31), "secretaría" (30), "delitos" (29) y "autoridades" (25). Con lo que se evidencia otra vez que una particularidad de esta iniciativa es el tema de la delimitación de responsabilidades y la coordinación de los actores de gobierno en la política de ciberseguridad.

Figura 7. World Cloud de Iniciativa de Ley de JGM 2022



Fuente: elaboración propia.

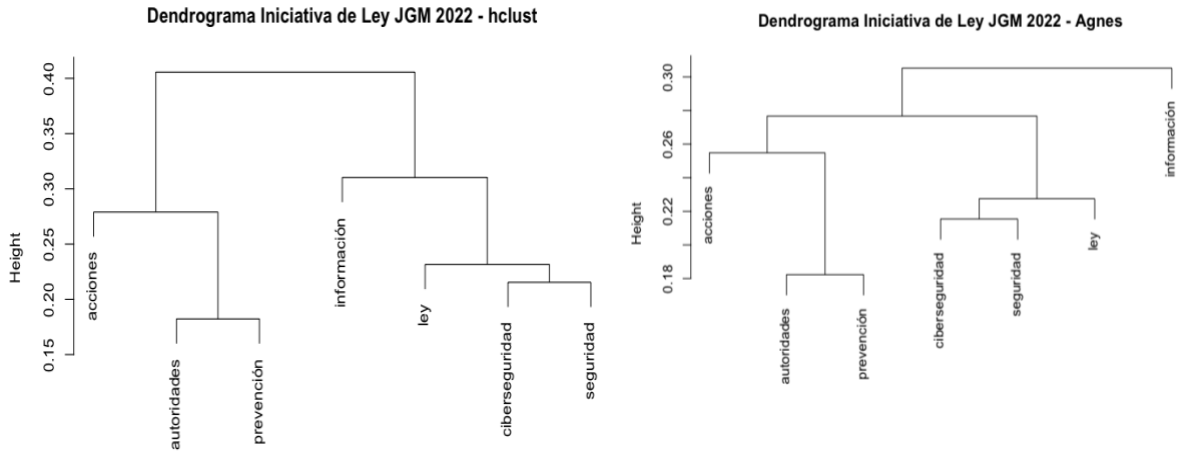
Figura 8. Diez palabras más citadas en Iniciativa de Ley de JGM 2022



Fuente: elaboración propia.

Mientras que en el caso de Agnes los conceptos crearon un solo árbol de relación con dos subdivisiones, donde el concepto central fue "información" y se relaciona con "acciones", "autoridades" y "prevención". De nuevo esta rama indica una relación de conceptos más profunda que une estas tres palabras. Lo que refuerza la idea de que en la iniciativa de JGM 2022 es central el tema de la coordinación y delimitación de responsabilidades para la política de ciberseguridad. Por último, la otra subdivisión unió a los conceptos de "ley", "ciberseguridad" y "seguridad" con un nivel de correlación de 0.18 y 0.22.

Figura 9. Dendrogramas de Iniciativa de Ley JGM 2022



Fuente: elaboración propia.

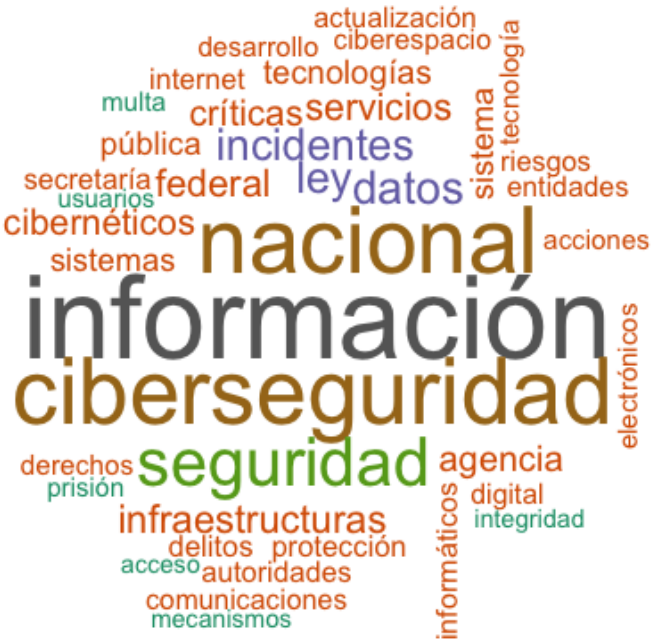
Iniciativa del diputado Javier López Casarín JLC (2023)

En el análisis de la *Word Cloud* resultante de la iniciativa de JLC 2023 se encontró que los conceptos más importantes en texto son "nacional", "información", "ciberseguridad" y "seguridad". De nueva cuenta el enfoque estado-céntrico se hace presente en esta iniciativa por encima de las perspectivas holísticas que consideran temas de derechos humanos, el sector privado, etc.

En segunda instancia destacan conceptos como "federal", "entidades, "acciones", "riesgos", "críticas", "sistemas". Esto ayuda a deducir que la legislación aborda en su contenido temas vinculados a la protección de INC y la coordinación de las instancias de gobierno para la implementación de la ley. Del mismo modo, destaca que la propuesta de JLC contiene palabras como "integridad", "actualización" y "desarrollo". Esto parecería indicar que dentro del texto se abordan temas como el involucramiento del gobierno nacional en torno al desarrollo de capacidades cibernéticas, más allá de la visión de prevención.

Desde una mirada jurídica destacan conceptos como "multa", "prisión" y "delitos", lo cual indica que la iniciativa tiene un enfoque penalista en el marco de la implementación de la política nacional de ciberseguridad a razón que promueve la creación de multas y penas de prisión ante incidentes cibernéticos. Por último, conceptos como "agencia", "entidades" y "federal" indicarían un contenido importante relacionado a crear agencias y/o entidades dentro del gobierno que se encarguen de estos temas específicos de ciberseguridad.

Figura 10. World Cloud de Iniciativa de Ley de JLC 2023

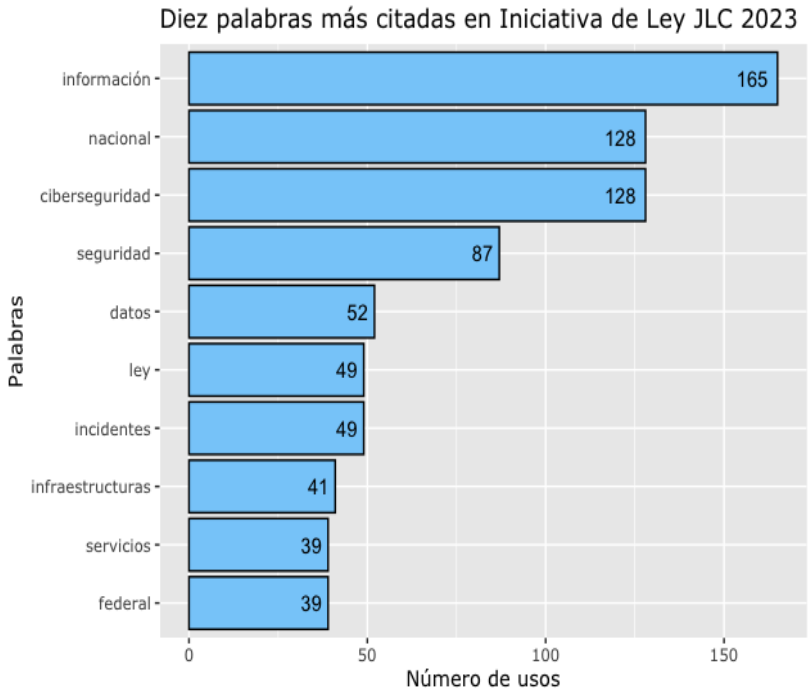


Fuente: elaboración propia.

En el análisis de las palabras más citadas se encontraron "información" con 165 repeticiones, "nacional" (128), "ciberseguridad" (128), "seguridad" (87) y "datos" (52). De nueva cuenta, el análisis presenta que el enfoque de la ley es estado-céntrico, con una visión que prioriza a la política de ciberseguridad con un enfoque en seguridad nacional.

Por otra parte, si bien no se encuentran entre las principales palabras destacan conceptos como "incidentes" (49), "infraestructuras" (41), "servicios" (39) y "federal" (39). Su presencia indica que la iniciativa da profundidad al tema de la protección de la INC como es el caso de MME (2020). Por otra parte, el concepto "federal" indica que el nivel de coordinación y aplicación de la política nacional de ciberseguridad está principalmente focalizado en el nivel de gobierno federal, sin dar profundidad al nivel subnacional e internacional.

Figura 11. Diez palabras más citadas en Iniciativa de Ley JCL 2023



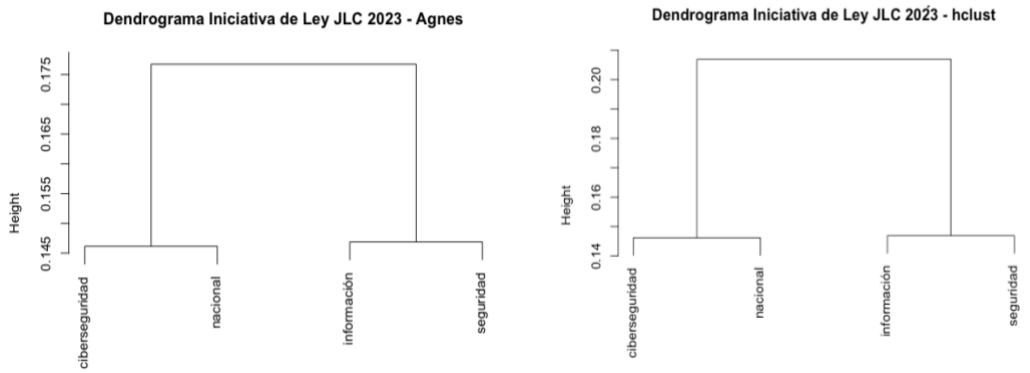
Fuente: elaboración propia.

Al analizar los dendrogramas se observa como estos son prácticamente iguales. En ellos se visualiza como dos ramas destacan. La primera une a los conceptos de "ciberseguridad" y "nacional", mientras que la segunda une a conceptos como "información" y "seguridad".

Es importante indicar que la única diferencia sustantiva entre ambos dendrogramas es el nivel de correlación que presentan. En el caso de hclust es más alta hasta alcanzar un rango que va de 0.14 a 0.20, mientras que en Agnes el rango es de 0.145 a 0.175. Sin embargo, los conceptos relacionados a temas de protección de INC, coordinación de actores gubernamentales en la aplicación de la política nacional de ciberseguridad no aparecen en ambas visualizaciones.

Esto indica que estos conceptos no tienen una profundidad objetiva. Esto se explica a razón que la iniciativa propone nuevas instituciones que regulen la ciberseguridad, pero no presenta una estrategia sobre cómo coordinar a los actores.

Figura 12. Dendrogramas de Iniciativa de Ley JLC 2023



Fuente: elaboración propia.

Conclusiones

La presente investigación partió de la hipótesis de que las iniciativas legislativas en materia de ciberseguridad en México tienen un enfoque estado-centrista, focalizado en la seguridad nacional y seguridad pública. Las cuales dejan de lado temas trascendentales en la creación de una ley de ciberseguridad. Para probar esto se realizó una revisión teórica que tuvo como fin responder las siguientes dos preguntas: ¿Qué necesita una ley de ciberseguridad? ¿Qué aspectos hay que tomar en consideración a la hora de redactar una iniciativa legislativa holística en la materia?

Después de la aplicación de la metodología cualitativa y cuantitativa a las dieciocho iniciativas identificadas se puede expresar que la hipótesis se cumplió a razón de los resultados obtenidos. Sin embargo, los hallazgos obtenidos en cada una de estas secciones contienen elementos para la mejora de las propuestas legislativas a futuro y del papel del Congreso en su estructuración.

Para el caso de la sección cualitativa, centrada en analizar la profundidad de las leyes con base en las propuestas de Riza Azmi, Tibben y Than Win (2018), Kossef (2020), Aguilar-Antonio (2020), Shackelford (2017), Deibert (2018) y Pavlova (2020) se expresa que es evidente que la mayoría de las propuestas legislativas se centran en fortalecer las capacidades cibernéticas del Estado, especialmente en términos de seguridad pública y nacional. A pesar de esto, existe una falta de enfoque colaborativo entre diferentes actores para la gobernanza del ciberespacio, esto a pesar de lo propuesto por organizaciones internacionales como la ITU, la OEA y BID. Este aspecto es muy evidente en todas las iniciativas que presentan una falta de un modelo de coordinación o gobernanza para las partes interesadas en México.

Esto es consecuencia de que la mayoría de las iniciativas no conciben la ciberseguridad más allá de la seguridad nacional. Por lo que ignoran, evaden o dejan de lado temas como los derechos humanos, las asociaciones público-privadas, la protección de infraestructuras críticas nacionales, la cooperación tanto en el nivel institucional, regional e internacional, la capacitación de expertos en ciberseguridad, investigación y desarrollo en la comprensión del avance de las tecnologías emergentes.

En el caso de la propuesta de Kossef se destaca el principio de información, el cual se aborda en la mayoría de las propuestas, pero a menudo falta proporcionar datos concretos y medidas específicas para solucionar las problemáticas identificadas. Resalta que la cooperación interinstitucional e internacional a menudo se relega a un segundo plano en las iniciativas. Así como que los principios de claridad, adaptación y comprensión son ignorados. De esta forma, Kossef brinda una mirada de cómo un país aborda con enfoque vanguardista el tema de la ciberseguridad.

Para el caso de la propuesta de Aguilar-Antonio (2020), las iniciativas carecen de una percepción clara del ciberespacio como componente del poder nacional y como instrumento de proyección internacional. Tampoco distinguen adecuadamente entre la parte física y virtual del ciberespacio. Consideran la importancia de proteger las Infraestructuras Críticas Nacionales (INC) y entienden la importancia del comercio y la economía digital en una ley de ciberseguridad, así como la necesidad de abordar las diferentes dimensiones.

Respecto del enfoque en derechos humanos, es importante mencionar que este contenido es frecuentemente olvidado por los legisladores. A razón que solo unas pocas propuestas lo abordan de manera puntual. A pesar de esto, la libertad de expresión, la protección de datos y la privacidad son los principales derechos humanos mencionados en las iniciativas.

Respecto de la sección cualitativa donde se aplicó la metodología de *Text Mining* a través de R Studio, se indica que el análisis detallado de las cuatro iniciativas de ley de ciberseguridad verificó también el enfoque estado-céntrico de estas. Esto fue más que evidente en las *Word Cloud* y los listados de las palabras más citadas y dendrogramas. A pesar de esto existen diferencias entre las iniciativas y sus enfoques distintos.

La iniciativa de Miguel Ángel Mancera tiene fuerte énfasis en la protección de la infraestructura crítica. La de Lucía Trasviña se centra más en combatir delitos cibernéticos desde una perspectiva de seguridad pública. Por su parte, la de Juanita Guerra Mena hace un mayor énfasis en el tema de la coordinación y delimitación de responsabilidades para la política de ciberseguridad.

Por último, la iniciativa presentada por Javier López Casarín parece conjuntar varios de los elementos de las iniciativas anteriores, esto puede explicarse a razón que es la última y más reciente propuesta de ley. A pesar de esto refleja un marcado énfasis estado-céntrico de la ciberseguridad. Mientras destaca la seguridad nacional, la protección de la información crítica, la coordinación a nivel federal y la aplicación de medidas punitivas como multas y penas de prisión en respuesta a incidentes cibernéticos. Este enfoque, aunque mantiene una preocupación por la seguridad nacional puede diferenciarse por su inclinación hacia aspectos relacionados con la regulación, la penalización y el fortalecimiento de las capacidades cibernéticas a nivel gubernamental.

Otro aspecto de relevancia es como las correlaciones y relaciones entre los términos de las iniciativas, a través del análisis de dendrogramas. Esto como consecuencia de que este instrumento ayuda a entender la estructura y la profundidad de los temas abordados en el contenido de los textos de cada propuesta.

A pesar de esto, es importante reconocer el interés y liderazgo de los legisladores y las dos cámaras del Congreso para impulsar iniciativas en materia de ciberseguridad. Si bien se acepta que las iniciativas no deben ser perfectas, el fin último de esta investigación es brindar elementos y mostrar las áreas de oportunidad del trabajo legislativo realizado durante el periodo 2018-2023. Para que, en las próximas legislaturas, los nuevos integrantes del Congreso puedan crear leyes más completas, holísticas y adecuadas con el fin de construir sobre los errores y aciertos del pasado.

Referencias

Aguilar-Antonio, J. M. (2020a). La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. Revista de estudios en seguridad internacional, 6(2), 17-43. DOI: http://dx.doi.org/10.18847/1.12.2

Aguilar-Antonio, J. M. (2020b). Presente y futuro de los retos de la ciberseguridad en México, una propuesta para la seguridad nacional. Revista legislativa de estudios sociales y de opinión pública, 13(29), 83-120.

Aguilar-Antonio, J. M. (2022). La necesidad de un enfoque multistakeholder en ciberseguridad para la seguridad nacional. En Jiménez Cabrera E. (Coord.), Seguridad nacional y ciberseguridad: Contexto y desafíos para América Latina y el Caribe (pp. 73-90). Tirant lo Blanch. Disponible en SSRN: https://ssrn.com/abstract=4900235

Aguilar-Antonio, J. M. (2024). Rezago y asimetrías de las política nacional e internacional de ciberseguridad de México frente Estados Unidos y Canadá: retos de cooperación para Norteamérica. Norteamérica, Revista Académica Del CISAN-UNAM, 19(1). DOI: https://doi.org/10.22201/cisan.24487228e.2024.1.663

Aguirre Quezada, J. P. (2022). Ciberseguridad, desafío para México y trabajo legislativo. Cuaderno de Investigación No. 87 (marzo 2022). Instituto Belisario Domínguez, recuperado de: https://bibliodigitalibd.senado.gob.mx/handle/123456789/5551?show=full

Badenes-Olmedo, C., Redondo-García, J. L. & Corcho, O. (2019). Legal document retrieval across languages: Topic hierarchies based on synsets [arXiv]. Recuperado de https://arxiv.org/abs/1911.12637

Cámara de Diputados (s.f.). Terminología Legislativa. Recuperado de https://www.diputados.gob.mx/sedia/biblio/doclegis/cuaderno_terminolegis.pdf

Cabrera Salvador, C. (2022). Iniciativa con proyecto de decreto por el que se reforman las fracciones XXX y XXXI y se adiciona la fracción XXXII al artículo 73 de la constitución. Recuperado de asun_4468483_20221213_1670374407.pdf

Corona Nakamura, M. R. (2022). Iniciativa con proyecto de decreto por el que se reforma y adiciona el artículo 5 de la ley de seguridad nacional. Senado de la República, Grupo Parlamentario del Partido Verde Ecologista. Recuperado de https://infosen.senado.gob.mx/sgsp/gaceta/65/1/2022-08-03-1/assets/documentos/Inic_PVEM_Dip_Nakamura_art_5_LSN.pdf

Danelyan, A. A. & Gulyaeva E. E. (2020). International Legal Aspects of Cybersecurity. Moscow Journal of International Law, (1), 44-53. DOI: https://doi.org/10.24833/0869-0049-2020-1-44-53

Deibert, R. J. (2018). Toward a Human-Centric Approach to Cybersecurity. Ethics and International Affairs, 32(4), 411-424. DOI: 10.1017/S0892679418000618

e-Governance Academy Foundation (e-GAF). (2024). National Cybersecurity Index (NCSI). Tallin: e-Governance Academy. Recuperado de https://ncsi.ega.ee/ncsi-index/

Enríquez Herrera, J. R. (2020). Iniciativa con Proyecto de Decreto por el que se adiciona la fracción XIV al Artículo 5 de la Ley de Seguridad Nacional. Senado de la República, Grupo Parlamentario del Movimiento Regeneración Nacional. Recuperado de https://infosen.senado.gob.mx/sgsp/gaceta/64/3/2020-11-04-1/assets/documentos/Inic_Morena_Sen_Enriquez_Art_5_Ciberseguridad.pdf

Firdhous, M. F. M. (2010). Automating legal research through data mining. International Journal of Advanced Computer Science and Applications, 1(6), 9–14. Recuperado de http://ijacsa.thesai.org/

García Anaya, L. (2021). Iniciativa que reforma los artículos 11 y 13 de la Ley de la Fiscalía de la República. Sistema de información Legislativa de la Secretaría de Gobernación, Grupo Parlamentario de Morena. Recuperado de http://sil.gobernacion.gob.mx/Archivos/Documentos/2021/12/asun_4291684_20211215_1638478336.pdf

Gómez, C., Blanco, J. M., García, J. L. & Sánchez, J. A. (2023). Automatic explanation of the classification of Spanish legal judgments in jurisdiction-dependent law categories with tree estimators [arXiv]. Recuperado de https://arxiv.org/abs/2404.00437

Guerra Mena, J. (2021). Iniciativa de reforma al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. Sistema de información Legislativa de la Secretaría de Gobernación, Grupo Parlamentario de Morena. Recuperado de http://sil.gobernacion.gob.mx/Archivos/Documentos/2021/09/asun_4224997_20210930_1632415529.pdf

Guerra Mena, J. (2022). Iniciativa con proyecto de decreto por el que se expide la ley general de ciberseguridad. Sistema de información Legislativa de la Secretaría de Gobernación, Grupo Parlamentario de Morena. Recuperado de http://sil.gobernacion.gob.mx/Archivos/Documentos/2022/12/asun_4475036_20221215_1665067316.pdf

Hernández Pérez, M. E. (2020). Iniciativa con proyecto de decreto por el que se declara el día 23 de noviembre como "Día Nacional de Ciberseguridad". Grupo Parlamentario de Morena. Recuperado de http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/08/asun_4059385_20200812_1597257570.pdf

Hernández Pérez, M. E. (2022). Iniciativa que adiciona los artículos 5, 6 y 13 de la Ley de Seguridad Nacional. Sistema de información Legislativa de la Secretaría de Gobernación, Grupo Parlamentario de Morena. Recuperado de http://sil.gobernacion.gob.mx/Archivos/Documentos/2022/12/asun_4465436_20221208_1665511763.pdf

International Telecommunication Union (ITU). (2024). Global Cybersecurity Index 2024 (GCI). Ginebra: Unión Internacional de Telecomunicaciones. Recuperado de https://www.itu.int/pub/D-HDB-GCI.01-2024

Kossef, J. (2020). Hacking Cybersecurity Law. University of Illinois Law Review, 3,811- 850. DOI: 10.2139/ssrn.3331350

Lagunes Soto Ruíz, A. (2018). Decreto para reformar y adicionar diversas disposiciones del código penal federal en materia de ciberseguridad. Senado de la República, Partido Verde Ecologista. Recuperado de https://infosen.senado.gob.mx/sgsp/gaceta/64/1/2019-04-23-1/assets/documentos/Inic_PVEM_Codigo_Penal_Ciberseguridad.pdf

Lagunes Soto Ruíz, A. (2019). Proposición para la adhesión de México al convenio sobre la ciberdelincuencia, o convenio de Budapest. Senado de la República, Partido Verde Ecologista. Recuperado de http://sil.gobernacion.gob.mx/Archivos/Documentos/2019/04/asun_3864659_20190425_1555026089.pdf

Lagunes Soto Ruíz, A. (2019). Iniciativa con proyecto de decreto que declara el mes de octubre como "El mes nacional de la ciberseguridad". Senado de la República, Partido Verde Ecologista. Recuperado de http://sil.gobernacion.gob.mx/Archivos/Documentos/2019/10/asun_3933760_20191010_1570717588.pdf

Lagunes, A., Gálvez, X., Ramírez, J. C., Madero, G., Mancera, M. A. (2023). Iniciativa con proyecto de decreto por el que se reforma la fracción XVII, al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, en materia de inteligencia artificial, ciberseguridad y neuroderechos. Senado de la República. Recuperado de https://infosen.senado.gob.mx/sgsp/gaceta/65/3/2023-09-26-1/assets/documentos/Inic_PVEM_diversos_senadores_art_73_CPEUM.pdf

López Casarín, J. J. (2023). Iniciativa con proyecto de decreto por el que se expide la ley federal de ciberseguridad. Sistema de información Legislativa de la Secretaría de Gobernación, Grupo Parlamentario del Partido Verde Ecologista. Recuperado de http://sil.gobernacion.gob.mx/Archivos/Documentos/2023/04/asun_4562814_20230426_1682446583.pdf

Mancera Espinosa, M. Á. (2020). Ley General de Ciberseguridad. Sistema de información Legislativa de la Secretaría de Gobernación, Grupo Parlamentario del Partido de la Revolución Democrática. Recuperado de http://sil.gobernacion.gob.mx/Archivos/Documentos/2020/09/asun_4064516_20200902_1599062884.pdf

McChesney, R. W. (2015). Desconexión digital: Cómo el capitalismo está poniendo a Internet en contra de la democracia. Barcelona: El Viejo Topo.

Mosco, V. (2017). Becoming digital: Toward a post-Internet society. Bingley, Reino Unido: Emerald Publishing Limited.

Papakonstantinou, V. (2022). Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity? Computer Law & Securiy Review, 22, 1-15. DOI: https://doi.org/10.1016/j.clsr.2022.105653.

Pavlova, P. (2020). Human-rights based approach to cybersecurity: Addressing the security risks of targeted groups. Peace Human Rights Governance, 4(3), 391-418. DOI: 10.14658/pupj-phrg-2020-3-4

Riza, A., Tibben, W., Than Win, K. (2018). Review of cybersecurity frameworks: context and shared concepts. Journal of Cyber Policy, 3(2), 258-283. DOI: 10.1080/23738871.2018.1520271

Rodríguez Prieto, R. & Martínez Cabezudo, F. (2016). Poder e Internet: Un análisis crítico de la red. Madrid: Cátedra.

Rosas Quintanilla, J. S. (2019). Iniciativa que reforma el artículo 211 Bis 1 del Código Penal Federal. Sistema de información Legislativa de la Secretaría de Gobernación, Partido Acción Nacional. Recuperado de http://sil.gobernacion.gob.mx/Archivos/Documentos/2019/03/asun_3822246_20190301_1550169543.pdf

Salinas Narváez, J. (2019). Iniciativa que reforma el artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. Sistema de información Legislativa de la Secretaría de Gobernación, Grupo Parlamentario de Morena. Recuperado de http://sil.gobernacion.gob.mx/Archivos/Documentos/2019/10/asun_3953044_20191029_1569348687.pdf

Shackelford, S. J. (2017). Human Rights and Cybersecurity Due Diligence: A Comparative Study. University of Michigan Journal of Law Reform, 50(4), 859-885. DOI: https://doi.org/10.36646/mjlr.50.4.human

Trasviña Waldenrath, J. L. (2021). Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Ciberseguridad y se derogan diversas disposiciones del Código Penal Federal. Senado de la República, Grupo Parlamentario del Movimiento Regeneración Nacional. Recuperado de https://infosen.senado.gob.mx/sgsp/gaceta/64/3/2021-04-06-1/assets/documentos/Inic_Morena_Sen_Trasvina_Ciberseguridad_Penal.pdf

Trasviña Waldenrath, J. L. (2021). Iniciativa con Proyecto de Decreto para reformar diversos artículos de la Ley General del Sistema Nacional de Seguridad Pública, en materia de creación de la Comisión Nacional de Ciberseguridad. Senado de la República, Grupo Parlamentario del Movimiento Regeneración Nacional. Recuperado de https://infosen.senado.gob.mx/sgsp/gaceta/65/1/2021-10-14-1/assets/documentos/Ini_Morena_Sen_Trasvina_Creacion_Com_Ciberseguridad.pdf

Agradecimientos

Este artículo se realizó con apoyo del Programa de Becas Posdoctorales de la UNAM, el autor es becario del Centro de Investigaciones sobre América del Norte (CISAN), asesorado por el Dr. Leonardo Curzio Gutiérrez y desarrolla el proyecto "El desafío de ético y político de la inteligencia artificial (IA) y la ciberseguridad en América del Norte: retos y oportunidades de cooperación para México, Estados Unidos y Canadá.

CÓMO CITAR ESTE ARTÍCULO:

Aguilar Antonio, J. M. y Quechol Maciel, K. (2025). ¿Qué necesita una ley de ciberseguridad? Análisis de las propuestas legislativas en México (2019-2023). *Paakat: Revista de Tecnología y Sociedad, 15*(28). http://dx.doi.org/10.32870/Pk.a15n28.892

*Juan Manuel Aguilar Antonio es Investigador Posdoctoral en el Centro de Investigaciones sobre América del Norte (CISAN), de la Universidad Nacional Autónoma de México (UNAM). Miembro del Sistema Nacional de Investigadores (SNI) con Nivel de Candidato para el periodo 2024-2027. Doctor en Ciencias Sociales por la Facultad de Ciencias Políticas y Sociales (FCPyS) de la UNAM. Maestro en Socioeconomía.

** Licenciada con honores en Relaciones Internacionales por la Universidad de las Américas, Puebla. Investigadora interesada en temas de género, ciberseguridad y cibercrimen. Ha colaborado en la redacción de un informe para el Comité Internacional de la Cruz Roja (CICR), así como en la redacción de un capítulo de libro que está por publicarse

[1] Dorking es todo el conjunto de operadores de búsqueda avanzados y poco usados, con los que cuenta este buscador en concreto. Estos operadores de búsqueda lo que permiten a rasgos muy generales es hacer un mejor filtrado de los resultados que queremos obtener a la hora de buscar información en Google.

[2] México ha participado activamente en diversos foros internacionales relacionados con ciberseguridad, incluyendo la Organización de los Estados Americanos (OEA), donde ha trabajado en programas de capacitación y desarrollo de capacidades cibernéticas; el Foro de Gobernanza de Internet (IGF), destacando su rol como anfitrión en 2016, así como el Grupo de Trabajo Abierto (Open-Ended Working Group en OEWG) de la ONU que fomenta la regulación y el comportamiento responsable en el ciberespacio. Ha colaborado en iniciativas del Foro Económico Mundial (WEF) sobre protección de infraestructuras críticas, el Global Forum on Cyber Expertise (GFCE) para el fortalecimiento de capacidades cibernéticas y los programas de la INTERPOL enfocados en la cooperación internacional contra el cibercrimen. Sin embargo, estas colaboraciones se han dado desde instituciones principalmente del poder ejecutivo (Secretaría de Relaciones Exteriores, Fiscalía General de la República, Secretaría de Economía o Secretaría de Infraestructura, Comunicaciones y Transportes). Del mismo modo se aclara que, desde el poder legislativo, institución encargada de la creación de una ley de ciberseguridad, México no ha firmado o ratificado ningún tratado o acuerdo en la materia como lo es el Convenio de Budapest.

[3] Un sinset (synonym set) es un conjunto de palabras con significado equivalente en un contexto específico, útil en desambiguación semántica y análisis lingüístico (Gómez, Blanco, García & Sánchez, 2023).

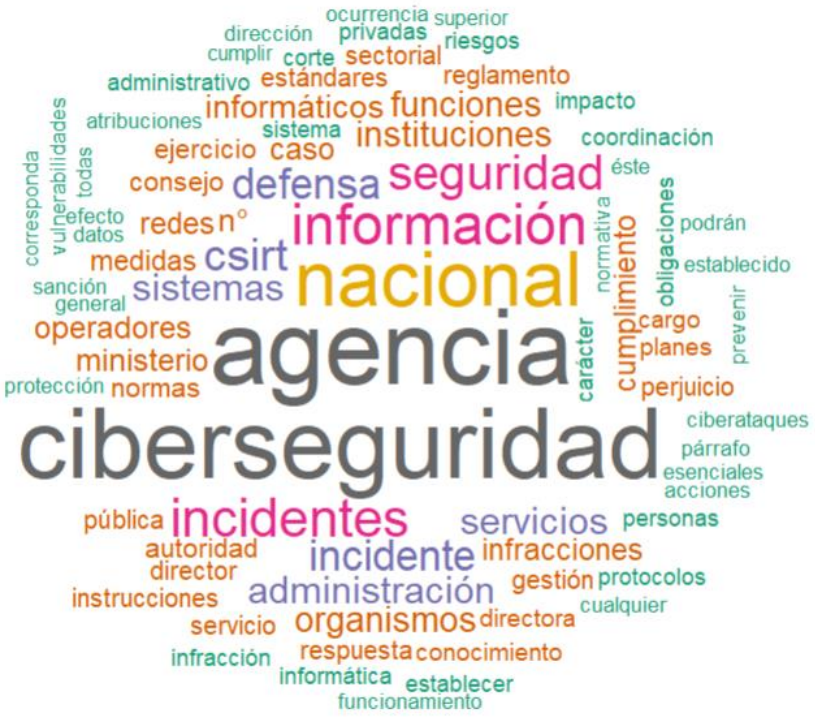
ANEXO 1. Análisis a la Ley Marco de Ciberseguridad (Chile, 2024) y a la propuesta de Ley de Ciberseguridad (Guatemala, 2024)

Ley Marco de Ciberseguridad de Chile

Análisis de *Word Cloud*

El análisis de la *Word Cloud* de la Ley Marco de Ciberseguridad de Chile permite identificar los elementos clave que estructuran el enfoque normativo de esta iniciativa. Las palabras más prominentes como "agencia", "nacional", "ciberseguridad" e "información" reflejan un marco centralizado que busca coordinar las acciones en torno a la protección de sistemas críticos y la respuesta ante incidentes cibernéticos. Este enfoque subraya la creación de la Agencia Nacional de Ciberseguridad (ANCI) como el eje articulador de las políticas en esta materia.

Figura 1. Análisis de *Word Cloud* de la Ley Marco de Ciberseguridad de Chile



Fuente: elaboración propia.

En términos específicos, las palabras "incidentes", "gestión" y "protocolos" destacan la importancia de establecer mecanismos claros para la prevención y respuesta a amenazas digitales. La obligatoriedad de reportar incidentes al CSIRT Nacional refuerza la intención de centralizar y estandarizar los procedimientos, garantizando una mayor eficiencia y coordinación entre sectores. Asimismo, términos como "sistemas" y

"servicios esenciales" evidencian el enfoque en la protección de infraestructuras críticas, posicionando a estos elementos como prioritarios dentro del marco regulatorio. La presencia de términos como "cumplimiento", "infracciones" y "sanciones" señala un componente normativo robusto que regula las obligaciones de los operadores críticos. Esto incluye auditorías, certificaciones periódicas y sanciones escalonadas que buscan fomentar el cumplimiento y la mejora continua. En este sentido, el sistema de sanciones no solo tiene un carácter punitivo, sino que también actúa como un incentivo para adoptar mejores prácticas de ciberseguridad.

En un nivel más amplio, palabras como "defensa" y "coordinación" subrayan la intención de integrar esfuerzos entre diferentes actores e instituciones, tanto a nivel nacional como internacional. Esto es reforzado por la inclusión de términos como "ministerio" e "instituciones", las cuales reflejan la estructura multisectorial que caracteriza a la propuesta chilena. La referencia a "estándares" y "normas" apunta hacia la alineación de la ley con marcos internacionales reconocidos como el Convenio de Budapest y el NIST CSF.

Términos como "redes" y "tecnologías" reflejan un enfoque adaptativo frente a las amenazas emergentes, mientras que palabras como "personas" y "obligaciones" destacan el componente humano y social de la ley. Este balance entre aspectos técnicos y derechos humanos posiciona a la Ley Marco de Ciberseguridad de Chile como una propuesta integral que aborda la complejidad del entorno digital de manera estructurada y efectiva.

En conjunto, la *Word Cloud* refleja un enfoque sólido y multidimensional en la Ley Marco de Ciberseguridad de Chile, enfatizando la importancia de la gobernanza centralizada, la colaboración multisectorial y la alineación con estándares internacionales. Estos elementos no solo fortalecen la capacidad del país para gestionar riesgos cibernéticos, sino que también establecen un marco normativo adaptable y alineado con las mejores prácticas globales.

Análisis de diez palabras más citadas

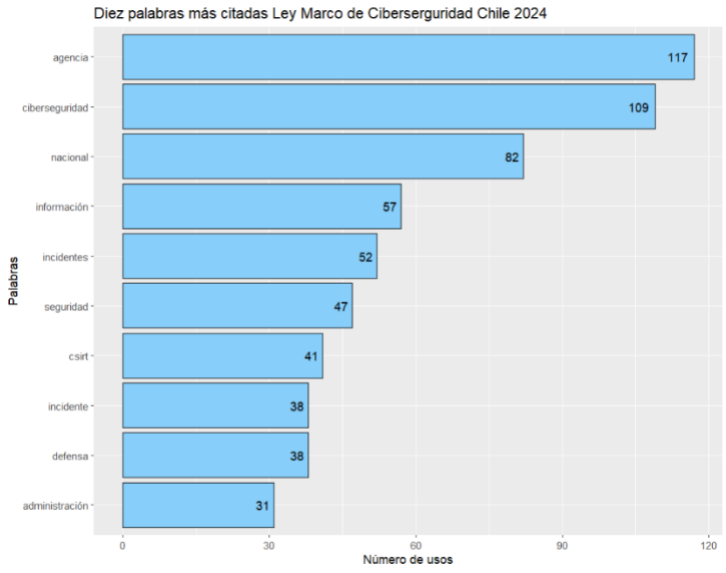
El gráfico de barras sobre las palabras más citadas en la propuesta de la Ley Marco de Ciberseguridad de Chile 2024 ofrece una visión detallada de los enfoques prioritarios de este marco normativo. El término "agencia", con 117 menciones, lidera la lista, lo cual refleja la centralidad de la Agencia Nacional de Ciberseguridad (ANCI) como el eje articulador de las políticas de ciberseguridad en Chile. Esta preeminencia pone de manifiesto la intención de consolidar una gobernanza centralizada y efectiva en la materia con una institución técnica y descentralizada que coordine las acciones entre sectores público y privado.

Palabras como "ciberseguridad" (109 menciones) y "nacional" (82 menciones) subrayan el compromiso de la ley con la protección del entorno digital a nivel país, articulando medidas que buscan fortalecer la resiliencia cibernética de las infraestructuras críticas y servicios esenciales. Este enfoque integral se refuerza con la inclusión de "información" (57 menciones), lo cual destaca la importancia de proteger la confidencialidad, integridad y disponibilidad de los datos sensibles frente a las crecientes amenazas digitales.

Palabras como "defensa" (38 menciones) y "administración" (31 menciones) sugieren un interés en fortalecer la capacidad del Estado para proteger sus sistemas críticos frente a ciberamenazas, mientras se establecen mecanismos administrativos sólidos para garantizar el cumplimiento de las disposiciones legales. Estas menciones destacan un equilibrio entre la prevención y la capacidad de respuesta operativa, alineando la normativa con los desafíos técnicos del entorno digital.

Términos como "incidentes" (52 menciones) y "seguridad" (47 menciones) evidencian la atención que la ley otorga a la gestión y respuesta ante ciberataques. El establecimiento de protocolos de reporte obligatorio al CSIRT Nacional y la tipificación de responsabilidades refuerzan un enfoque preventivo y reactivo para mitigar riesgos en tiempo real. Además, el término "CSIRT" (41 menciones) resalta el rol crucial de este organismo como punto focal para la coordinación nacional e internacional en la gestión de incidentes cibernéticos.

Figura 2. Diez palabras más citadas en la propuesta de Ley Marco de Ciberseguridad de Chile



Fuente: elaboración propia.

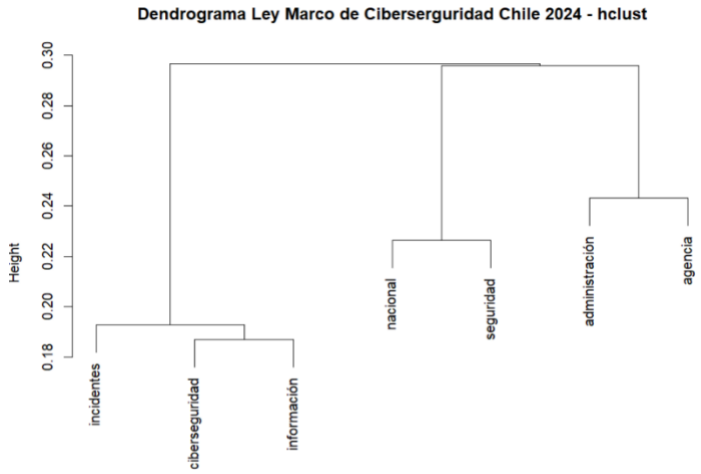
El análisis de las palabras más citadas evidencia que la Ley Marco de Ciberseguridad de Chile busca abordar, tanto los aspectos operativos como normativos de la ciberseguridad. Sin embargo, el gráfico también permite identificar áreas de mejora como la incorporación de términos relacionados con la educación digital y la colaboración multisectorial, elementos clave para fomentar una cultura de ciberseguridad y garantizar la inclusión de todos los sectores en la protección del ciberespacio. La ausencia de términos como "innovación tecnológica" podría sugerir una oportunidad para fortalecer el marco con disposiciones que impulse el desarrollo de nuevas soluciones tecnológicas y de investigación.

En conclusión, el análisis del gráfico muestra un marco normativo sólido y estructurado, pero que podría enriquecerse con estrategias orientadas a largo plazo, asegurando que la ley no solo aborde las necesidades actuales, sino que también anticipe futuras amenazas y fomente un ecosistema digital seguro y sostenible.

Análisis del dendrograma hclust

El dendrograma generado a partir de las palabras clave más destacadas en la Ley Marco de Ciberseguridad de Chile 2024 ofrece una visión jerárquica de las prioridades y conexiones conceptuales que sustentan el marco normativo. Los términos "incidentes", "ciberseguridad" e "información", agrupados en el primer nivel, reflejan el enfoque operativo de la legislación con énfasis en la gestión de amenazas cibernéticas y la protección de datos críticos. Este grupo destaca la importancia de responder de manera ágil y eficiente a los eventos cibernéticos, asegurando la integridad de los sistemas digitales.

Figura 3. Dendrograma de la Ley Marco de Ciberseguridad de Chile 2024



Fuente: elaboración propia.

El segundo grupo, compuesto por "nacional" y "seguridad", indica el alcance y la escala de las políticas establecidas con un enfoque que trasciende lo técnico para abarcar la resiliencia a nivel país. Este grupo enfatiza la necesidad de proteger infraestructuras críticas y servicios esenciales como una prioridad nacional, vinculando directamente la seguridad del ciberespacio con la estabilidad social y económica de Chile.

En el tercer nivel, las palabras "administración" y "agencia" forman un clúster que resalta el papel central de la Agencia Nacional de Ciberseguridad (ANCI) como el órgano responsable de coordinar las políticas y supervisar su implementación. Este grupo refuerza la importancia de contar con una estructura institucional sólida que garantice la sostenibilidad y efectividad de las políticas de ciberseguridad.

Relaciones jerárquicas entre los conceptos

El dendrograma establece conexiones claras entre los distintos niveles conceptuales, reflejando un diseño normativo bien articulado:

Gestión de incidentes y seguridad nacional: la relación entre "incidentes" y "nacional" indica que la capacidad de responder ante ciberamenazas es una prioridad estratégica para el país.

Estructura institucional y enfoque operativo: la conexión entre "administración" y "ciberseguridad" demuestra que la gestión operativa de la ANCI está diseñada para responder eficazmente a los desafíos técnicos y estratégicos.

El análisis jerárquico del dendrograma evidencia que la Ley Marco de Ciberseguridad de Chile 2024 presenta un equilibrio adecuado entre los aspectos técnicos, estratégicos e institucionales. Sin embargo, se identifican posibles áreas de fortalecimiento:

La inclusión de conceptos como "colaboración" y "derechos" podría reforzar el enfoque en los derechos digitales y en la cooperación multisectorial, elementos críticos para la gobernanza cibernética.

Ampliar las conexiones entre la gestión administrativa y los aspectos operativos podría asegurar una mejor alineación entre las políticas y los retos tecnológicos emergentes.

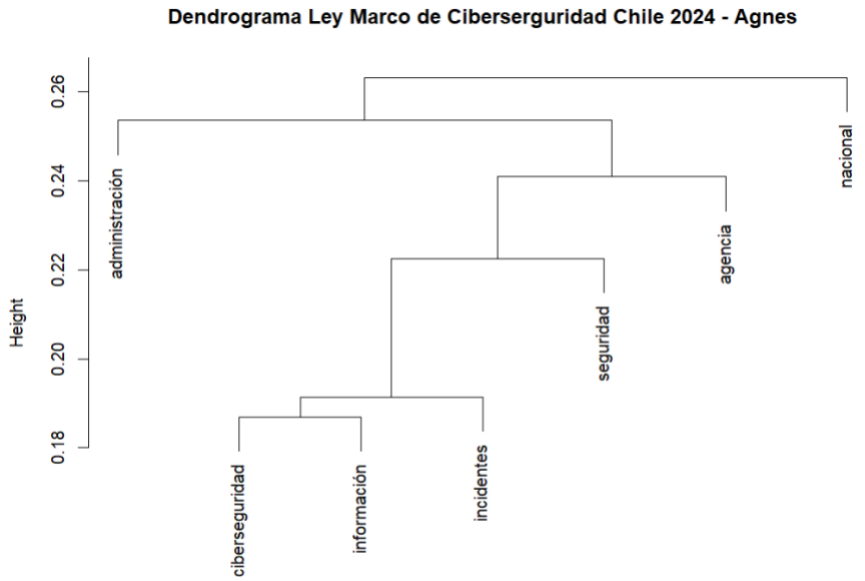
El dendrograma confirma que la Ley Marco de Ciberseguridad de Chile 2024 está diseñada con un enfoque integral y estructurado, priorizando la respuesta a incidentes, la seguridad nacional y la construcción de una infraestructura institucional robusta. Este análisis jerárquico subraya el potencial del marco normativo para abordar de manera efectiva los desafíos de la ciberseguridad en un entorno globalizado.

El dendrograma generado mediante el método Agnes para la Ley Marco de Ciberseguridad de Chile 2024 proporciona una representación jerárquica de las conexiones conceptuales más relevantes dentro de la propuesta normativa. Los términos "ciberseguridad", "información" e "incidentes", agrupados en el nivel más bajo, destacan el enfoque técnico-operativo de la leyque prioriza la protección de datos y la gestión de ciberamenazas. Este grupo refleja la importancia de implementar medidas que garanticen la seguridad y resiliencia del entorno digital chileno.

En un nivel intermedio, el grupo formado por "seguridad" y "agencia" pone de manifiesto el papel central de la Agencia Nacional de Ciberseguridad (ANCI) como el organismo encargado de coordinar y supervisar las políticas de seguridad digital. Este clúster subraya la necesidad de una gestión centralizada para enfrentar las amenazas cibernéticas de manera eficiente y garantizar una protección adecuada de los sistemas críticos del país.

Por último, el término "nacional", en un nodo más alto y conectado con el grupo de "seguridad" y "agencia", enfatiza el alcance estratégico del marco normativo que abarca la protección de la infraestructura crítica y la seguridad a nivel país. De forma complementaria, "administración" aparece como un nodo separado, reflejando la importancia de los procesos internos y organizativos para la implementación efectiva de las políticas, aunque algo desvinculado de los aspectos técnicos y estratégicos.

Figura 4. Dendrograma Agnes de la Ley Marco de Ciberseguridad de Chile 2024



Fuente: elaboración propia.

Análisis del dendrograma Agnes

El dendrograma Agnes destaca cómo los diferentes niveles conceptuales de la ley se estructuran jerárquicamente:

Base técnica-operativa: el grupo de "ciberseguridad", "información" e "incidentes" refleja la prioridad de proteger los datos y gestionar las ciberamenazas en tiempo real.

Gestión centralizada: la conexión entre "seguridad" y "agencia" resalta el rol crucial de la ANCI como eje articulador de la ciberseguridad nacional.

Alcance estratégico: la posición destacada de "nacional" refuerza el enfoque integral de la ley, dirigido a proteger la seguridad digital del país.

El dendrograma sugiere que la Ley Marco de Ciberseguridad de Chile 2024 presenta un diseño jerárquico sólido y bien estructurado. Sin embargo, existen oportunidades de mejora para fortalecer la propuesta:

Fomentar la colaboración internacional: incorporar conceptos relacionados con cooperación global podría enriquecer el marco normativo y alinearlo con estándares internacionales.

Conectar la administración con los aspectos técnicos: la vinculación de "administración" con los términos operativos podría reforzar la capacidad de implementación de las políticas.

El análisis del dendrograma Agnes evidencia que la Ley Marco de Ciberseguridad de Chile 2024 está diseñada con un enfoque integral que prioriza la protección de datos, la gestión centralizada y la seguridad nacional. Este análisis jerárquico destaca la coherencia de la normativa y su potencial para enfrentar los desafíos del entorno digital contemporáneo.

Propuesta de Ley de Ciberseguridad (Guatemala, 2024)

Análisis de World Cloud

El análisis de *Word Cloud* permite identificar los elementos clave en el discurso analizado, centrado en la ciberseguridad y la gestión de la información. Las palabras más destacadas como "información", "datos", "sistema" y "seguridad" sugieren que el núcleo del análisis gira en torno a la protección de los recursos digitales en un ambiente tecnológicamente complejo.

Este enfoque resalta la importancia de desarrollar sistemas robustos que salvaguarden la integridad y confidencialidad de la información, mientras se abordan las crecientes amenazas en el ciberespacio. La presencia de términos como

"tecnologías" y "ciberdelitos" también apunta hacia la necesidad de un marco técnico y normativo que permita gestionar de manera eficaz los incidentes cibernéticos.

Figura 1. Análisis de World Cloud de la propuesta Ley de Ciberseguridad de Guatemala

Fuente: elaboración propia.

En un nivel más específico términos como "nacional", "internacional", "cooperación" e "infraestructura" evidencian la amplitud del análisis que abarca, tanto las dinámicas locales como las globales en ciberseguridad. Esto indica que el texto subraya la importancia de la colaboración multisectorial e internacional para enfrentar las amenazas transfronterizas que caracterizan el entorno digital. Palabras como "penal" y "delitos" refuerzan el componente normativo del análisis, sugiriendo que la tipificación de ciberdelitos y la implementación de sanciones legales son elementos críticos en la discusión. La inclusión de términos como "usuarios", "derechos" y "confidencialidad" refleja un énfasis en los derechos digitales, destacando la necesidad de equilibrar la seguridad con la protección de las libertades fundamentales.

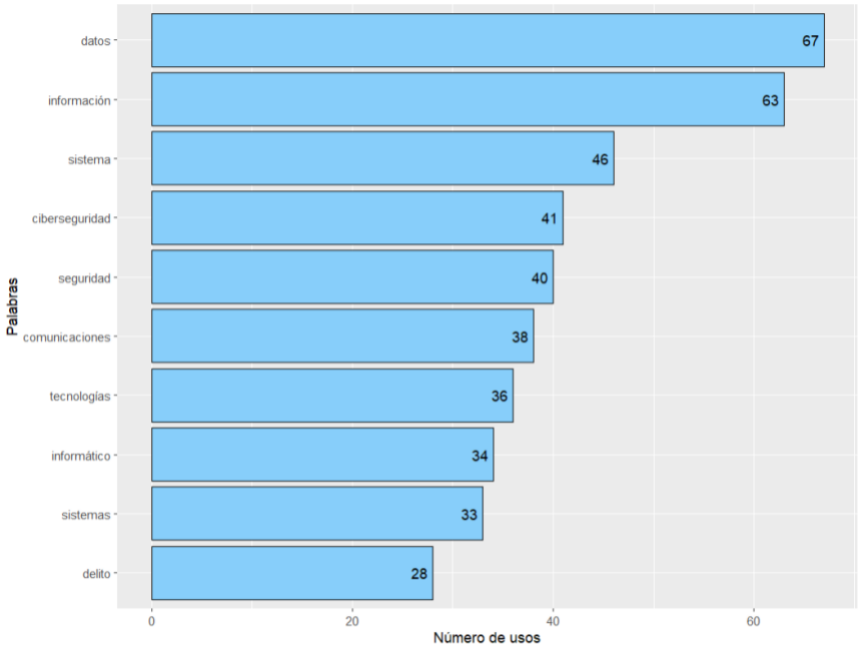
Finalmente, la aparición de palabras "agrícolas" y "años" plantea la posibilidad de que el análisis contemple sectores específicos como el agrícola y aborde cuestiones relacionadas con la evolución de la ciberseguridad en un marco temporal determinado. Esto abre una oportunidad para explorar cómo los avances tecnológicos y las políticas de ciberseguridad impactan en sectores clave de la economía y en los derechos de las comunidades afectadas. En conjunto, la *Word Cloud* refleja un enfoque integral que combina aspectos técnicos, legales, sociales y económicos de la ciberseguridad, ofreciendo una base sólida para desarrollar investigaciones más profundas y propuestas de política pública.

Análisis de diez palabras más citadas

El gráfico de barras sobre las palabras más citadas en la propuesta Ley de Ciberseguridad de Guatemala 2024 ofrece un panorama claro de las prioridades y enfoques centrales de este marco normativo. Los términos "datos" e "información" encabezan la lista con 67 y 63 menciones, respectivamente, los cuales reflejan la importancia que la ley otorga a la protección de la privacidad y la gestión segura de la información en el entorno digital. Este énfasis es coherente con los desafíos contemporáneos, donde la seguridad de los datos personales y sensibles es una preocupación global. Asimismo, palabras como "sistema", "ciberseguridad" y "seguridad" subrayan un enfoque en la gestión técnica y normativa para mitigar riesgos en el ciberespacio.

Términos como "comunicaciones" y "tecnologías" resaltan la inclusión de la infraestructura digital y las herramientas tecnológicas como elementos esenciales en la implementación de medidas de ciberseguridad. Estos conceptos sugieren que la ley aborda no solo la protección de datos, sino también los sistemas y las redes que los sustentan, reconociendo su importancia para garantizar la resiliencia cibernética. Sin embargo, el término "delito", con 28 menciones, enfatiza la dimensión normativa del marco legal, evidenciando un enfoque en la tipificación y sanción de conductas ilícitas en el ciberespacio, lo cual contribuye a fortalecer la confianza en el uso de plataformas digitales y redes informáticas.

Figura 2. Diez palabras más citadas en la propuesta de Ley de Ciberseguridad de Guatemala



Fuente: elaboración propia.

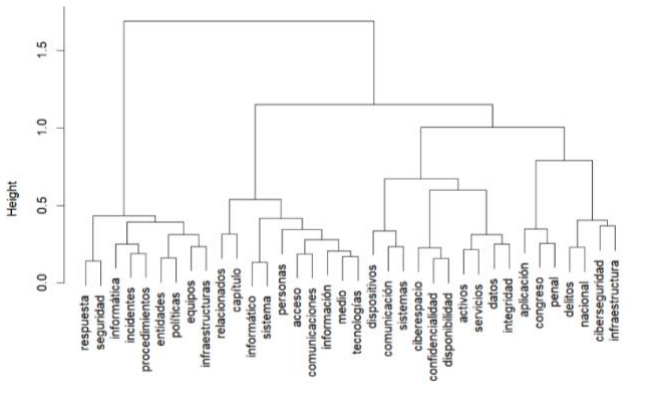
El análisis muestra un equilibrio entre las dimensiones técnicas y normativas de la ley, reflejando su intención de abordar de manera integral los desafíos operativos y legales del entorno digital. Sin embargo, el gráfico también permite inferir áreas potenciales de mejora como la posible inclusión de términos relacionados con la educación digital, la colaboración multisectorial y la innovación tecnológica. Estos elementos son fundamentales para complementar las disposiciones actuales y garantizar que el marco legal no solo responda a las necesidades inmediatas, sino que también anticipe amenazas futuras y fomente un entorno digital seguro y sostenible.

Análisis del dendrograma hclust

El primer dendrograma proporciona una visión jerárquica de la relación entre términos clave de la propuesta de propuesta de Ley de Ciberseguridad de Guatemala 2024, organizándolos según su proximidad semántica y frecuencia en el texto. Este análisis destaca cómo la ley estructura sus prioridades en términos de conceptos técnicos, normativos y sociales, reflejando un enfoque integral en la regulación del ciberespacio. Por ejemplo, términos como "respuesta", "seguridad" e "informática" están agrupados, lo cual sugiere un énfasis en la gestión de incidentes cibernéticos y en la implementación de medidas proactivas de protección.

El clúster que incluye "infraestructuras", "equipos" y "sistemas" resalta la importancia de proteger infraestructuras críticas como redes de telecomunicaciones y bases de datos esenciales para la seguridad nacional. Además, la cercanía entre "personas", "comunicaciones" e "información" refleja un enfoque social en la ley, donde los derechos digitales y la privacidad tienen una posición relevante. Este balance entre elementos técnicos y sociales es fundamental para abordar, tanto las amenazas técnicas como las preocupaciones de los ciudadanos.

Figura 3. Dendrograma de propuesta de Ley de Ciberseguridad de Guatemala 2024 – hclust



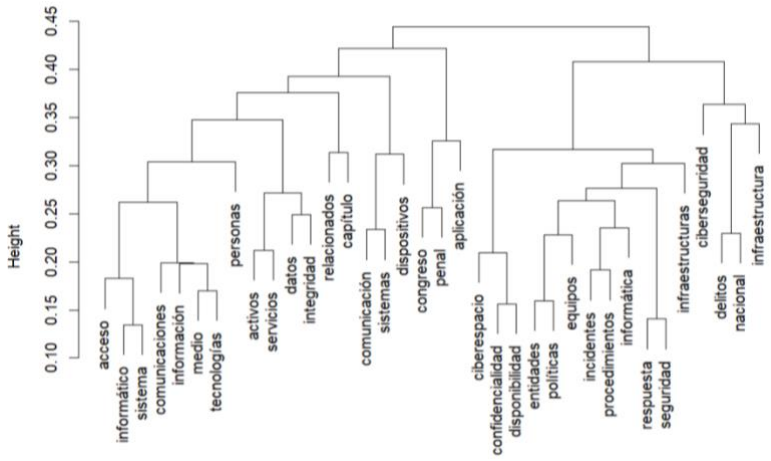
Fuente: elaboración propia.

No obstante, el gráfico también revela algunas áreas que podrían fortalecerse. La ausencia de agrupaciones relacionadas con la cooperación público-privada y la educación digital sugiere un vacío en estos aspectos, que son críticos para desarrollar una ciberseguridad sostenible e inclusiva. Por tanto, sería relevante que futuros ajustes legislativos incorporen estos componentes para garantizar una mayor resiliencia cibernética y participación multisectorial.

Análisis del dendrograma Agnes

El dendrograma generado mediante el método Agnes ofrece una representación jerárquica de los términos clave presentes en la propuesta Ley de Ciberseguridad de Guatemala 2024, destacando cómo se organizan las prioridades normativas, operativas y sociales en el marco legislativo. Un aspecto destacado es el énfasis en la gestión técnica y operativa como lo evidencia el clúster que agrupa términos como "respuesta", "seguridad", "procedimientos" e "informática." Este grupo refleja un enfoque proactivo en la creación de procedimientos y herramientas necesarias para garantizar la seguridad cibernética, subrayando la importancia de la respuesta rápida y efectiva frente a incidentes cibernéticos.

Figura 5. Dendrograma de la propuesta de Ley de Ciberseguridad de Guatemala 2024 – Agne



Fuente: elaboración propia.

Otro clúster relevante es el relacionado con la protección de infraestructuras críticas que incluye términos como "infraestructuras", "ciberseguridad", "delitos" y "nacional". Este agrupamiento resalta la preocupación del marco normativo por proteger los activos estratégicos esenciales para la estabilidad del país, mientras se sancionan las conductas ilícitas que podrían amenazarlos.