Barriers and Solutions in Global Cybersecurity Policy Harmonization: A Systematic Review of Regulatory, Technical, and Sociocultural Challenges

Fernando Antonio Ramos Zaga, Maestro en Gerencia Social[1]
[1]Universidad Privada del Norte, Perú, fernandozaga@gmail.com

Abstract*– In an era marked by the relentless escalation of cyber threats and the transformative impact of technological advancements, the world faces a critical challenge: the urgent need for unified global cybersecurity policies. Despite the glaring necessity, efforts are hindered by fragmented regulations, stark technological inequalities between nations, and deep-seated sociocultural divergences that obstruct cohesive international frameworks. This study aims to identify the key barriers to harmonizing international cybersecurity regulations and propose strategies for their resolution, focusing on regulatory, technical, and sociocultural dimensions. A systematic review was conducted following PRISMA guidelines, utilizing databases such as Web of Science, Scopus, and IEEE Xplore. The findings reveal significant fragmentation in global cybersecurity practices due to misaligned legal frameworks, insufficient infrastructure in developing nations, and divergent cultural perceptions of privacy and security. Challenges include the technological divide, lack of standardized protocols, and limited collaboration between public and private sectors. In conclusion, effective global cybersecurity governance requires inclusive strategies that bridge regulatory gaps, promote international collaboration, and address technological and cultural disparities.

Keywords*-- Cybersecurity governance, cybersecurity policy, cyber norms, cyber sovereignty, cybersecurity standards.

Desafíos y estrategias para la armonización de políticas de ciberseguridad global: Revisión sistemática de literatura

Fernando Antonio Ramos Zaga, Maestro en Gerencia Social[1]
[1]Universidad Privada del Norte, Perú, fernandozaga@gmail.com

Resumen–En una era definida por el crecimiento constante de las ciberamenazas y el impacto transformador de los avances tecnológicos, el mundo enfrenta un desafío crítico: la urgente necesidad de establecer políticas globales unificadas de ciberseguridad. Sin embargo, a pesar de su evidente importancia, estos esfuerzos se ven obstaculizados por normativas fragmentadas, desigualdades tecnológicas entre las naciones y profundas diferencias socioculturales que dificultan la cohesión de los marcos internacionales. En ese sentido, el presente artículo tiene por objetivo identificar los principales obstáculos para la armonización de las normativas internacionales de ciberseguridad y proponer estrategias para superarlos, abordando las dimensiones normativa, técnica y sociocultural. Para ello, se llevó a cabo una revisión sistemática siguiendo las directrices PRISMA, utilizando bases de datos reconocidas como Web of Science, Scopus e IEEE Xplore. Los resultados evidencian una significativa fragmentación en las prácticas globales de ciberseguridad, derivada de la desalineación de los marcos jurídicos, la insuficiencia de infraestructuras en los países en desarrollo y las divergentes percepciones culturales sobre privacidad y seguridad. Entre los desafíos más relevantes se encuentran la brecha tecnológica, la ausencia de protocolos estandarizados y la limitada cooperación entre los sectores público y privado. En conclusión, la gobernanza eficaz de la ciberseguridad a nivel global requiere estrategias integradoras que eliminen las disparidades normativas, fomenten la cooperación internacional y aborden las desigualdades tecnológicas y culturales, promoviendo así un entorno digital más seguro y resiliente.

Palabras clave-- gobernanza de la ciberseguridad, políticas de ciberseguridad, cibernormas, cibersoberanía, estándares de ciberseguridad.

I. Introducción

El desarrollo de normas internacionales de ciberseguridad y de una cibergobernanza responsable, en particular en el ámbito de las Naciones Unidas (ONU), sigue siendo una cuestión crítica en el cambiante ámbito del ciberespacio [1], cuyos esfuerzos se centran en la creación de marcos regulatorios, abordando los avances tecnológicos y la interconexión de las infraestructuras digitales mundiales [2], [3]. Ante este escenario, los responsables políticos deben de las naciones abordan las complejidades de los sistemas digitales internacionales adaptándose al mismo tiempo a un panorama tecnológico dinámico para mantener su cibersoberanía [4].

En el ámbito académico, las contribuciones de Duncan Hollis y Martha Finnemore aportan ideas fundamentales sobre la gobernanza cibernética [5], los cuales hacen hincapié en enfoques jurídicos estructurados para entender la soberanía y la jurisdicción de los Estados en el ciberespacio, cruciales para desarrollar estándares internacionales en ciberseguridad. Por ese motivo, se destaca la necesidad de que las naciones equilibren sus intereses con la colaboración internacional, abordando las cambiantes dinámicas de poder, control y responsabilidad en el ámbito digital.

La naturaleza omnipresente de los riesgos cibernéticos exige una exploración académica y política exhaustiva de la ciberregulación mundial. Debido a las vulnerabilidades digitales planteando amenazas significativas a la seguridad mundial, la comprensión de la evolución en la regulación de la ciberseguridad es esencial para los estudiosos y los responsables políticos [6]. Asimismo, la ONU desempeña un papel central en el fomento de la cooperación internacional y la creación de consenso, cruciales para mitigar las ciberamenazas [7], los cuales contribuyen a comprender la compleja interacción entre la ciberdefensa y los retos globales más amplios.

En una era digital interconectada, las directrices internacionales sobre ciberseguridad han adquirido una importancia creciente. La escalada de incidentes cibernéticos dirigidos contra infraestructuras críticas, procesos electorales e información sensible pone de relieve la gravedad de estas amenazas para la estabilidad nacional y mundial [8]. Por ese motivo, los protocolos normalizados de conducta estatal en el ciberespacio son vitales para mitigar los riesgos y fomentar un entorno cibernético seguro a fin de disuadir las actividades maliciosas y fomentan estrategias globales cohesionadas, dando forma a enfoques estratégicos eficaces.

Ante lo antes señalado, el objetivo del presente artículo es identificar los principales obstáculos a la armonización de las normativas internacionales de ciberseguridad y proponer estrategias para su resolución, centrándose en las dimensiones normativa, técnica y sociocultural. A medida que las amenazas cibernéticas crecen en sofisticación y escala, la cooperación global y las políticas unificadas se han vuelto imperativas, a fin de establecer marcos cohesivos para la gobernanza mundial de la ciberseguridad, abordando los complejos retos de su regulación internacional.

II. Metodología

La revisión se adhirió a las directrices PRISMA para garantizar la fiabilidad y reproducibilidad, el cual facilitó el proceso de selección, los criterios de elegibilidad de los estudios y la síntesis de datos, minimizando los errores

sistemáticos y las omisiones. El estudio utilizó múltiples bases de datos de renombre, tales como Web of Science (WoS), Scopus e IEEE Xplore, para garantizar una cobertura exhaustiva de la literatura sobre ciberseguridad, regulación y política, así como por su alto impacto y amplio alcance. Los términos de búsqueda incluían *cybersecurity regulation, regulatory barriers, policy implementation, compliance challenges, governance frameworks*, combinados mediante operadores booleanos para optimizar tanto la precisión como la amplitud.

La fórmula de búsqueda utilizada para títulos y resúmenes fue:
(cybersecurity AND regulation AND (barriers OR implementation OR policy))
La búsqueda se limitó a publicaciones de los últimos cinco años para garantizar la inclusión de las investigaciones más actuales, lo que refleja el panorama dinámico y en rápida evolución de la ciberseguridad.

Los criterios de inclusión se centraron en investigaciones sobre los obstáculos normativos, tecnológicos o socioculturales a la aplicación de políticas de ciberseguridad, publicados en revistas arbitradas por pares en los últimos cinco años. Los estudios requerían una transparencia de datos suficiente para un análisis crítico y un acceso completo a la información. Los criterios de exclusión eliminaron los estudios no empíricos, las publicaciones fuera del intervalo de cinco años y los que carecían de rigor metodológico, identificación clara de la población objetivo o datos suficientes para un análisis exhaustivo. Asimismo, se excluyeron los estudios que no abordaban los retos normativos pertinentes sobre regulación de la ciberseguridad.

La sistemática se ciñó estrictamente a los criterios de inclusión y exclusión, garantizando que el proceso de selección fuera transparente, organizado y libre de sesgos. Durante todo el proceso se siguieron directrices éticas, incluida la cita adecuada de todas las fuentes para mantener la integridad académica y evitar el plagio. No se manipuló ningún dato de los estudios seleccionados; todos los resultados se presentaron de forma precisa y objetiva, reflejando la verdadera forma de los datos originales, lo cual garantizó la fiabilidad y credibilidad de la revisión realizada.

III. Resultados

Se realizó una búsqueda sistemática en múltiples bases de datos electrónicas, la cual identificó un total de 1.421 artículos. El desglose por bases de datos es el siguiente: Web of Science devolvió 237 artículos, Scopus 626 artículos, IEEE Xplore 558 artículos, con muchos duplicados de otras fuentes.

La recuperación inicial de 1.421 artículos contenía numerosos duplicados. Se utilizó el software de gestión de referencias Zotero para automatizar el proceso de eliminación de duplicados, eliminando 325 duplicados en función del título, la autoría y el año de publicación. Esto redujo el conjunto de datos a 1.096 artículos únicos, preparados para su posterior selección según los criterios establecidos.

Tras el filtro por duplicación, se examinaron 1.096 artículos a partir de los títulos y resúmenes para afinar aún más la selección. En esta fase se comprobó que los estudios abordaban los obstáculos a la armonización de la normativa internacional sobre ciberseguridad. Se excluyeron los artículos que se centraban en áreas no relacionadas, como soluciones tecnológicas generales, editoriales, o que carecían de datos empíricos. Se excluyeron 1.013 artículos, de modo que quedaron 83 para la revisión del texto completo.

La revisión del texto completo incluyó una evaluación detallada de 83 artículos preseleccionados. De ellos, 78 fueron accesibles y se analizaron, mientras que 5 se excluyeron por ser de pago o no estar disponibles. Durante el proceso de confirmación de la elegibilidad, 13 estudios no cumplían los criterios de inclusión, 7 estudios presentaban resultados no pertinentes y 3 estudios carecían de una metodología apropiada. Tras aplicar estos criterios, se consideraron 55 artículos que cumplían los criterios de inclusión y se consideraron pertinentes para la posterior extracción y análisis de datos.

A continuación, se presenta el diagrama de flujo PRISMA que ilustra el proceso de selección y extracción de datos, detallando las etapas de identificación, cribado, elegibilidad e inclusión de los estudios analizados.

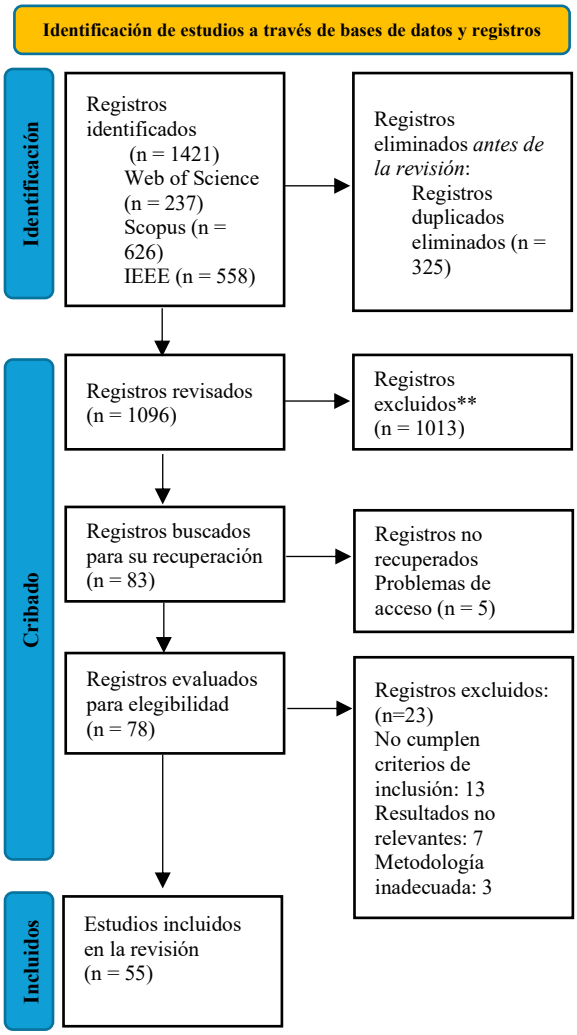

Fig. 1 Diagrama de flujo PRISMA para selección y extracción de datos

A. Barreras regulatorias globales

TABLA I
BARRERAS REGULATORIAS DE LA GOBERNANZA GLOBAL DE LA CIBERSEGURIDAD

Temática	Subtemática	Autor(es)
Desafíos regulatorios globales	Fragmentación normativa	AllahRakha [9]
	Definiciones divergentes de amenazas	Adeyeri & Abroshan [10]
	Políticas nacionales vs globales	Alshabib & Martins [11]
Estándares y políticas nacionales	Reglamentación de privacidad y datos	Mishra et al. [12]
	Soberanía y proteccionismo	Heim [13]
	Costos de alineación normativa	Santaniello & Barbieri [14]
	Limitaciones de recursos	Atkins & Lawson [15]
Capacidades de aplicación de la ley	Infraestructura y experiencia técnica	Alfiyah [16]
	Disparidades entre países	Saleem et al. [17]
Barreras legales y cooperación	Privacidad y protección de datos	Macidov [18]

La Tabla I sintetiza las principales barreras regulatorias en la gobernanza global de la ciberseguridad, incluyendo desafíos regulatorios globales, estándares y políticas nacionales, capacidades de aplicación de la ley barreras legales y de cooperación. Se exploran temas como la fragmentación normativa, las discrepancias entre políticas nacionales y globales, las limitaciones en infraestructura y recursos para la aplicación de la ley, así como las dificultades en privacidad y protección de datos en el ámbito legal y cooperativo.

El panorama normativo mundial de la ciberseguridad se enfrenta a importantes obstáculos debido a la falta de compatibilidad entre los marcos nacionales e internacionales [9], los cuales surgen de los diferentes enfoques jurídicos para hacer frente a las amenazas cibernéticas, que van desde la ciberdelincuencia a la ciberguerra patrocinada por los Estados [10]. Asimismo, las variaciones en las definiciones y respuestas a estas amenazas complican la creación de políticas globales cohesivas [11].

Algunas naciones adoptan definiciones restringidas de las ciberamenazas, mientras que otras adoptan enfoques más amplios. Las diferencias en las normas nacionales de protección de datos, ciberdefensa y gestión de incidentes fragmentan aún más los esfuerzos de ciberseguridad. Por ejemplo, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea impone estrictos requisitos de privacidad de datos, mientras que muchos otros países tienen normativas menos exhaustivas, lo que complica la cooperación transfronteriza [12].

La desalineación entre las leyes nacionales y los marcos internacionales, como el GDPR o la Estrategia Global de Ciberseguridad de las Naciones Unidas, exacerba estos problemas. Muchas naciones dan prioridad a la soberanía y la seguridad nacionales, resistiéndose a menudo a las normas

internacionales. Las políticas proteccionistas que restringen las tecnologías extranjeras o los flujos de datos también obstaculizan la colaboración, dando lugar a prácticas fragmentadas entre jurisdicciones [13].

Armonizar la legislación nacional con las normas internacionales es especialmente difícil en países con sistemas políticos, económicos o de gobernanza diferentes. Los regímenes autoritarios suelen rechazar normas mundiales como el RGPD, por considerarlas una amenaza para el control del Estado. Inclusive en los países democráticos, las preocupaciones sociopolíticas y económicas pueden obstaculizar la adaptación a las normas internacionales [14]. La actualización de los marcos jurídicos para cumplir las normas mundiales es costosa y compleja, pues requiere importantes inversiones en infraestructuras, conocimientos jurídicos y reformas políticas. Para los países con recursos limitados, estos retos son más pronunciados, ampliando la brecha entre las expectativas internacionales y las capacidades nacionales [15].

Los retos que plantea la aplicación de la normativa internacional en materia de ciberseguridad son mayores en regiones con marcos jurídicos débiles, como sucede con muchos países en vías de desarrollo, debido a que carecen a menudo de los sistemas judiciales, los conocimientos técnicos y la infraestructura necesarios para aplicar leyes eficaces de ciberseguridad. Por otro lado, la inestabilidad política y la escasa coordinación entre organismos complican aún más la creación y aplicación de tales políticas. La escasez de recursos para investigar los ciberdelitos o proteger las infraestructuras críticas agrava las dificultades para ajustarse a las normas internacionales [16].

La capacidad de hacer cumplir la legislación varía considerablemente de un país a otro, lo que crea un entorno mundial de ciberseguridad fragmentado. Las naciones desarrolladas, con recursos tecnológicos avanzados, están mejor equipadas para hacer cumplir las leyes de ciberseguridad, mientras que los países menos desarrollados luchan por establecer marcos básicos. Ante estas disparidades, que permiten a los ciberdelincuentes aprovecharse de los sistemas jurídicos más débiles, se socavan los esfuerzos mundiales para hacer frente a las ciberamenazas. Las diferencias políticas, económicas y culturales dificultan aún más la cooperación internacional, complicando las respuestas transnacionales a la ciberdelincuencia [17].

Las barreras legales, como las discrepancias en las leyes de privacidad y protección de datos, a menudo obstaculizan la cooperación transnacional en ciberseguridad. Por ejemplo, los estrictos requisitos del GDPR de la UE limitan el intercambio transfronterizo de información, incluso con fines policiales. Los tratados de extradición desactualizados o insuficientes aumentan la complejidad de la detención de los ciberdelincuentes que operan a escala internacional. Adicionalmente, las variaciones en las definiciones jurídicas de la ciberdelincuencia en las distintas jurisdicciones complican aún más las investigaciones y los enjuiciamientos, creando lagunas jurídicas que permiten a los ciberdelincuentes eludir la justicia y debilitando los esfuerzos mundiales para combatir eficazmente las ciberamenazas [18].

B. Barreras tecnológicas y operativos

TABLA II
BARRERAS TECNOLÓGICAS Y OPERATIVAS DE LA GOBERNANZA GLOBAL DE LA CIBERSEGURIDAD

Temática	Autores
Brecha tecnológica y desafíos infraestructurales	Creese, Dutton, Esteve-González, et al. [56]; Tijerina [20]; Khan et al. [21]; Soldani [22]
Acceso a tecnologías avanzadas	Zaid & Garai [23]; Ani et al. [24]; Peter [25]; Qobo [26]; Ogwueleka [27]
Protección de infraestructura crítica	Venkatachary et al. [28]; Javaid et al. [29]; Saeed et al. [30]; Cartwright [31]
Desafíos de interoperabilidad	Henderson [32]; Kulesza & Weber [33]; Chen & Yang [34]
Colaboración público-privada	Grigaliūnas et al. [35]; Nwankwo et al. [36]; Pawar & Palivela [37]; Arshad & Asghar [38]; Safitra et al. [39]; Wylde et al. [40]
Tensiones geopolíticas y políticas nacionales	Hassib & Shires [41]; Racionero-Garcia & Shaikh [42]
Compatibilidad tecnológica	Möller [43]; Usmani et al. [44]; Szczepaniuk & Szczepaniuk [45]

La Tabla II detalla las principales barreras tecnológicas y operativas en la gobernanza global de la ciberseguridad. Aborda la brecha tecnológica y los desafíos infraestructurales, el acceso a tecnologías avanzadas y la protección de infraestructura crítica. Además, se analiza los desafíos de interoperabilidad, la colaboración público-privada, las tensiones geopolíticas y políticas nacionales, así como la compatibilidad tecnológica, destacando los factores clave que dificultan la implementación de una gobernanza efectiva.

La aplicación efectiva de la normativa internacional sobre ciberseguridad se enfrenta a importantes retos técnológicos y operativos, derivados principalmente de las brechas en la infraestructura tecnológica mundial. Un problema crítico es la brecha tecnológica entre los países desarrollados y los países en vías de desarrollo [19], [20]. Muchos países emergentes enfrentan desafíos con infraestructuras inadecuadas, conectividad limitada, redes poco fiables y acceso limitado a la banda ancha [21]. Los desafíos antes mencionados son especialmente pronunciadas en regiones donde el despliegue de la 5G es aún incipiente, lo que deja los sistemas críticos expuestos a ciberamenazas y complica la adhesión a las normas mundiales de ciberseguridad [22].

La falta de acceso a tecnologías avanzadas de ciberseguridad constituye un obstáculo considerable en muchos países en vías desarrollo. Las herramientas de alta gama, como los sistemas de detección de intrusos, las soluciones de seguridad basadas en inteligencia artificial y los sofisticados mecanismos de cifrado, suelen ser inaccesibles o demasiado costosas [23]. Asimismo, la brecha tecnológica se ve agravada por la escasez de personal cualificado capaz de gestionar dichas herramientas, lo que hace que se dependa de ayuda externa [24], lo cual permite a las naciones con mayores recursos establecer sólidos marcos de ciberseguridad, mientras que las naciones

más pobres siguen expuestas a los ciberataques, lo que no solo aumenta los riesgos de seguridad, sino que también amplía la brecha económica, ya que los países en desarrollo a menudo dependen de la ayuda extranjera o de tecnologías importadas, que pueden comprometer la soberanía local e introducir vulnerabilidades adicionales[25], [26], [27].

La protección de las infraestructuras críticas pone de manifiesto la vulnerabilidad de sectores como la energía, la sanidad y las telecomunicaciones, debido a que son objetivos frecuentes de los ciberdelincuentes, ya que en muchos países en desarrollo carecen de medidas adecuadas para proteger estos sistemas vitales [28], [29], [30], [31]. Por otro lado, la ausencia de instrumentos internacionales universalmente vinculantes para la protección de infraestructuras críticas agrava esta vulnerabilidad. Ante esta situación, sin normas aplicables, las medidas de seguridad varían mucho de un país a otro, lo que se traduce en niveles de protección desiguales en todo el mundo.

Los problemas de interoperabilidad complican aún más los esfuerzos por reforzar la ciberseguridad mundial. La falta de protocolos normalizados entre países y organizaciones impide una colaboración transfronteriza eficaz [32], [33], [34] . Marcos como ISO/IEC 27001 proporcionan directrices para la seguridad de la información, pero la ausencia de normas mundiales obligatorias fragmenta las prácticas de seguridad y debilita los mecanismos de defensas ante ataques cibernéticos. Además, la insuficiente cooperación entre los sectores público y privado agrava esta fragmentación [35], [36], [37], [38]. Las empresas privadas suelen mostrar reticencia a compartir información sobre incidentes cibernéticos por temor a posibles repercusiones legales y daños a su reputación, mientras que las regulaciones gubernamentales pueden limitar la flexibilidad de estas entidades para hacer frente a las amenazas emergentes [39], [40].

Las tensiones geopolíticas y los conflictos entre las prioridades de seguridad nacional crean obstáculos adicionales a nivel internacional. Los desacuerdos entre las naciones respecto a las políticas de ciberseguridad pueden retrasar o impedir el desarrollo de estrategias globales cohesionadas, especialmente ante ciberataques transnacionales que exigen respuestas rápidas y coordinadas [41], [42]. Además, las incompatibilidades tecnológicas también dificultan la colaboración transfronteriza, ya que las diferencias entre sistemas operativos, plataformas y lenguajes de programación impiden la interoperabilidad entre las herramientas de ciberseguridad desarrolladas por gobiernos, empresas privadas y organizaciones internacionales. Por ende, la falta de integración de los marcos regulatorios en ciberseguridad socava los esfuerzos por crear soluciones integrales que puedan funcionar eficazmente en todas las jurisdicciones, debilitando la capacidad mundial para proteger la infraestructura digital y combatir la ciberdelincuencia [43], [44], [45].

C. Barreras culturales y sociales

TABLA III
BARRERAS CULTURALES Y SOCIALES DE LA GOBERNANZA GLOBAL DE LA CIBERSEGURIDAD

Tema	Subtema	Autores Citados
Cultural y sociales	Diversidad cultural	Uchendu et al. [46]; AlDaajeh & Alrabaee [47]; Alhalafi & Veeraraghavan [48]; Sadeghi et al. [49]
	Percepciones regionales	Dodge et al. [50]; Yusif & Hafeez-Baig [51]
	Actitudes hacia la privacidad	Wang [52]; Balarabe [53]; Zuboff [54]; Bridenbaker [55]
	Tradiciones de derechos civiles	Creese, Dutton, & Esteve-González [56]; Kharlamov & Pogrebna [57]
	Equilibrio ciberseguridad-privacidad	Renaud et al. [58]
Privacidad y normativa	Regulaciones internacionales	Ameen et al. [59]
	Resistencia normativa	Raymond & Sherman [60]
Desafíos institucionales	Gobiernos autoritarios	Bokhari [61]
	Empresas privadas	Song & Park [62]; Chandna & Tiwari [63]

La Tabla III aborda las barreras culturales, sociales, normativas e institucionales que afectan la gobernanza global de la ciberseguridad. En el ámbito cultural y social, se destacan la diversidad cultural, las percepciones regionales, las actitudes hacia la privacidad, las tradiciones de derechos civiles y el equilibrio entre ciberseguridad y privacidad. En cuanto a privacidad y normativa, se analizan las regulaciones internacionales y la resistencia normativa. Por otro lado, respecto a los desafíos institucionales, se abordan las dinámicas en gobiernos autoritarios y el rol de las empresas privadas en este contexto.

Los factores culturales y sociales plantean importantes retos a la formulación y aplicación de políticas universales de ciberseguridad [46], [47], [48], [49]. Las percepciones regionales de la privacidad y la seguridad varían mucho, lo que influye tanto en la aceptación como en la eficacia de las políticas [50], [51]. En las democracias occidentales, la privacidad es considerado como un derecho fundamental e inalienable, mientras que en las sociedades autoritarias o colectivistas tiende a ser subordinada a la seguridad nacional o intereses sociales más amplios. De ese modo, bajo estos principios, se definen las respuestas regulatorias a actividades tales como la recopilación de datos, la vigilancia y el intercambio de información. Las culturas que valoran privacidad pueden oponerse a estas medidas, mientras que aquellas más familiarizadas con la vigilancia tienden a aceptarlas si las perciben como esenciales para el bienestar o la seguridad pública [52], [53], [54], [55].

Las normas culturales también influyen en la implementación de las políticas. En sociedades con una sólida

tradición de derechos civiles, medidas como la vigilancia masiva o la retención extensiva de datos suelen enfrentar resistencia debido a la preocupación por las libertades individuales [56], [57]. Por el contrario, en regiones en las que la intervención gubernamental está normalizada, es menos probable que estas políticas encuentren oposición por parte de la sociedad civil. En ese sentido, lograr un equilibrio entre medidas eficaces de ciberseguridad y el respeto de la privacidad y las libertades se convierte en un reto persistente [58]

Los esfuerzos para establecer normas globales en ciberseguridad deben tener en cuenta estas diferencias culturales, a fin de abordar los desafíos regulatorios pertinentes. Por ejemplo, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que establece normas estrictas de privacidad a nivel mundial, puede ser considerado demasiado restrictivo por naciones que evidencien diferentes puntos de vista sobre la privacidad [59]. Tal es el caso de los regímenes autoritarios, los cuales pueden oponerse al cumplimiento de estas normas internacionales, percibiéndolas como amenazas a su soberanía [60].

La resistencia al cambio por parte de gobiernos y empresas privadas complica aún más la implementación global de marcos de ciberseguridad. Los gobiernos con estructuras centralizadas o autoritarias se enfrentan a menudo a la inercia burocrática, la desorganización interinstitucional y la oposición a la regulación externa, lo cual da lugar a políticas fragmentadas y retrasos en la adopción de normas internacionales. Asimismo, algunos gobiernos también se resisten a la normativa internacional, por considerarla una restricción de su control sobre la información [61].

Las empresas privadas, especialmente las pequeñas y medianas, suelen mostrar resistencia a la adopción de nuevas normativas de ciberseguridad debido a preocupaciones relacionadas con los costos, la complejidad y el impacto en sus operaciones. El cumplimiento de las normas internacionales exige importantes inversiones en infraestructura, formación y protección de datos, que a menudo resultan onerosas para las empresas con recursos limitados. Además, las empresas pueden mostrarse reticentes a la hora de compartir información sobre ciberamenazas o infracciones, debido al temor ante posibles daños a su reputación o a la pérdida de ventaja competitiva [62], [63].

IV. Discusión

Los resultados de esta revisión ponen de relieve la naturaleza polifacética de los retos de la ciberseguridad global, revelando disparidades significativas en las dimensiones regulatoria, tecnológica y cultural. De acuerdo con la revisión de literatura existente, los resultados subrayan la tensión entre las normas internacionales de ciberseguridad y la fragmentación impulsada por la soberanía nacional, la desigualdad económica y las diferencias socioculturales.

Autores como AllahRakha [9] y Adeyeri y Abroshan [10] identifican la incompatibilidad entre los marcos nacionales e internacionales como un obstáculo primario, agravado por definiciones jurídicas y capacidades de aplicación divergentes, tal como ilustran Alshabib y Martins [11]. Al respecto, Mishra et al. [12] analizan cómo las normativas estrictas, como el GDPR de la UE, podrían generar obstáculos operativos para la cooperación transfronteriza. Mientras que Heim [13] critica el desajuste entre las políticas soberanas y las iniciativas mundiales, Santaniello y Barbieri [14] atribuyen la falta de consenso a las disparidades políticas y de gobernanza.

Desde una perspectiva tecnológica, la brecha tecnológica entre las naciones desarrolladas y en desarrollo es un problema persistente, tal como señalan Creese et al. [56] y Khan et al. [21]. Las naciones avanzadas aplican medidas sólidas, mientras que las naciones en vías de desarrollo luchan debido a sus recursos y conocimientos limitados, pues dependen de soluciones externas que socavan la autonomía local [23]. En ese sentido, las disparidades perpetúan las desigualdades económicas y las vulnerabilidades, como subrayan Javaid et al. [29] y Saeed et al. [30].

Los problemas de interoperabilidad dificultan aún más el avance en la regulación de la ciberseguridad. La ausencia de protocolos normalizados, como señalan Henderson [32] y Kulesza & Weber [33], debilita la cooperación internacional. A pesar de la existencia de marcos como ISO/IEC 27001, la falta de normas mundiales vinculantes crea prácticas fragmentadas, agravadas por una colaboración inadecuada entre los sectores público y privado [35]. Las entidades privadas suelen mostrarse reacias a compartir información debido a preocupaciones legales y de reputación [37].

Las dimensiones culturales y sociales añaden complejidad al asunto. Las percepciones divergentes de la privacidad y la seguridad, como señalan Uchendu et al. [46] y Sadeghi et al. [49], influyen en la aceptación y la aplicación de las políticas. Las naciones democráticas priorizan las libertades civiles, y con frecuencia, se oponen a medidas como la vigilancia masiva [50], mientras que las sociedades colectivistas pueden dar prioridad a la seguridad sobre las libertades personales [52], lo cual impide la armonización de las normas mundiales y reflejan retos éticos y políticos más amplios.

Los gobiernos y las empresas privadas también se muestran reacios a adoptar normas internacionales. La inercia burocrática y las limitaciones financieras disuaden de su cumplimiento, especialmente a las PYME con recursos limitados [63]. Ante esta situación se requieren enfoques flexibles y rentables para fomentar una adopción más amplia sin comprometer la viabilidad operativa.

La presente revisión revela que los retos mundiales de la ciberseguridad están interconectados. Los desajustes normativos, las disparidades tecnológicas y las diferencias culturales se refuerzan mutuamente, formando una compleja red de barreras. Abordar estos problemas requiere estrategias integradoras que tengan en cuenta los diversos contextos políticos, económicos y culturales, fomentando al mismo tiempo la cooperación internacional y la distribución equitativa de los recursos. Tales enfoques, como sugiere la bibliografía revisada, son esenciales para colmar las lagunas de la

ciberseguridad mundial y construir infraestructuras digitales resistentes.

El proceso de revisión, aunque riguroso, tiene limitaciones. La dependencia de los estudios en lengua inglesa puede excluir pruebas relevantes, así como la dependencia de las bases de datos electrónicas puede pasar por alto la literatura gris. La heterogeneidad de metodologías y definiciones limitó la comparabilidad. La naturaleza dinámica de la ciberseguridad implica que algunas conclusiones puedan quedar obsoleta, lo que subraya la importancia de contar con actualizaciones continuas.

En conclusión, es crucial adoptar enfoques coordinados e integradores para la gobernanza mundial de la ciberseguridad. Los responsables políticos deben diseñar normas internacionales flexibles que se adapten a los diversos contextos sociopolíticos, al tiempo que promueven la colaboración y el intercambio de recursos. Asimismo, el fortalecimiento de capacidades en los países en desarrollo, a través de inversiones en infraestructura, tecnología y formación, resulta esencial para cerrar las brechas en ciberseguridad. La investigación futura debería abordar cuestiones como la sostenibilidad a largo plazo de los marcos regulatorios, la participación del sector privado y el impacto de tecnologías emergentes como la inteligencia artificial, mediante enfoques multidisciplinares que permitan alinear las políticas emergentes con el cambiante panorama de ciberamenazas.

V. Estrategias para la armonización de las políticas de ciberseguridad

A. Desarrollo de un marco normativo internacional unificado

Un marco internacional unificado de ciberseguridad es esencial para hacer frente a las crecientes amenazas cibernéticas a nivel global, ya que permite establecer estándares mínimos para la seguridad de los datos, la gestión de riesgos y la notificación de incidentes. Además, garantiza su aplicación universal en diversos entornos tecnológicos y normativos, promoviendo un enfoque un enfoque coherente y eficaz en la protección cibernética a nivel mundial. El reconocimiento de la privacidad de los datos como un derecho humano fundamental establecería normas internacionales para la protección de la información personal, con un enfoque especial en la computación en la nube y los flujos de datos transfronterizos, a fin de armonizar legislaciones regionales, como el GDPR de la UE, con estándares globales. Por otro lado, la implementación de protocolos de protección de datos, que incluyan métodos avanzados de cifrado y comunicación segura, reforzaría la seguridad tanto durante la transmisión como en el almacenamiento de la información.

Un organismo global de gobernanza de la ciberseguridad desempeñaría un papel fundamental en la coordinación de los esfuerzos internacionales, estableciendo estándares, brindando apoyo técnico y alineando las estrategias nacionales con los marcos globales. Siguiendo el modelo de organizaciones como la UIT (Unión Internacional de Telecomunicaciones), se podría involucrar a gobiernos, empresas y sociedad civil en la implementación de políticas, la reducción de brechas tecnológicas y la promoción de la cooperación con entidades como la ONU y la OEA. Las funciones clave de este organismo incluirían la auditoría de las políticas nacionales de ciberseguridad para garantizar su conformidad con las normativas globales, así como la integración de la ciberseguridad en marcos de seguridad más amplios, fortaleciendo la resiliencia digital a nivel mundial.

Los mecanismos neutrales de mediación y resolución de conflictos son esenciales para armonizar las diferencias entre normativas nacionales, como las leyes de privacidad y las políticas de protección de datos. Los sistemas dirigidos por expertos garantizarían la soberanía nacional mientras promueven la coherencia regulatoria. Por otro lado, una cámara de arbitraje internacional proporcionaría soluciones rápidas y vinculantes a desafíos como los flujos de datos transfronterizos y los ciberataques, fomentando la transparencia y la confianza. Bajo este enfoque colaborativo, se fortalecería un marco global de ciberseguridad fundamentado en la confianza mutua y la responsabilidad compartida.

B. Fomento de la cooperación internacional

La cooperación internacional es fundamental para enfrentar los desafíos de la ciberseguridad a nivel global. Los acuerdos multilaterales y regionales, promovidos por organizaciones como la OEA, la ASEAN, el G7 y el G20, facilitan el intercambio estructurado de información, la coordinación en defensa y la formulación de políticas. No obstante, las diferencias en prioridades nacionales, capacidades tecnológicas y marcos normativos representan obstáculos significativos para el avance. Para abordar estos desafíos, resulta crucial fortalecer la capacidad institucional, alinear las estrategias nacionales con los objetivos globales y promover acuerdos regionales que permitan enfrentar amenazas específicas, como los ataques a infraestructuras críticas. Asimismo, los tratados bilaterales y multilaterales, junto con las disposiciones sobre ciberseguridad incluidas en los acuerdos comerciales, podrían fortalecer la seguridad colectiva.

La cooperación transnacional es fundamental para combatir la ciberdelincuencia, que a menudo trasciende las fronteras. Grupos de trabajo conjuntos de expertos en ciberseguridad, fuerzas de seguridad y fiscales pueden facilitar las investigaciones supranacionales. Acuerdos como el Convenio de Budapest abordan los retos jurisdiccionales, mientras que los protocolos de seguridad garantizan la integridad de las pruebas digitales compartidas. Los tratados de extradición y las bases de datos penales internacionales permiten superar las barreras legales y a seguir la pista de los delincuentes.

La colaboración entre el sector público y privado fortalece la resiliencia en ciberseguridad. Los incentivos financieros, los marcos normativos y la creación de consorcios público-privados impulsan la participación del sector privado y fomentan la innovación en tecnologías emergentes como la inteligencia artificial, la cadena de bloques y la computación cuántica. Establecer marcos jurídicos claros para el intercambio seguro de información no solo promueve la confianza entre las

partes, sino que también asegura el cumplimiento de las normativas de privacidad.

Las plataformas mundiales de intercambio de información sobre ciberamenazas mejoran los esfuerzos de defensa a nivel mundial. Las bases de datos centralizadas sobre amenazas y vulnerabilidades, junto con protocolos estandarizados para el intercambio de datos y sistemas de alerta temprana, facilita la coordinación eficaz frente riesgos emergentes. Además, los centros internacionales de investigación especializados en ciberseguridad contribuyen significativamente el desarrollo de competencias y la resiliencia global.

C. Capacitación y transferencia de tecnología

Desarrollar capacidades de ciberseguridad en países en desarrollo es crucial para la defensa global. La falta de recursos, talento e infraestructuras dificulta su respuesta a amenazas avanzadas. Las iniciativas efectivas deben incluir formación específica, evaluaciones de riesgos y planes de estudio adaptados a necesidades locales y globales. La colaboración con instituciones internacionales para integrar tecnologías emergentes como IA y blockchain impulsa la innovación y el intercambio de conocimientos. Por ende, las becas, programas de intercambio y plataformas de aprendizaje en línea pueden superar barreras económicas y geográficas, fortaleciendo el capital humano.

Reforzar la infraestructura global requiere transferencias tecnológicas mediante alianzas internacionales, especialmente público-privadas, las cuales pueden proporcionan herramientas clave como cifrado y cortafuegos, además de fomentar la investigación en amenazas emergentes. Asimismo, el financiamiento a través de subvenciones y marcos normativos adecuados facilita su adopción en sectores críticos como energía y salud.

Para una defensa global cohesionada, es clave la alineación con normativas internacionales. La asistencia técnica especializada y la creación de agencias de ciberseguridad son esenciales para cerrar brechas legales, tecnológicas e infraestructurales mediante auditorías transparentes, promoviendo la confianza y la resiliencia mediante la cooperación internacional.

VI. Conclusiones

Se identificaron los principales retos a los que se enfrentan los esfuerzos mundiales en materia de ciberseguridad, centrándose en las barreras normativas, tecnológicas, operativas, culturales y sociales. Las principales conclusiones ponen de relieve una fragmentación significativa debida a políticas nacionales e internacionales incoherentes, disparidades tecnológicas y tensiones geopolíticas que impiden una cooperación y normalización eficaces. Los países avanzados se benefician de marcos sólidos, mientras que los países en desarrollo se enfrentan a vulnerabilidades sistémicas relacionadas con recursos limitados, infraestructuras deficientes y conocimientos técnicos insuficientes.

El análisis subraya el potencial de armonizar las normas mundiales y fomentar las asociaciones público-privadas para hacer frente a las amenazas. Sin embargo, la resistencia a las normativas internacionales y las actitudes culturales contradictorias hacia la privacidad y la seguridad siguen siendo obstáculos sustanciales para construir un marco de ciberseguridad cohesionado e integrador.

Los resultados revelan la existencia de diferencias entre los países en cuanto a armonización normativa, capacidad tecnológica y perspectivas culturales, lo que pone de relieve el impacto desigual de las divisiones geopolíticas y económicas. Aunque se ha avanzado en el fomento de la colaboración y el desarrollo de marcos, las disparidades existentes y la resistencia a las normas mundiales dificultan la adopción de soluciones integrales. Para alcanzar avances significativos en la regulación global de la ciberseguridad, es fundamental adoptar un enfoque integral y adaptable, que tenga en cuenta las particularidades y el constante desarrollo de las tecnologías emergentes.

Referencias

[1] S. Karakhodjayeva, «Navigating State Accountability in Cyberspace: Balancing Cyber-security, Artificial Intelligence, and Data Protection Conflict of Laws», *Uzbek Journal of Law and Digital Policy*, vol. 1, n.º 1, Art. n.º 1, feb. 2023, doi: 10.59022/ujldp.64.

[2] B. Madnick K. Huang y S. Madnick, «The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process», *Information Security Journal: A Global Perspective*, vol. 0, n.º 0, 2023, doi: 10.1080/19393555.2023.2201482.

[3] O. Michalec, B. Shreeve, y A. Rashid, «Who will keep the lights on? Expertise and inclusion in cyber security visions of future energy systems», *Energy Research and Social Science*, vol. 106, n.º 103327, dic. 2023, doi: 10.1016/j.erss.2023.103327.

[4] M. Carr y F. Lesniewska, «Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance», *International Relations*, vol. 34, n.º 3, pp. 391-412, sep. 2020, doi: 10.1177/0047117820948247.

[5] M. Finnemore y D. B. Hollis, «Constructing Norms for Global Cybersecurity», *American Journal of International Law*, vol. 110, n.º 3, pp. 425-479, jul. 2016, doi: 10.1017/S0002930000016894.

[6] C. Solar, «Cybersecurity and cyber defence in the emerging democracies», *Journal of Cyber Policy*, vol. 5, n.º 3, pp. 392-412, sep. 2020, doi: 10.1080/23738871.2020.1820546.

[7] T. O. Were, «Implementation of UN Cyber Norms in the Promotion of International Security: a Case Study of Kenya.», Thesis, University of Nairobi, 2021. Accedido: 29 de noviembre de 2024. [En línea]. Disponible en: http://erepository.uonbi.ac.ke/handle/11295/160302

[8] J. Osawa, «The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?», *Asia-Pacific Review*, vol. 24, n.º 2, pp. 113-131, jul. 2017, doi: 10.1080/13439006.2017.1406703.

[9] N. AllahRakha, «Cybersecurity Regulations for Protection and Safeguarding Digital Assets (Data) in Today's Worlds», *Lex Scientia Law Review*, vol. 8, n.º 1, Art. n.º 1, sep. 2024, doi: 10.15294/lslr.v8i1.2081.

[10] A. Adeyeri y H. Abroshan, «Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era», *Information*, vol. 15, n.º 11, Art. n.º 11, nov. 2024, doi: 10.3390/info15110682.

[11] H. Alshabib y J. Martins, «Cybersecurity: Perceived Threats and Policy Responses in the Gulf Cooperation Council», *IEEE Transactions on Engineering Management*, vol. 69, n.º 6, pp. 3664-3675, dic. 2022, doi: 10.1109/TEM.2021.3083330.

[12] A. Mishra, Y. I. Alzoubi, M. J. Anwar, y A. Q. Gill, «Attributes impacting cybersecurity policy development: An evidence from seven

nations», *Computers & Security*, vol. 120, p. 102820, sep. 2022, doi: 10.1016/j.cose.2022.102820.
[13] T. N. Heim, «Global governance and regulation of cybersecurity: Towards coherence or fragmentation?», PhD Thesis, University of Twente, Enschede, 2023. Accedido: 8 de enero de 2025. [En línea]. Disponible en: https://doi.org/10.3990/1.9789036556248
[14] M. Santaniello y M. Barbieri, «Monocratic cybersecurity in the EU member states: insights from Italy, France, Germany and Spain», *European Politics and Society*, vol. 0, n.º 0, pp. 1-25, 2024, doi: 10.1080/23745118.2024.2349893.
[15] S. Atkins y C. Lawson, «An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure», *Public Administration Review*, vol. 81, n.º 5, pp. 847-861, 2021, doi: 10.1111/puar.13322.
[16] A. B. Alfiyah, «Satellite Cybersecurity: Integration of International Law and Geopolitical Strategy», 5 de agosto de 2024, *Social Science Research Network, Rochester, NY*: 4918410. doi: 10.2139/ssrn.4918410.
[17] B. Saleem, M. Ahmed, M. Zahra, F. Hassan, M. A. Iqbal, y Z. Muhammad, «A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: a case study of Pakistan to bridge the gap», *Int. Cybersecur. Law Rev.*, vol. 5, n.º 4, pp. 533-561, dic. 2024, doi: 10.1365/s43439-024-00128-y.
[18] S. T. oglu Macidov, «Prosecuting Cybercrimes under International Legal Frameworks: Challenges and Innovations», *Futurity Economics&Law*, vol. 3, n.º 3, pp. 80-96, sep. 2023, doi: 10.57125/FEL.2023.09.25.05.
[19] S. Creese, W. H. Dutton, P. Esteve-González, y R. Shillair, «Cybersecurity capacity-building: cross-national benefits and international divides», *Journal of Cyber Policy*, vol. 6, n.º 2, pp. 214-235, may 2021, doi: 10.1080/23738871.2021.1979617.
[20] W. Tijerina, «Industrial policy and governments' cybersecurity capacity: a tale of two developments?», *Journal of Cyber Policy*, vol. 7, n.º 2, pp. 194-212, may 2022, doi: 10.1080/23738871.2022.2071747.
[21] N. F. Khan, N. Ikram, y S. Saleem, «Effects of socioeconomic and digital inequalities on cybersecurity in a developing country», *Secur J*, vol. 37, n.º 2, pp. 214-244, jun. 2024, doi: 10.1057/s41284-023-00375-4.
[22] D. Soldani, «5G and the Future of Security in ICT», en *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, nov. 2019, pp. 1-8. doi: 10.1109/ITNAC46935.2019.9078011.
[23] T. Zaid y S. Garai, «Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers», *Blockchain in Healthcare Today*, vol. 7, p. 10.30953/bhty.v7.302, abr. 2024, doi: 10.30953/bhty.v7.302.
[24] U. D. Ani, H. He, y A. Tiwari, «Human factor security: evaluating the cybersecurity capacity of the industrial workforce», *Journal of Systems and Information Technology*, vol. 21, n.º 1, pp. 2-35, mar. 2019, doi: 10.1108/JSIT-02-2018-0028.
[25] A. Peter, «Cyber Dependency and Weaponization: A Framework for Assessing Critical Infrastructure Risks and State Strategies», 30 de diciembre de 2024, *Social Science Research Network, Rochester, NY*: 5076760. doi: 10.2139/ssrn.5076760.
[26] M. Qobo, «US–China Tech Wars: Shaping Africa's Agency», en *The Political Economy of China—US Relations: Digital Futures and African Agency*, M. Qobo, Ed., Cham: Springer International Publishing, 2022, pp. 183-203. doi: 10.1007/978-3-030-86410-1_9.
[27] F. N. Ogwueleka, «Information Communication Technology, CyberSecurity and Small Arms in Africa», en *The Palgrave Handbook of Small Arms and Conflicts in Africa*, U. A. Tar y C. P. Onwurah, Eds., Cham: Springer International Publishing, 2021, pp. 647-677. doi: 10.1007/978-3-030-62183-4_31.
[28] S. K. Venkatachary, J. Prasad, A. Alagappan, L. J. B. Andrews, R. A. Raj, y S. Duraisamy, «Cybersecurity and cyber-terrorism challenges to energy-related infrastructures – Cybersecurity frameworks and economics – Comprehensive review», *International Journal of Critical Infrastructure Protection*, vol. 45, p. 100677, jul. 2024, doi: 10.1016/j.ijcip.2024.100677.
[29] M. Javaid, A. Haleem, R. P. Singh, y R. Suman, «Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends», *Cyber Security and Applications*, vol. 1, p. 100016, dic. 2023, doi: 10.1016/j.csa.2023.100016.
[30] S. Saeed *et al.*, «Digital Transformation in Energy Sector: Cybersecurity Challenges and Implications», *Information*, vol. 15, n.º 12, Art. n.º 12, dic. 2024, doi: 10.3390/info15120764.
[31] A. J. Cartwright, «The elephant in the room: cybersecurity in healthcare», *J Clin Monit Comput*, vol. 37, n.º 5, pp. 1123-1132, oct. 2023, doi: 10.1007/s10877-023-01013-5.
[32] C. Henderson, «Chapter 28: The United Nations and the regulation of cyber-security», 2021. Accedido: 8 de enero de 2025. [En línea]. Disponible en: https://doi.org/10.4337/9781789904253.00041
[33] J. Kulesza y R. H. Weber, «Protecting the Internet with international law», *Computer Law & Security Review*, vol. 40, p. 105531, abr. 2021, doi: 10.1016/j.clsr.2021.105531.
[34] X. Chen y Y. Yang, «Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance», *The International Spectator*, vol. 57, n.º 3, pp. 48-65, jul. 2022, doi: 10.1080/03932729.2022.2066841.
[35] Š. Grigaliūnas, M. Schmidt, R. Brūzgienė, P. Smyrli, y V. Bidikov, «Leveraging Taxonomical Engineering for Security Baseline Compliance in International Regulatory Frameworks», *Future Internet*, vol. 15, n.º 10, Art. n.º 10, oct. 2023, doi: 10.3390/fi15100330.
[36] I. Nwankwo *et al.*, «Data Protection and Cybersecurity Certification Activities and Schemes in the Energy Sector», *Electronics*, vol. 11, n.º 6, Art. n.º 6, ene. 2022, doi: 10.3390/electronics11060965.
[37] S. Pawar y Dr. H. Palivela, «LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)», *International Journal of Information Management Data Insights*, vol. 2, n.º 1, p. 100080, abr. 2022, doi: 10.1016/j.jjimei.2022.100080.
[38] R. Arshad y M. R. Asghar, «Characterisation and Quantification of User Privacy: Key Challenges, Regulations, and Future Directions», *IEEE Communications Surveys & Tutorials*, pp. 1-1, 2024, doi: 10.1109/COMST.2024.3519861.
[39] M. F. Safitra, M. Lubis, y H. Fakhrurroja, «Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity», *Sustainability*, vol. 15, n.º 18, Art. n.º 18, ene. 2023, doi: 10.3390/su151813369.
[40] V. Wylde *et al.*, «Cybersecurity, Data Privacy and Blockchain: A Review», *SN COMPUT. SCI.*, vol. 3, n.º 2, p. 127, ene. 2022, doi: 10.1007/s42979-022-01020-4.
[41] B. Hassib y J. Shires, «Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy», *Middle East Policy*, vol. 29, n.º 1, pp. 90-103, 2022, doi: 10.1111/mepo.12616.
[42] J. Racionero-Garcia y S. A. Shaikh, «Space and cybersecurity: Challenges and opportunities emerging from national strategy narratives», *Space Policy*, vol. 70, p. 101648, nov. 2024, doi: 10.1016/j.spacepol.2024.101648.
[43] D. P. F. Möller, «Cybersecurity in Digital Transformation», en *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*, D. P. F. Möller, Ed., Cham: Springer Nature Switzerland, 2023, pp. 1-70. doi: 10.1007/978-3-031-26845-8_1.
[44] U. A. Usmani, A. Happonen, y J. Watada, «Advancements in Industry 4.0 Asset Management: Interoperability and Cyber Security Challenges and Opportunities», en *Proceedings of the Future Technologies Conference (FTC) 2023, Volume 4*, K. Arai, Ed., Cham: Springer Nature Switzerland, 2023, pp. 468-488. doi: 10.1007/978-3-031-47448-4_35.
[45] H. Szczepaniuk y E. K. Szczepaniuk, «Cryptographic evidence-based cybersecurity for smart healthcare systems», *Information Sciences*, vol. 649, p. 119633, nov. 2023, doi: 10.1016/j.ins.2023.119633.
[46] B. Uchendu, J. R. C. Nurse, M. Bada, y S. Furnell, «Developing a cyber security culture: Current practices and future needs», *Computers & Security*, vol. 109, p. 102387, oct. 2021, doi: 10.1016/j.cose.2021.102387.
[47] S. AlDaajeh y S. Alrabaee, «Strategic cybersecurity», *Computers & Security*, vol. 141, p. 103845, jun. 2024, doi: 10.1016/j.cose.2024.103845.

[48] N. Alhalafi y P. Veeraraghavan, «Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model», *Smart Cities*, vol. 6, n.º 3, Art. n.º 3, jun. 2023, doi: 10.3390/smartcities6030072.

[49] B. Sadeghi *et al.*, «Modelling the ethical priorities influencing decision-making in cybersecurity contexts», *Organizational Cybersecurity Journal: Practice, Process and People*, vol. 3, n.º 2, pp. 127-149, may 2023, doi: 10.1108/OCJ-09-2022-0015.

[50] C. E. Dodge, N. Fisk, G. W. Burruss, R. K. Moule Jr., y C. M. Jaynes, «What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory», *Criminology & Public Policy*, vol. 22, n.º 4, pp. 849-868, 2023, doi: 10.1111/1745-9133.12641.

[51] S. Yusif y A. Hafeez-Baig, «Cybersecurity Policy Compliance in Higher Education: A Theoretical Framework», *Journal of Applied Security Research*, vol. 18, n.º 2, pp. 267-288, abr. 2023, doi: 10.1080/19361610.2021.1989271.

[52] W. W. Wang, «Contextualizing Personal Information: Privacy's Post-Neoliberal Constitutionalism and Its Heterogeneous Imperfections in China», *Computer Law & Security Review*, vol. 55, p. 106030, nov. 2024, doi: 10.1016/j.clsr.2024.106030.

[53] K. Balarabe, «Digital Borders and Beyond: Establishing Normative Grounds for Cybersecurity and Sovereignty in International Law», 25 de junio de 2024, *Social Science Research Network, Rochester, NY*: 4876617. doi: 10.2139/ssrn.4876617.

[54] S. Zuboff, «Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization», *Organization Theory*, vol. 3, n.º 3, p. 26317877221129290, jul. 2022, doi: 10.1177/26317877221129290.

[55] J. Bridenbaker, «The digital citizen as technoliberal subject: The politics of constitutive rhetoric in the European Union's Digital Decade», *Communication and Democracy*, vol. 58, n.º 2, pp. 159-182, jul. 2024, doi: 10.1080/27671127.2024.2385912.

[56] S. Creese, W. H. Dutton, y P. Esteve-González, «The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions», *Pers Ubiquit Comput*, vol. 25, n.º 5, pp. 941-955, oct. 2021, doi: 10.1007/s00779-021-01569-6.

[57] A. Kharlamov y G. Pogrebna, «Using human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity†», *Regulation & Governance*, vol. 15, n.º 3, pp. 709-724, 2021, doi: 10.1111/rego.12281.

[58] K. Renaud, K. van der Schyff, y S. MacDonald, «Would US citizens accept cybersecurity deresponsibilization? Perhaps not», *Computers & Security*, vol. 131, p. 103301, ago. 2023, doi: 10.1016/j.cose.2023.103301.

[59] N. Ameen, A. Tarhini, M. H. Shah, N. Madichie, J. Paul, y J. Choudrie, «Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce», *Computers in Human Behavior*, vol. 114, p. 106531, ene. 2021, doi: 10.1016/j.chb.2020.106531.

[60] M. Raymond y J. Sherman, «Authoritarian multilateralism in the global cyber regime complex: The double transformation of an international diplomatic practice», *Contemporary Security Policy*, vol. 45, n.º 1, pp. 110-140, ene. 2024, doi: 10.1080/13523260.2023.2269809.

[61] S. A. A. Bokhari, «A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan», *Social Sciences*, vol. 12, n.º 11, Art. n.º 11, nov. 2023, doi: 10.3390/socsci12110629.

[62] J. Song y M. J. Park, «A system dynamics approach for cost-benefit simulation in designing policies to enhance the cybersecurity resilience of small and medium-sized enterprises», *Information Development*, p. 02666669241252996, may 2024, doi: 10.1177/02666669241252996.

[63] V. Chandna y P. Tiwari, «Cybersecurity and the new firm: surviving online threats», *Journal of Business Strategy*, vol. 44, n.º 1, pp. 3-12, oct. 2021, doi: 10.1108/JBS-08-2021-0146.