PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS SOCIALES

La Participación del Perú en Instituciones Internacionales de Ciberdefensa y Ciberseguridad: Un Análisis en la Respuesta al Ciberataque de Guacamaya en 2022

Tesis para obtener el título profesional de Licenciada en Relaciones Internacionales presentada por:

Tito Bellota, Georgia Braha

Asesor(es):
Cardone, Ignacio Javier

Lima, 2025

Informe de Similitud

Yo, *Cardone , Ignacio Javier,* docente de la Facultad de Ciencias Sociales de la Pontificia Universidad Católica del Perú, asesor(a) de la tesis/el trabajo de investigación titulado *La Participación del Perú en Instituciones Internacionales de Ciberdefensa y Ciberseguridad: Un Análisis en la Respuesta al Ciberataque de Guacamaya en 2022* del/de la autor (a)/ de los(as) autores(as) *Tito Bellota, Georgia Braha* dejo constancia de lo siguiente:

- El mencionado documento tiene un índice de puntuación de similitud de 21%. Así lo consigna el reporte de similitud emitido por el software *Turnitin* el 06/06/25.
- He revisado con detalle dicho reporte y la Tesis o Trabajo de Suficiencia Profesional, y no se advierte indicios de plagio.
- Las citas a otros autores y sus respectivas referencias cumplen con las pautas académicas.

Lugar y fecha: Lima, 09 de Junio del 2025

Apellidos y nombres del asesor / de la asesora: *Cardone , Ignacio Javier*	
CE: 005503525	Firma
ORCID: 0000-0001-5743-9469	

Agradecimientos

Quiero expresar mi gratitud a todas las personas que, de una u otra manera, contribuyeron al desarrollo de esta tesis. Sus comentarios, sugerencias y apoyo fueron fundamentales para enriquecer este trabajo y superar los desafíos del proceso.

A mis padres, Vianey Bellota y Eddy Tito, por estar siempre conmigo y apoyarme a lo largo de mis estudios. Su paciencia y confianza en mí han sido esenciales en cada paso de este camino.

También agradezco a mis amigos y compañeros de la universidad, quienes con su apoyo y compañía hicieron este proceso más llevadero. En especial a Meloddy, Samantha y Alejandro por confiar en mi trabajo.

Finalmente, extiendo mi agradecimiento a mi asesor, cuya guía y retroalimentación han sido clave para la elaboración de esta investigación. Su orientación fue crucial para consolidar este proyecto.

Resumen

La presente tesis analiza el papel de la participación del Perú en instituciones internacionales de ciberseguridad y ciberdefensa en la respuesta al ciberataque del grupo hacktivista Guacamaya en 2022. La pregunta central que guía este estudio es: ¿contribuyó esta participación a la respuesta de Perú frente a dicha amenaza? Basándose en la hipótesis de que la adhesión a estas instituciones facilitó el acceso a mecanismos de cooperación, recursos, información y apoyo técnico, se analiza su papel en la respuesta del país para gestionar la crisis. Teóricamente, este estudio se fundamenta en una comprensión del concepto de seguridad adaptada al contexto contemporáneo del hacktivismo, un fenómeno que ha añadido complejidad a la defensa cibernética global. Desde el marco del institucionalismo liberal, se sostiene que las instituciones internacionales promueven la cooperación y el intercambio de información, esenciales para una respuesta mejor coordinada ante las amenazas cibernéticas. Asimismo, se analiza cómo el ciberespacio redefine las relaciones de poder y obliga a los Estados a colaborar más estrechamente para proteger sus infraestructuras críticas. Los hallazgos del análisis destacan que, aunque la participación de Perú en instituciones como la Organización de Estados Americanos (OEA) contribuyó a una defensa más sólida frente al ataque de Guacamaya, la respuesta fue en gran medida defensiva, dejando de lado posibles estrategias ofensivas. Además, se observa que Perú puede colaborar con entidades internacionales, como la OTAN, sin necesariamente ser miembro de estas, ampliando así sus opciones de cooperación. El estudio resalta que, si bien Perú ha avanzado en su seguridad digital mediante la cooperación internacional, es importante que el país continúe adaptándose a las cambiantes dinámicas del ciberespacio. Esto implica fortalecer tanto sus compromisos internacionales como el desarrollo de estrategias internas que equilibren defensas y respuestas ofensivas, para así enfrentar de manera más integral futuras amenazas cibernéticas.

Palabras clave: Ciberseguridad, Ciberdefensa, Instituciones Internacionales, Hacktivismo, Guacamaya

Abstract

This thesis analyzes the role of Peru's participation in international cybersecurity and cyberdefense institutions in its response to the 2022 cyberattack by the hacktivist group Guacamaya. The central question guiding this study is: Did this participation contribute to Peru's response to the threat? Based on the hypothesis that membership in these institutions facilitated access to cooperation mechanisms, resources, information, and technical support, the study examines their role in the country's response to managing the crisis. Theoretically, this study is grounded in a contemporary understanding of security, adapted to the context of hacktivism, a phenomenon that has added complexity to global cybersecurity defense. From the perspective of liberal institutionalism, it is argued that international institutions foster cooperation and information exchange, which are essential for a more coordinated response to cyber threats. Additionally, the study explores how cyberspace redefines power relations and compels states to collaborate more closely to protect their critical infrastructures. The findings highlight that, while Peru's participation in institutions such as the Organization of American States (OAS) contributed to a stronger defense against the Guacamaya attack, the response was largely defensive, neglecting potential offensive strategies. Moreover, it is noted that Peru can collaborate with international entities, such as NATO, without necessarily being a member, thus broadening its cooperation options. The study emphasizes that, although Peru has advanced its digital security through international cooperation, it is crucial for the country to continue adapting to the evolving dynamics of cyberspace. This entails strengthening both its international commitments and the development of internal strategies that balance defense and offensive responses, in order to more comprehensively address future cyber threats.

Key words: Cybersecurity, Cyber Defense, International Institutions, Hacktivism, Guacamaya.

Índice

Índice de Figuras

Índice de tablas

Introducción

En octubre de 2022, el Ejército Peruano y el Comando Conjunto de las Fuerzas Armadas sufrieron un ciberataque perpetrado por el grupo hacktivista internacional Guacamaya, que previamente había llevado a cabo su operación “Fuerzas Represivas” en países latinoamericanos como México, Chile y Brasil. Esta operación se centró en la divulgación de información de los organismos estatales encargados de la seguridad nacional de las naciones afectadas. La presente investigación se enfoca en el ciberataque a Perú, explorando la importancia de la participación del país en instituciones internacionales de ciberdefensa y ciberseguridad, y analizando el papel que dicha participación desempeñó en la respuesta al ciberataque del grupo Guacamaya en 2022. En este sentido, la pregunta que guía el trabajo es: ¿La participación de Perú en instituciones internacionales de ciberseguridad y ciberdefensa contribuyó a la respuesta del país al ciberataque del grupo Guacamaya en 2022?

Una de las principales características de esta investigación es que se enmarca dentro de los nuevos estudios de Seguridad en las Relaciones Internacionales, abordando lo que se considera como “las nuevas amenazas”. Este enfoque implica un desplazamiento del concepto tradicional de seguridad estatal, que se limitaba a la protección del territorio y las fronteras, hacia la consideración de nuevos espacios, como el ciberespacio, y la inclusión de actores emergentes, como los grupos hacktivistas. Asimismo, enfatiza la necesidad de desarrollar nuevas estrategias para abordar las amenazas que estos actores representan. En este contexto, se explica brevemente cómo ocurrió esta transición para así establecer la relación entre el ciberespacio, las nuevas amenazas y la participación en instituciones internacionales. Por último, se brinda una justificación del caso elegido y de su importancia.

Para comprender lo que implica la seguridad internacional en el contexto contemporáneo, es necesario considerar los cambios estructurales que ha experimentado el Sistema Internacional desde finales del siglo XX (Rossi, 2021, p.01). Esto se debe a que procesos como la globalización, el fin de la Guerra Fría y la Cuarta Revolución Industrial han reformulado las dinámicas entre los Estados, reconfigurado las prioridades políticas y económicas, e influido en la manera en que se concibe y gestiona la seguridad internacional. De esta manera, luego de la caída del muro de Berlín y la posterior disolución de la Unión Soviética, el año 1989 marcó un hito

importante en el paso hacia un nuevo orden mundial, caracterizado por la unipolaridad norteamericana. En este contexto, “Estados Unidos comenzó a gozar del monopolio que le confiere ser la única gran potencia convirtiéndose en el abanderado del capitalismo” (Zurita, 2007, p.01) a través de lo que el historiador Eric Hobsbawm denominó “la megalomanía estadounidense” (Hobsbawm, 1995, como se cita en Zurita, 2007, p.01).

El surgimiento de un nuevo orden unipolar significó una disminución de amenaza de conflictos entre las grandes potencias, lo que generó interrogantes acerca de la dirección que debía tomar la seguridad. En este escenario, “se comenzaron a ampliar y profundizar los estudios sobre seguridad, donde se abandonó el enfoque centrado en el posible conflicto entre el bloque occidental y comunista, y se empezó a considerar otras problemáticas relevantes” (Cardinale, 2016, p. 57). Según Orozco (2006, como se cita en Cardinale 2016, p. 54), este nuevo entendimiento de seguridad se clasifica en dos enfoques, entre las que se encuentran la tradicional o restringida, y la expansiva o amplia. La primera perspectiva destaca por su enfoque estado-céntrico, en el que el Estado desempeña el papel principal en el Sistema Internacional, y las amenazas a las que debe protegerse se caracterizan por ser objetivas, concretas y, en su mayoría, procedentes de otros Estados. Por otro lado, la segunda perspectiva pone énfasis en lo internacional y transnacional y ya no solo en el Estado. En este sentido, el foco de atención son las “nuevas amenazas”, definidas como “problemas globales” que engloban el terrorismo, la degradación medioambiental, la disputa por recursos naturales, la inmigración no regulada, la pobreza, entre otros (Iglesias, 2011, p.02). Así, la seguridad comienza a ser comprendida de manera multidimensional, por lo que los medios concretos para enfrentarla ya no solo son medios militares, sino que abarcan otros mecanismos tales como la diplomacia, el desarrollo y la cooperación.

Dicho de otra forma, “el sistema, en términos de seguridad, se comienza a convertir en un rompecabezas cada vez más difícil de descifrar y entender por la evolución, invención y complejización de amenazas y espacios” (Niño & Ortega, 2018, p. 285). El ciberespacio es uno de estos nuevos ámbitos, el cual, al carecer de fronteras claras y un espacio tangible, maneja una lógica distinta al espacio físico en donde se centraba tradicionalmente la seguridad estatal. En este sentido, es un terreno que permite a actores estatales y no estatales actuar por fuera de las consideraciones del espacio físico, lo que diluye las fronteras tradicionales y plantea

nuevos desafíos logrando la ubicuidad de los ataques. Esto se debe a que “es más barato y sencillo para actores no estatales y Estados pequeños, mover electrones por todo el mundo y atravesar las barreras del dominio cibernético que mover grandes barcos o armas físicas largas distancias y atravesar fronteras físicas” (Nye, 2012). De esta forma, como señala Ochoa (2021, p.19-47), los ataques cibernéticos, como el ciberterrorismo[1], el cybergroomed[2] y la ciberguerra[3], podrían originarse en diferentes ubicaciones y ser ejecutados por organizaciones de hackers, crackers o hacktivistas, cuyos operadores son desconocidos, e incluso tercerizados. En este contexto, se plantean nuevas formas de proteger el ciberespacio y surge la ciberseguridad y ciberdefensa como “medios para hacer frente a amenazas cibernéticas influyendo en la gobernanza nacional, la política nacional e internacional, la integridad de la economía y la protección de la información de sus ciudadanos” (Borbúa, Herrera, & Reyes, 2017, p.33-34). No obstante, debido a la complejidad que presenta el espacio cibernético, como las mayores posibilidades de anonimato y ubicuidad de los ataques, la cooperación internacional también aparece como un aspecto necesario para cualquier respuesta por parte de un Estado a las ciberamenazas, ya sea para la adquisición de equipos, sistemas y capacidades humanas o para el accionar conjunto en un espacio que trasciende las fronteras. De esta forma, organizaciones como la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) han buscado fortalecer la cooperación en áreas que trascienden la provisión de recursos y conocimientos, y han promovido el desarrollo de estándares y normas que fortalezcan una respuesta eficaz a estas nuevas amenazas.

Cabe señalar que, la cooperación no surge de manera automática; diversas barreras, como la falta de información entre los colaboradores, la desconfianza mutua y el aprovechamiento gratuito del esfuerzo ajeno, dificultan su ejecución o materialización. En este contexto, “las instituciones internacionales ofrecen un marco para facilitar esta cooperación al fomentar el diálogo, la coordinación y la colaboración entre los países promoviendo la confianza y garantizando la permanencia a largo plazo de la cooperación internacional” (Prado, 2017, p.375-378). Además, muchas de estas instituciones ofrecen a los Estados miembros beneficios como “el apoyo técnico en el desarrollo de normas y estándares nacionales, capacitaciones especializadas

[1] Uso de tecnologías para llevar a cabo actos terroristas (Ochoa, 2021, p.38).
[2] Actos de acoso a través de internet (Ochoa, 2021, p.38).
[3] Conflictos y hostilidades digitales entre Estados realizados en el ciberespacio (Ochoa, 2021, p.39).

en técnicas de ciberseguridad y ciberdefensa, así como también una coordinación de respuestas a incidentes cibernéticos a nivel internacional" (Patiño, 2019, p.175-176). De esta forma, al proporcionar un marco institucional para la cooperación entre países, las instituciones internacionales se tornan importantes en el estudio de la ciberdefensa y ciberseguridad para los Estados.

La presente investigación se centra en analizar la participación de Perú en estas instituciones internacionales de ciberseguridad y ciberdefensa, tomando como caso de estudio el ciberataque perpetrado por el grupo Guacamaya. Esta elección se fundamenta en que representa el primer ataque de un grupo hacktivista internacional en el Perú y plantea un dilema[4] al momento de definir su naturaleza, ya que enfrenta a la seguridad humana con la seguridad entendida en términos estatales. Además, involucra a un grupo que ha tenido un historial de actividades en la región latinoamericana, lo que ofrece una oportunidad para evaluar la cooperación y coordinación en ciberseguridad a nivel regional. En este caso, analizar cómo los Estados latinoamericanos pueden mejorar su respuesta a amenazas cibernéticas que trascienden las fronteras nacionales. Finalmente, la elección también se vio influenciada por ciertas particularidades que el país presenta, entre ellas su infraestructura digital, las respuestas gubernamentales previas frente a amenazas cibernéticas, la estructura de su red de ciberseguridad, y la legislación existente en materia de ciberdelitos.

En este sentido, el presente trabajo busca aportar a múltiples áreas de estudio. Primero, pretende profundizar en la comprensión del hacktivismo como un fenómeno complejo, analizando sus motivaciones, impacto y estrategias utilizadas, lo que contribuirá a ampliar el conocimiento existente sobre este campo poco explorado, sobre todo en el Perú. Segundo, busca llenar vacíos en la literatura existente y ofrecer una visión más detallada de un caso específico de hacktivismo, que ha recibido poca atención académica. Tercero, busca entender las respuestas de países de mediano tamaño, como el Perú, frente a los ataques cibernéticos mediante su participación en instituciones internacionales en materia de ciberseguridad y ciberdefensa. Al abordar estas áreas de estudio, se espera no solo enriquecer la comprensión académica del

[4] A modo de explicación, los hacktivistas utilizan medios ilegales como sentadas electrónicas, bloqueos virtuales, virus y robos de sistemas informáticos para acciones políticas o de protesta. No obstante, a diferencia de hackers o crackers, sus fines no son lucrativos, sino que a menudo abogan por derechos de minorías, de género o ambientalistas (Baldi, Gelbstein y Kurbalija, 2003).

fenómeno del hacktivismo y sus implicaciones, sino también ofrecer perspectivas útiles para la formulación de políticas y estrategias de ciberseguridad a nivel nacional. Asimismo, dado que el hacktivismo se presenta como una defensa de ciertos derechos y garantías de los individuos, se espera comprender la perspectiva del Estado hacia el hacktivismo. En otras palabras, conocer si lo considera como una forma de ciberactividad que busca proteger los derechos y garantías de minorías, o si lo engloba dentro de fenómenos más generales de amenazas cibernéticas.

Capítulo I: Diseño de Investigación

El presente capítulo establece las bases de esta investigación a partir de una revisión de la literatura existente, que permitirá evaluar el nivel de avance en las temáticas relacionadas con el caso de estudio y establecer un diálogo con las diferentes perspectivas. A partir de esta revisión, se ha elaborado un marco analítico que aborda los conceptos y teorías pertinentes, especialmente aquellos vinculados con la ciberseguridad, el hacktivismo y el papel de la cooperación, analizados desde la perspectiva del liberalismo institucionalista. Finalmente, se presenta el diseño metodológico, que abarca las fuentes y métodos de recolección y sistematización de información utilizados, con especial énfasis en las dimensiones identificadas como relevantes para esta investigación.

1.1. Estado del Arte y Revisión de Literatura

Dentro de las Relaciones Internacionales, el ciberespacio ha recibido un creciente interés. Esto se aprecia en el trabajo de Reardon y Choucri (2012), los cuales, mediante un relevamiento de 49 artículos académicos del periodo comprendido entre 2001 y 2010, clasificaron la intersección entre el mundo cibernético y las Relaciones Internacionales en cinco áreas temáticas: sociedad civil global, gobernanza, desarrollo económico, impacto en regímenes autoritarios y seguridad. Aunque se trata de un análisis realizado hace más de una década y con un número limitado de artículos, es relevante destacar que en ese momento ya se identificaban trabajos que abordaban estas cuestiones.

El estado del arte que se presenta a continuación se centra en la última área temática ofrecida por los autores: la relación entre seguridad y ciberespacio en las Relaciones Internacionales. De esta forma, se realizó una revisión sistemática de trabajos académicos[5] que abordan temas como grupos hacktivistas, ataques cibernéticos, ciberseguridad estatal e instituciones internacionales relacionadas con la protección y defensa en el ciberespacio.

[5] Dichos trabajos fueron encontrados en diversos libros y bases de datos como “Scopus”, “Elsevier”, “Researchgate”, “Academia”, “Jstor” y “Journal of Cybersecurity”. Cabe resaltar que dentro de las bases de datos, las palabras claves de búsqueda fueron: “ciberseguridad”, “ciberdefensa”, “hacktivismo”, “instituciones internacionales” y “ciberamenazas.

Con respecto al área securitaria y en función de los intereses del presente trabajo, la producción académica más reciente puede ser clasificada en tres grupos: el primero abarca estudios desarrollados sobre países fuera de la región, mayormente en el norte global, como Estados Unidos y España; el segundo se centra en investigaciones realizadas dentro de América Latina; y el tercer grupo aborda estudios en el contexto peruano. Finalmente, se presenta una breve conclusión sobre los hallazgos encontrados.

1.1.1. Estudios sobre casos fuera de la región Latinoamericana

La literatura sobre ciberseguridad fuera de América Latina se enfoca principalmente en países del norte global, especialmente en Estados Unidos y Europa. Algunos estudios destacan el papel del Estado como catalizador de la ciberseguridad, argumentando que su autoridad y recursos permiten una respuesta coordinada frente a las ciberamenazas (Trautman, 2015). Otros trabajos, sin embargo, también ponen énfasis en la participación de actores como las empresas privadas y organizaciones, destacando sus ventajas tecnológicas y las limitaciones de recursos en las estructuras estatales (Bendjek[6], 2012).

Por otro lado, se encontró trabajos que estudian el rol de algunos Estados, principalmente Rusia, China y Estados Unidos, como agentes de inseguridad cibernética. De esta forma, las ciberamenazas o ciberataques son usados en el ámbito militar como mecanismos de coerción (Valeriano, Jensen y Maness, 2018), así como para defensa y ataque (Martínez, 2015). Cabe resaltar que también pueden ser usados para fines comerciales o tecnológicos (Val y Akyesilmen, 2021) como el ciberespionaje económico (Magen[7], 2017). Adicionalmente a los Estados, instituciones estatales específicas suelen estar relacionadas a estos tipos de ciberataques. Tal es el caso de la NSA, la cual llevó a cabo un ciberespionaje a gran escala, que no solo se centró en seguridad y defensa, sino también en intereses comerciales para beneficiar a sus contratistas y consolidarlos en el mercado global en detrimento de empresas europeas y chinas (Fojón y Colom, 2014). Asimismo, fue

[6] Al estudiar las políticas de ciberseguridad de la UE, el autor descubre que estas se desarrollan en un entorno multinivel, lo que implica que el sector privado también ejerce influencia en su formulación.
[7] Las conclusiones de la autora subrayan que China actualmente lidera el ciberespionaje económico a nivel mundial.

acusada de una vigilancia masiva, recopilación de datos e inteligencia, el monitoreo de conversaciones extranjeras (Aid, 2014) y el uso del programa PRISM en sus operaciones en Pakistán (Abbasi, 2016).

Asimismo, se hallaron investigaciones que estudian y debaten la relación entre la difusión y el impacto de las filtraciones realizadas por grupos de hacktivistas en los Estados afectados. Por ejemplo, mientras una de ellas enfatiza la importancia de la prensa tradicional en papel como un factor clave para legitimar y amplificar el impacto de fenómenos digitales como WikiLeaks (Quian y Elias, 2018), existe otra tendencia que sostiene que el impacto de dichas filtraciones provienen principalmente de la información transmitida, independientemente de los medios utilizados para su difusión (Comas, 2010). A estos estudios se suman investigaciones que analizan el efecto de WikiLeaks en la imagen y el soft power de Estados Unidos, concluyendo que las filtraciones han generado consecuencias negativas para su influencia global, evidenciando una pérdida de control que contrasta con las promesas de transparencia y moralidad del gobierno de Obama (Parmar, 2014).

Finalmente, hay estudios que se centran en el modus operandi, la evolución y la identidad de grupos hacktivistas como Cult of the Dead Cow[8] (cDc) (Menn, 2019) y Anonymous (Coleman, 2013; Coleman, 2014; Dobusch y Schoeneborn, 2015). Además, se encuentran investigaciones que analizan la respuesta de instituciones internacionales europeas, especialmente de la OTAN, destacando la importancia de la cooperación internacional y la necesidad de cuantificar la efectividad de los esfuerzos mediante estadísticas (Choucri, Madnick y Koepke, 2017). También se subraya la necesidad de establecer una definición común del término, enfatizando la relevancia de medidas legales internacionales (Dogrul, Aslan y Celik, 2011; Burton, 2015).

1.1.2. Investigaciones sobre América Latina

Las investigaciones sobre América Latina son menos numerosas en comparación con la sección anterior, pero introducen un nuevo enfoque en la literatura al analizar ciertos ciberataques y su impacto en las relaciones entre los países

[8] Grupo que ha sido clave en el hacktivismo y en el contexto político-social, al desarrollar Tor, la herramienta de privacidad más crucial de la red.

latinoamericanos y Estados Unidos. Por ejemplo, algunos de estos estudios se centran en WikiLeaks y examinan cómo sus filtraciones han influido en la percepción de América Latina sobre Estados Unidos. Estos análisis revelan que, a pesar de las críticas públicas hacia las acciones de este país, muchos gobiernos de la región todavía buscan mantener relaciones diplomáticas favorables, lo que sugiere que los intereses estratégicos a menudo superan el discurso crítico (Sohr, 2011).

Otras investigaciones se centran en el modus operandi de grupos hacktivistas en la región, algunas basadas en las filtraciones de Edward Snowden para analizar cómo operó la NSA en América Latina, revelando el uso de empresas tecnológicas, alianzas con países como Canadá y Australia, satélites, conexiones de fibra óptica y ataques de malware (Bonifaz, 2017). Otros estudios exploran el papel de Anonymous (Bansi, 2015) o WikiLeaks (Oxfam, 2016) en la región.

Finalmente, también hay estudios que analizan cómo optimizar los limitados recursos económicos, humanos y financieros para reducir la vulnerabilidad ante amenazas cibernéticas en gobiernos latinoamericanos, como el de Ecuador (Mogollón, 2017), e identificar deficiencias en políticas nacionales de ciberseguridad, destacando la necesidad de una definición clara, el desarrollo de protocolos para crisis y la cooperación internacional en ciberseguridad (Aguilar, 2021).

1.1.3. Estudios de Ciberseguridad en el Perú

En el contexto peruano, las investigaciones sobre ciberseguridad y grupos hacktivistas son limitadas, pero no inexistentes. Estas se centran en mejorar la ciberseguridad del país, identificando desafíos como la falta de recursos humanos y logísticos especializados, equipos y software obsoletos, y la insuficiente colaboración entre entidades públicas y privadas para abordar adecuadamente las investigaciones. También hay una creciente preocupación en áreas como la protección de infraestructuras críticas, la formación de talento especializado y el desarrollo de políticas nacionales que fortalezcan la defensa ante ciberataques (García, 2019; Defensoría del Pueblo, 2022).

Además, Vilca y Gabi (2018) destacan el vacío legal en el Código Penal peruano en torno a las comunicaciones electrónicas comerciales y los hackers, subrayando su relevancia jurídica y los efectos negativos sobre el derecho a la intimidad. Quevedo (2023) señala que la inversión en seguridad y defensa cibernética

es insuficiente, y sugiere que una estrategia eficaz requiere la integración y cooperación entre los sectores público, privado y militar para garantizar la seguridad nacional.

En el ámbito de la política exterior, Rossi (2021) propone estrategias para mejorar las capacidades cibernéticas de Perú, vinculando la ciberseguridad con la defensa nacional e internacional. Complementando estos estudios, Ormachea (2019) plantea que es crucial enfrentar las amenazas desde una perspectiva preventiva y destaca la falta de integración entre los distintos sectores como un obstáculo para la defensa cibernética eficaz.

A lo largo de esta revisión, se ha constatado que la producción académica sobre ciberseguridad en América Latina, y particularmente en el contexto peruano, es limitada pero relevante. Los estudios han identificado diversos desafíos en la región, tales como la falta de un marco normativo robusto, la escasez de recursos humanos y técnicos especializados, y la insuficiente cooperación entre entidades públicas y privadas para hacer frente a las amenazas cibernéticas. Estos trabajos sugieren que el fortalecimiento de las capacidades de ciberdefensa en la región requiere una mayor integración entre los marcos normativos nacionales y las prácticas internacionales exitosas, así como un enfoque preventivo frente a las amenazas cibernéticas.

Sin embargo, la literatura actual muestra varias lagunas. En primer lugar, los estudios sobre hacktivismo, aunque abordados como fenómenos sociales y políticos, no han profundizado en la respuesta de los estados latinoamericanos, y particularmente del Perú, frente a estos actores. Además, se ha explorado relativamente poco cómo estos grupos y sus acciones pueden influir en las dinámicas diplomáticas, especialmente en contextos de creciente interdependencia digital. Otro vacío se encuentra en la falta de análisis sobre la efectividad de las políticas de ciberseguridad implementadas en la región, tanto en términos de prevención como de respuesta ante ciberataques.

En este sentido, esta investigación pretende aportar una perspectiva más amplia sobre la conexión entre hacktivismo, ciberseguridad y las relaciones internacionales en América Latina, con un énfasis en el caso peruano. A diferencia de estudios previos que se han enfocado en la creación de marcos normativos o en los vacíos institucionales, esta tesis busca no solo analizar el impacto de los ataques cibernéticos y el hacktivismo en la política de ciberseguridad del país, sino también evaluar cómo los gobiernos, en especial el peruano, han adaptado sus estrategias de

defensa ante este fenómeno. Así, se pretende contribuir a la discusión sobre cómo los Estados pueden responder de manera más eficaz a los retos que plantea el ciberespacio, integrando una perspectiva multidimensional que considere tanto las implicaciones de seguridad como las operativas.

1.2. Marco Analítico

Este estudio se basa en una evaluación del concepto de seguridad, un análisis del hacktivismo como fenómeno contemporáneo y complejo, las particularidades del ciberespacio en el ámbito internacional, y los fundamentos del institucionalismo liberal como teoría que respalda la cooperación en instituciones internacionales y las respuestas coordinadas ante amenazas cibernéticas.

Esta sección se estructura para integrar conceptos clave que son fundamentales para abordar la problemática de este estudio. En una primera subsección, se presenta una definición de seguridad, vinculada a las particularidades que adquiere en el ciberespacio. Estas particularidades resaltan la necesidad de cooperación entre diversos actores para enfrentar las nuevas amenazas cibernéticas. En una segunda subsección, se explora el papel de las instituciones internacionales como respuestas a estos desafíos, destacando cómo facilitan la cooperación en ciberseguridad y ciberdefensa.

1.2.1. La seguridad, el ciberespacio y la necesidad de cooperación

La seguridad es un concepto amplio y complejo que involucra una serie de dimensiones, prácticas y enfoques que varían según el contexto y las perspectivas que la abordan. En un principio, como parte de una perspectiva tradicional, se tuvo una mirada estado céntrica de la realidad internacional, en la cual “el Estado era el único actor a proteger de las amenazas que le presentaba otro Estado a través de medios militares” (Cardinale, 2016, p.52). Sin embargo, a medida que la Unión Soviética se disolvía, también se desvanecía la primacía que sostenía el enfrentamiento entre los dos principales bloques mundiales y los conflictos entre naciones como aspectos urgentes o predominantes dentro de las preocupaciones del Sistema Internacional. Además de que el surgimiento y la magnificación de otras amenazas a escala global alteraron significativamente la percepción de lo que

constituía seguridad, tanto en la práctica como en la investigación académica. Esta evolución llevó a la inclusión de nuevas problemáticas para abordar los crecientes desafíos, ampliando así el espectro de estudios existentes y complicando su análisis.

De esta manera, la seguridad tradicional, en la que la preocupación principal era el conflicto interestatal, deja de ser la única concepción y comienzan a emerger varias percepciones sobre seguridad, las cuales se caracterizan por ser concepciones pluralistas y eclécticas. Una de ellas es la “seguridad tradicional ampliada”, que presta atención a nuevas amenazas provenientes de actores no estatales o eventos naturales que afectan al Estado. La otra es la “seguridad humana”, en la que el Estado pasa a ser un medio y no el fin de la seguridad, siendo reemplazada por el individuo, los grupos sociales o las comunidades, superando el enfoque exclusivamente militar y estatal (Orozco, 2006, p.76-83). Sin embargo, a pesar de que ambas definiciones poseen enfoques y prioridades diferentes, coinciden en la necesidad de la existencia real o potencial de una amenaza o riesgo.

Lo anterior hace alusión a la noción de que la seguridad adquiere sentido en función de la presencia de amenazas. Porque, “los mecanismos de seguridad surgen precisamente como respuesta a posibles riesgos o peligros” (Boemcken y Schetter, 2016, p.02-04). Por ello, cuando se habla de seguridad, se deben de identificar los fines, las amenazas y los medios. En otras palabras, las preguntas clave son: “¿quién debe ser protegido?, ¿de qué o de quiénes debe estar seguro?, y ¿a través de qué medios o formas debe ser protegido?” (Kahhat, 2019).

No obstante, teniendo en cuenta que el Estado no es el único actor que puede ser vulnerado o el único que puede perpetrar amenazas, la categorización de atacante y damnificado se complejiza. Los grupos hacktivistas se enmarcan en este dilema porque, por un lado, podrían ser considerados como parte de las "nuevas amenazas" que vulneran a los Estados a través del hacking; pero, por el otro, podrían ser vistos como movimientos en defensa de la seguridad humana, utilizando el hacking para “defender derechos humanos, retar a gobiernos totalitarios y luchar contra la injusticia social” (Andrei, 2016, p. 01).

Esto se debe a que los grupos hacktivistas actúan de manera distinta a otros grupos que roban o filtran información. Por ejemplo, a diferencia de los hackers, cuyas acciones suelen centrarse en la defensa de sus propios intereses y la libertad de la información, “los hacktivistas comparten principios alineados con la Declaración Universal de Derechos Humanos y la Convención Internacional sobre Derechos

Civiles y Políticos" (García-Estévez, 2018, p.150). De igual manera, "a diferencia de los crackers, quienes buscan obtener beneficios económicos mediante el robo de información, los hacktivistas no persiguen ganancias financieras porque sus acciones están motivadas por causas sociales y políticas" (Vicente, 2004, p.87-88).

Por ende, "el hacktivismo, llevado a cabo por colectivos de individuos que promueven determinadas causas utilizando como medio de acción el ciberespacio" (Wray, 1998, como se cita en García-Estévez, 2018, p.148), se presenta como un fenómeno complejo en el ámbito de la seguridad. Porque "desafía la estabilidad estatal al operar fuera de los límites legales y, en ocasiones, en contra de las instituciones gubernamentales; y, al mismo tiempo, busca impulsar causas sociales y medioambientales" (García-Estévez, 2018, p.148-151), lo que podría interpretarse como un intento por fortalecer la seguridad humana, al exponer violaciones a la privacidad y a los derechos fundamentales. Ante esta dualidad, surge la interrogante de si el hacktivismo representa una amenaza genuina para el Estado o simplemente actúa como un vehículo para defender derechos que el Estado está socavando, planteando así la cuestión de quién asume realmente el papel de atacante.

La presente investigación reconoce la complejidad de la dimensión de seguridad en cuanto al fenómeno del hacktivismo. Sin embargo, dado que el trabajo se centra en entender el papel de la participación en instituciones internacionales y la respuesta del Estado peruano ante un ciberataque, el hacktivismo será considerado como una amenaza a la seguridad. Porque, a pesar de que los fines del hacktivismo no sean económicos y puedan abogar en beneficio de una población vulnerada, los medios que utilizan para alcanzar dichos objetivos son ilegales, y la posibilidad de desencadenar eventos impredecibles, como el mal uso de la información filtrada, puede tener un impacto negativo en el poder, estabilidad estatal e incluso en los propios individuos o grupos que pretendían defender. De esta forma, estos actos pueden ocasionar daños involuntarios a personas, comunidades e instituciones, o pueden desencadenar dinámicas que desembocan en situaciones de crisis o incluso confrontaciones violentas.

Asimismo, debido a las estrategias y tácticas utilizadas en el hacktivismo, estos grupos podrían ser instrumentalizados para favorecer los intereses de entidades criminales o de otros estados que busquen perjudicar a un gobierno o nación. En este sentido, independientemente de las motivaciones de estos grupos, desde una perspectiva analítica, constituyen un motivo genuino de preocupación en términos de

seguridad internacional. Sumada a dicha complejidad, encontramos la dificultad que plantea el hacktivismo en el espacio en el cual actúa: el ciberespacio. El hacktivismo, a diferencia de amenazas tradicionales, como las militares, donde era más fácil identificar al atacante, se desarrolla en un nuevo espacio de disputa. Este nuevo terreno, conocido como ciberespacio y definido como "una nueva arena de competencia entre los Estados y el quinto dominio de la guerra, luego de los dominios de la tierra, del mar, del aire y del espacio exterior" (Rossi, 2021, p.34), difiere de los dominios tradicionales al carecer de fronteras geográficas claramente definidas (Barbachan, 2009). Porque, mientras que “las fronteras convencionales delimitan el territorio físico, en un espacio terrestre, marítimo y aéreo, donde un Estado ejerce su autoridad” (Agnew, 1994, p.53-54), en el ciberespacio estas fronteras no son tan evidentes. Esto desafía las concepciones tradicionales de seguridad y soberanía, ya que la ausencia de límites territoriales plantea desafíos para la seguridad y supervivencia de un Estado en este ámbito virtual.

De esta forma, la seguridad estatal deja de ser entendida en términos netamente territoriales y fronterizos para expandirse hacia una noción más amplia y dinámica, que contempla la protección de infraestructuras críticas, la gestión de riesgos emergentes, y la adaptación a un entorno globalizado y digitalizado, donde los límites físicos son menos definitorios (Vallés, 2007). Cabe resaltar que “el ciberespacio no sustituye al espacio geográfico tradicional, sino que redimensiona las dimensiones espacio-temporales tradicionales” (Barbachán, 2009). Es decir, el ciberespacio amplía la comprensión de la seguridad, generando la necesidad de estrategias más flexibles y adaptativas que aborden tanto los riesgos tradicionales como las nuevas amenazas provenientes de la esfera digital.

En este contexto, surge la necesidad estatal de proteger no solo las fronteras físicas, sino también de salvaguardar el espacio digital. En consecuencia, “la ciberseguridad y la ciberdefensa se consolidan como las disciplinas encargadas de proteger sistemas críticos e información sensible contra ataques digitales o ciberataques” (Rossi, 2021, p.30–40). Ataques que se caracterizan por su extrema complejidad, falta de claridad y visibilidad, lo que dificulta la comprensión de las capacidades y motivaciones del adversario. Por ejemplo, en un ciberataque, es más fácil malinterpretar las acciones o asignarlas incorrectamente a otro actor, ya que “el ciberespacio permite la suplantación de identidad, el anonimato y el uso de infraestructuras de terceros” (Cubeiro, 2023, p.62). Asimismo, surge la dificultad de

rastrear y localizar a los atacantes, ya que los ataques cibernéticos pueden ser ejecutados desde fuera del territorio nacional e, incluso, desde diversas localizaciones. Como ejemplo, podemos nombrar el ciberataque que se llevó a cabo en el 2007 en Estonia por parte de atacantes ubicados en Rusia, en el que sitios web gubernamentales, medios de comunicación y empresas se vieron afectados, desencadenando, de manera indirecta, una serie de protestas y disturbios en el país (McGuinness, 2017).

En este sentido, la estrategia nacional relacionada a proteger el espacio cibernético debe de reconocer la naturaleza transfronteriza que debe de tener la ciberseguridad y ciberdefensa, ya que los ataques cibernéticos pueden venir desde fuera del territorio receptor e incluso con atacantes tercerizados. La naturaleza transnacional de las amenazas en el ciberespacio hace indispensable que las políticas de ciberseguridad y ciberdefensa contemplen la colaboración tanto a nivel nacional como internacional. “Esta cooperación permite generar confianza entre los actores involucrados, establecer canales de diálogo efectivos, construir soluciones compartidas ante desafíos comunes y fomentar una cultura global enfocada en la protección del entorno digital” (Unión Internacional de Telecomunicaciones [UIT], Banco Mundial, Secretaría de la Commonwealth [Comsec], Organización de Telecomunicaciones de la Commonwealth [CTO], & Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN [CCDCOE OTAN], 2018, pp. 48-49). Para ello, es fundamental contar con un marco institucional y normativo sólido, con el fin de facilitar procesos como la cooperación jurídica internacional, la investigación de delitos informáticos, la recolección de pruebas digitales y la extradición de personas implicadas (Unión Internacional de Telecomunicaciones [UIT] et al., 2018).

1.2.2. Instituciones internacionales, cooperación y respuesta a los ataques cibernéticos

No existe una única definición de cooperación debido a que el contexto, la cultura y la época desempeñan un papel importante en la manera en que se percibe y se practica. Sin embargo, muchas concepciones coinciden en que “cooperar implica renunciar voluntariamente a ciertas libertades a cambio de un beneficio mutuo o conjunto en diversos ámbitos, como el de la seguridad” (Guiora, 2018, citado en Gómez, 2022, p. 129). En este sentido, la cooperación internacional se torna en una

colaboración conjunta y coordinada, donde los actores globales, como los Estados, buscan satisfacer sus demandas mutuas para abordar desafíos compartidos, resolver conflictos y lograr objetivos mutuos (Calduch, 1991). No obstante, “la cooperación no debe entenderse como una ausencia de conflicto ni de armonía, sino más bien como una reacción frente a tales escenarios o a la posibilidad de que los mismos se presenten” (Prado, 2017, p.370). Dicho de otra manera, la cooperación es un mecanismo para gestionar conflictos o amenazas, y buscar soluciones compartidas que beneficien a las partes involucradas.

Sin embargo, existen diversas barreras que dificultan la cooperación, como la falta de información entre los actores sobre sus verdaderas intenciones, la desconfianza mutua, el riesgo de traición, la tendencia al free riding —es decir, beneficiarse del esfuerzo ajeno sin contribuir—, y la renuencia a asumir los costos de transacción. Estas limitaciones obstaculizan su implementación, lo que hace necesario el desarrollo de mecanismos que permitan superarlas (Prado, 2017, p. 370). De esa manera, las instituciones adquieren un rol importante porque son ellas quienes “promueven, mejoran y aumentan la permanencia en el tiempo de la cooperación internacional” (Prado, 2017, p.372). Es decir, quienes actúan como facilitadoras al establecer normas, procedimientos y mecanismos de seguimiento que promuevan la confianza, la transparencia y la rendición de cuentas entre los actores involucrados, contribuyendo así a la consolidación y sostenibilidad de la cooperación internacional.

Las instituciones vienen a ser “el conjunto de reglas formales e informales, persistentes e interconectadas que prescriben roles de comportamiento, constriñen actividades y moldean expectativas” (Keohane, 1984, p.59), por lo que se convierten en instrumentos normativos que influyen en el comportamiento de los Estados para lograr beneficios comunes y compartidos. En este sentido, “la cooperación es entendida como un juego de suma positiva donde todos los que cooperan ganan y las instituciones se convierten en los instrumentos que ayudan a promoverla” (Ripoll, 2007, p.71) para “poder satisfacer necesidades comunes con menores costos, esfuerzos y plazos de tiempo” (Prado, 2017, p.373). Estas instituciones, como describe y conceptualiza Lallande (2021), se dividen en:

- Organizaciones intergubernamentales: Creadas por gobiernos nacionales, conformadas por organismos internacionales que operan de acuerdo con normas específicas, como tratados internacionales y reglas internas que rigen su estructura y actividades. Entre estas destacan la Organización de Naciones

Unidas (ONU), la Organización del Tratado del Atlántico Norte (OTAN), la Organización de Estados Americanos (OEA), entre otros.

- Regímenes internacionales: Sistemas de reglas institucionalizadas que involucran a diversos actores y se crean para abordar temas específicos, como el medio ambiente y el comercio. Aunque sus normas no siempre son obligatorias, influyen en el comportamiento de los participantes y desempeñan un papel importante en la regulación de las relaciones internacionales.
- Convenciones: Instituciones internacionales menos formales, las cuales se basan en la costumbre y consisten en reglas y procedimientos implícitos en temas específicos. Estas permiten a los actores coordinar su comportamiento y a menudo se basan en la reciprocidad, donde una parte espera que la otra responda de manera similar en las negociaciones internacionales.

Las instituciones desempeñan un papel fundamental en esta investigación ya que “proporcionan un marco necesario para facilitar y promover la cooperación internacional, ofreciendo una respuesta adaptativa y colaborativa entre naciones” (Guiora, 2018, citado en Gómez López, 2022, p. 129). De manera que proporcionan mecanismos institucionales para prevenir o minimizar el daño que trae consigo un ciberataque o su amenaza, los cuales, se caracterizan por ser de “naturaleza transnacional” (Valencia, 2015, p.140). Es decir, que van más allá de las fronteras nacionales.

De esta forma, “el intercambio de información, coordinación y operación conjunta entre países adquiere importancia para la rápida detección del atacante y para el fortalecimiento tecnológico y legal de una nación” (Croasdell & Palustre, 2019, p. 5601). Estas dinámicas, fundamentales para enfrentar amenazas transnacionales, suelen estar mediadas por instituciones internacionales, las cuales actúan como facilitadoras de la cooperación entre Estados. Y, “aunque este proceso no siempre es perfecto, sin dichas instituciones alcanzar objetivos comunes sería mucho más difícil” (Keohane, 1988). Esto responde a que los Estados se enfrentan a dos problemas al intentar cooperar:

- La preocupación de que el otro haga trampa, como se explica en el dilema del prisionero.
- La dificultad de coordinar sus acciones sobre un resultado cooperativo estable particular.

En este sentido, las instituciones internacionales proporcionan "centros focales construidos" ofreciendo información, reduciendo los costos de transacción, construyendo compromisos más creíbles, estableciendo puntos focales para la coordinación y, en general, facilitando el funcionamiento de la reciprocidad (Keohane y Martin, 1995). Es decir, proporcionan la creación de un entorno más eficiente y confiable para la colaboración entre países, asegurando que los esfuerzos conjuntos sean más efectivos y sostenibles en la lucha contra amenazas transnacionales.

En el ámbito de la ciberseguridad, “la cooperación institucionalizada puede evitar o minimizar el daño que representa la amenaza de un ciberataque” (Guiora, 2018, citado en Gómez López, 2022, p. 129). De esta forma, se pueden establecer protocolos comunes, compartir información crítica en tiempo real, coordinar respuestas rápidas y efectivas entre los diferentes países, aprovechar recursos y capacidades tecnológicas de manera conjunta, entre otros.

Sin embargo, esta cooperación no ocurre de manera automática. Requiere de “un acto soberano y voluntario por parte de los Estados para integrarse a las instituciones internacionales que la promueven” (Prado, 2017, p. 373). Este proceso de participación, implica comprometerse con las reglas y mecanismos que dichas instituciones establecen. Al comprometerse con estas reglas, los países asumen obligaciones, pero también acceden a una serie de beneficios, entre ellos, el desarrollo de competencias. A través de su participación, los Estados tienen la oportunidad de fortalecer sus capacidades nacionales en ciberseguridad, aprender de las mejores prácticas de otros miembros y participar en programas de capacitación que mejoren su preparación ante los desafíos cibernéticos. Este proceso de aprendizaje mutuo puede llegar a fomentar la creación de estándares comunes que facilitan la colaboración efectiva en la resolución de incidentes y la prevención de amenazas.

Esta sección ha mostrado cómo el fenómeno de la seguridad, en el contexto actual, se redefine frente a la aparición de nuevas amenazas en el ciberespacio. Este entorno, caracterizado por su naturaleza transnacional y su capacidad para desafiar los límites físicos, exige un enfoque integral que trascienda las fronteras nacionales. Las políticas de seguridad deben adaptarse para enfrentar las complejidades emergentes en este ámbito, reconociendo que la cooperación internacional es importante para reducir riesgos y responder de manera coordinada a incidentes cibernéticos. Sin embargo, esta cooperación no se da de manera automática; requiere

la participación de los Estados a través de su adhesión a instituciones internacionales que promuevan la seguridad cibernética global.

La participación de los países en estas instituciones representa un acto soberano y voluntario que implica comprometerse con las normas y mecanismos de operación que estas plataformas establecen. En este sentido, la participación se convierte en un vehículo para acceder a los beneficios que ofrecen estas instituciones, como el desarrollo de competencias, el fortalecimiento de la seguridad cibernética y la formulación de estrategias conjuntas frente a las amenazas globales.

1.3. Metodología y operacionalización de variables

La hipótesis que sigue este trabajo es que la participación de Perú en instituciones internacionales de ciberseguridad y ciberdefensa contribuyó a la respuesta al ciberataque del grupo Guacamaya en 2022, al proporcionar mecanismos de cooperación que facilitaron el acceso a recursos, información y apoyo técnico, mejorando así la reacción del país para gestionar la amenaza cibernética. En este sentido, la hipótesis sostiene que la participación en estos organismos contribuye a estructurar una respuesta más organizada y efectiva frente a amenazas cibernéticas transnacionales. Este enfoque permite evaluar el alcance y los límites de la participación del Perú en estas instituciones al momento de enfrentar desafíos complejos como el hackeo perpetrado por el grupo Guacamaya.

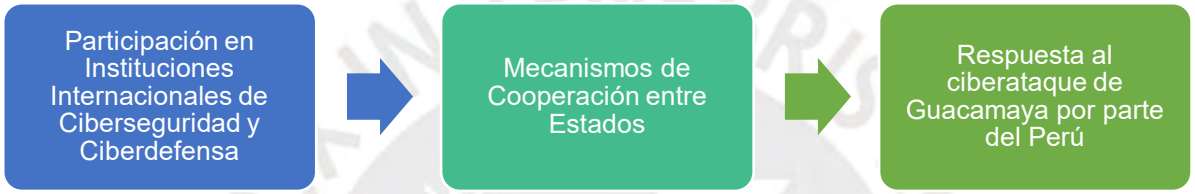
Es necesario resaltar que, este trabajo no tiene la intención de afirmar que la participación en instituciones ha sido el único factor que condicionó la respuesta del Perú, pero se espera que, por las condiciones propias de la ciberseguridad, esta participación haya sido importante para dar respuesta a la amenaza. En ese sentido, se ha buscado entender la relación que existe entre la participación en instituciones internacionales, la cooperación internacional y las posibilidades de respuesta ante una nueva amenaza securitaria en el caso peruano.

Se incluyen así tres variables concatenadas: una variable independiente, la participación en instituciones internacionales; una variable intermediaria, que son los mecanismos de cooperación entre Estados; y una variable dependiente, que es la

respuesta del Estado peruano. La variable intermediaria[9] ha sido colocada en función de ser entendida como "el mecanismo o proceso a través del cual la variable independiente influye en la variable dependiente, actuando como mediador en la relación causal entre ambas variables" (Baron y Kenny, 1983, p. 1174). En este sentido, permite entender y complejizar la relación entre la participación en instituciones internacionales y la respuesta del Estado peruano, como se muestra a continuación:

Figura 1

Relación entre la Participación en Instituciones Internacionales y la Respuesta al ciberataque de Guacamaya



Fuente: Elaboración propia

El cuadro muestra cómo la participación de Perú en instituciones internacionales de ciberseguridad y ciberdefensa permitió el acceso a mecanismos de cooperación entre Estados, lo que contribuyó a la respuesta frente al ciberataque de Guacamaya. De esta forma, se establece una relación en la que la participación en dichas instituciones facilita la cooperación, y esta última fortalece las condiciones del país para gestionar amenazas cibernéticas.

Para los propósitos de este estudio, se han adoptado las siguientes definiciones conceptuales para cada una de las variables:

1. Participación del Perú en instituciones internacionales de ciberseguridad y ciberdefensa: Se considera el compromiso formal del Perú de adherirse a normativas y esfuerzos conjuntos a nivel internacional, orientados a promover, regular y fortalecer la seguridad cibernética a nivel global.
2. Mecanismos de cooperación internacional: Se refiere a los marcos de cooperación establecidos con otros Estados, específicamente orientados a la

[9] La variable intermediaria actúa como catalizador, mientras que la interviniente puede moderar, intensificar o desviar el efecto, por lo que se ha optado por utilizar la intermediaria en este análisis, dado su papel como puente necesario entre la variable independiente y la dependiente.

ciberseguridad y ciberdefensa. En este sentido, se analizará si dichos marcos de cooperación han sido resultado de la participación del Perú en los marcos institucionales internacionales en los que está involucrado.

3. Respuesta del Estado peruano frente al ataque de Guacamaya: Se define como el conjunto de acciones que tomó el Perú en reacción al ciberataque de Guacamaya, incluyendo tanto las acciones de prevención como las de contención del ataque, persecución de los responsables y el fortalecimiento de las capacidades e infraestructuras de seguridad informática.

En este sentido, se presenta el siguiente cuadro con las variables y sus respectivos indicadores:

Tabla 1
Variables e Indicadores

Variable	Indicadores
Participación del Perú en instituciones internacionales en materia de ciberseguridad y ciberdefensa	a. Adhesión a instituciones internacionales que promuevan la ciberseguridad y ciberdefensa: Indica la unión formal del Perú a instituciones internacionales que se especializan en fortalecer la seguridad cibernética y la defensa contra amenazas digitales
Mecanismos de cooperación	a. Consultas realizadas por el Perú para el desarrollo o actualización de normativas: Indica las solicitudes de asistencia técnica internacional para el desarrollo de nuevas normativas o la actualización de las existentes. b. Programas de capacitación y ejercicios conjuntos en los que el Perú ha participado: Indica los programas de capacitación y ejercicios conjuntos en los cuales el Perú ha participado. Estos programas incluyen actividades diseñadas para fortalecer las capacidades técnicas y operativas del país en respuesta a amenazas cibernéticas. c. Fondos recibidos por el Perú a través de iniciativas internacionales de ciberseguridad: Indica los recursos financieros provenientes de colaboraciones internacionales destinados a fortalecer la seguridad cibernética del país para implementar proyectos, mejorar infraestructuras y capacitar personal en la prevención y respuesta ante amenazas digitales.
Respuesta del Estado peruano frente al ataque de Guacamaya	a. Tiempo promedio de detección del ataque: Indica el lapso promedio transcurrido desde el inicio del ataque cibernético hasta su detección por parte de las autoridades o sistemas de seguridad pertinentes. b. Equipos de respuesta ante incidentes activados: Indica los equipos[10] desplegados para gestionar y responder a incidentes de ciberseguridad. c. Mejoras implementadas en sistemas de monitoreo y alerta: Indica las acciones tomadas post-ataque para mitigar las consecuencias negativas y evitar que un evento similar vuelva a pasar.

Fuente: Elaboración propia

Respecto a la metodología, este trabajo se caracteriza por su enfoque cualitativo, fundamentado en tres aspectos. En primer lugar, los datos que se utiliza son heterogéneos y no pueden ser agregados a una única medida, ya que presentan diversas aproximaciones y unidades. En segundo lugar, aunque la teoría juega un papel importante, el énfasis está en explicar el caso específico de la participación del Perú en instituciones internacionales de ciberseguridad y ciberdefensa, y su relación con la respuesta del Estado peruano al ciberataque del grupo hacktivista Guacamaya

[10] Equipos entendidos como conjuntos organizados y coordinados de individuos que colaboran entre sí para alcanzar metas comunes

a través de la cooperación. De esta manera, el objetivo es determinar si esta participación ha dado lugar a mecanismos de cooperación que permitan responder al ataque.

Por último, este estudio se considera un caso ideográfico que requiere una aproximación desde múltiples dimensiones y perspectivas, lo cual es facilitado por una metodología cualitativa. En línea con estos objetivos, no se busca la agregación de datos para vincular las variables de manera estadística, sino comprender el proceso a la luz de su progresión histórica, utilizando información heterogénea de diversas fuentes, tanto entrevistas como un relevamiento documental.

Para el relevamiento documental, se utilizó los portales en línea de los principales órganos del Estado peruano relacionados con la ciberseguridad y ciberdefensa. En particular, se priorizó las plataformas del Congreso, el Consejo de Ministros, el Ministerio del Interior y el Ministerio de Relaciones Exteriores. A través de estas fuentes, se logró listar los acuerdos, resoluciones y convenios que Perú ha suscrito en materia de ciberseguridad y ciberdefensa. Asimismo, se recopiló información sobre la participación del país en foros, conferencias y eventos relevantes en esta área. También se revisaron registros relacionados con capacitaciones, intercambios tecnológicos y detalles sobre el ciberataque perpetrado por el grupo hacktivista Guacamaya. Este proceso permitió obtener un panorama integral de las acciones y compromisos del Perú en el ámbito de la ciberseguridad y la ciberdefensa.

Además, se accedió a la página oficial del Comando Conjunto de las Fuerzas Armadas a través del portal del Ministerio del Interior. Este recurso resultó relevante para el estudio, ya que se utilizó para identificar la participación de las Fuerzas Armadas peruanas en conferencias y simulacros relacionados con la ciberdefensa nacional. De la misma manera, se empleó la plataforma oficial del programa de ciberseguridad de la OEA, la cual ofrece informes, publicaciones y noticias sobre los esfuerzos regionales en seguridad cibernética. A través de esta plataforma, se recopiló información detallada sobre las iniciativas en las que Perú ha estado involucrado en materia de ciberseguridad a nivel regional. Este proceso contribuyó a construir un panorama más completo sobre las acciones del Perú en el ámbito de la ciberdefensa.

Finalmente, se recurrió a fuentes de prensa oficiales como medios de información en lo relacionado con la respuesta del Estado peruano al ataque, ya que proporcionaron cobertura detallada sobre los eventos posteriores al hackeo y las

acciones emprendidas por las autoridades. En particular, se utilizaron diarios de gran relevancia como “El Peruano”, “La República” y “RPP” para recopilar información y, además, para identificar a las personas que podrían ser entrevistadas en el marco de esta investigación.

Luego de realizar un relevamiento documental exhaustivo de fuentes primarias y secundarias, se identificaron personas clave para ser entrevistadas. Estas entrevistas fueron de tipo semiestructurado, con una guía de preguntas elaborada en función del perfil de cada entrevistado. Debido a que la mayor parte de la información sobre la variable independiente e intermedia se obtuvo de fuentes digitales, las entrevistas se centraron en personal de las Fuerzas Armadas, con el objetivo de profundizar en la respuesta del Estado peruano ante el ciberataque. Las entrevistas fueron grabadas, previa autorización de los participantes, para su posterior análisis. A continuación, se presenta una lista de los entrevistados:

- David Guillermo Ojeda Parra: Comandante General del Ejército del Perú desde el 20 de diciembre del 2022.
- Octavio Martín Freitas Farfán: Oficial del Ejército del Perú, jefe del Departamento de Planeación.

Capítulo II: Seguridad Cibernética en Instituciones Internacionales, en el Perú y la presencia del grupo Guacamaya en la región latinoamericana

Debido a que este trabajo contempla la temática sobre seguridad y defensa en el ciberespacio, tanto en el ámbito internacional y nacional, el presente capítulo se encarga de brindar un panorama general del desarrollo de acciones, normativas y proyectos que se han llevado a cabo en instituciones internacionales y dentro del Perú para hacer frente a las crecientes amenazas y desafíos en el ciberespacio, destacando los esfuerzos tanto a nivel global y local para salvaguardar la seguridad digital. Además, se profundiza en las características y el impacto del grupo Guacamaya, delineando quiénes son y su presencia en la región y en el Perú.

2.1. La Seguridad cibernética en Instituciones Internacionales

Las instituciones internacionales, como se indicó en el marco teórico, se convierten en una herramienta para promover, mejorar y aumentar la cooperación internacional entre actores internacionales respecto a diferentes temáticas. La ciberseguridad y ciberdefensa son una de ellas puesto que son áreas cada vez más relevantes dada “la creciente interconexión e interdependencia que se ha dado en el Sistema Internacional desde la Cuarta Revolución Industrial” (Rossi, 2021, p.01). En este sentido, se ha promovido la protección del ciberespacio en tratados, convenios, acuerdos bilaterales o multilaterales, entre otros.

El inicio de los ciberdelitos encuentra sus inicios en la década de los 40, cuando se empezaron a desarrollar los primeros ordenadores informáticos y redes informáticas. En sus inicios, “estas actividades eran realizadas principalmente por entusiastas de la informática y surgían por curiosidad o entretenimiento más que por beneficios geopolíticos y comerciales, por lo que eran consideradas un riesgo de bajo nivel” (Ruiz y Borrero, 2023, p.75). Además, considerando que en esa época los ordenadores eran de gran tamaño, como el ENIAC (Electronic Numerical Integrator And Computer), que llegaba a pesar 27 toneladas, el acceso a la información que contenían era difícil y limitado, ya que “se requería ingresar físicamente al lugar donde estaban ubicados” (Nebreda, 2013, p.22). Por lo tanto, se comprende que, hasta ese momento, los ciberdelitos se enfocaban principalmente en acciones a nivel local y de menor magnitud.

Sin embargo, con el paso del tiempo, especialmente desde principios de la década de los 60, la aparición de los ordenadores de segunda, tercera y cuarta generación, seguida de la creación de Internet y el avance tecnológico, hizo que los ciberdelitos se volvieran cada vez más peligrosos y comenzaran a tener un impacto significativo en la vida de las personas.

Uno de estos fue el “Creeper”, el primer malware creado en 1971, que se replicaba a través de la red ARPANET y dejaba el mensaje “Soy el Creeper, atrápame si puedes” en los ordenadores infectados. Este evento marcó el inicio de la ciberseguridad con la invención del programa “Reaper” (el primer gusano informático), diseñado para perseguir y eliminar al Creeper (Ruiz y Cortés Borrero, 2023, p.75-79). El segundo malware más importante apareció en 1986, ya que fue el primer virus informático con fines delictivos económicos. Se llamaba “Brain” y se instalaba en los ordenadores enseñando un mensaje solicitando un pago para eliminarlo (Prieto y Pan, 2014, p.06).

La situación se modificó substancialmente a partir de la década de 1990, con la extensión de redes de informáticas y la posterior conectividad global por medio de Internet. Porque, “a partir de esta evolución en la irrupción de las redes de información en la vida cotidiana, comienzan a surgir nuevas maneras de ciberdelitos como el spamming, el phishing, ataques de ransomware y el malware” (Ruiz & Cortés Borrero, 2023, p.76).

De este modo, debido al incremento y modernización de los ciberdelitos, en 1990 la OTAN unificó las definiciones de seguridad de transmisión (TRANSEC), seguridad de redes (NETSEC) y seguridad de ordenadores (COMPUSEC) en un único concepto, llamado “seguridad de la información" (INFOSEC), para así comenzar a proteger la información en sus tres dimensiones: confidencialidad, integridad y disponibilidad (Candau, 2021, p.462). En este sentido, se buscó establecer un marco integral para que los aspectos de la información digital estuvieran protegidos contra accesos no autorizados, alteraciones y destrucción.

Luego, en 1997, el Consejo de Europa toma la iniciativa de elaborar una convención internacional para abordar estos delitos cibernéticos mediante la cooperación internacional. Esta convención internacional, adoptada el 2001 por el Consejo de Europa, es lo que se pasó a llamar la Convención de Budapest sobre el Cibercrimen, y fue “el primer tratado internacional que buscó hacer frente a los delitos informáticos y los delitos en Internet” (Rossi, 2021, p.48) a través de “la unificación de

las normas de derecho penal sustantivo, la estandarización de los procedimientos penales y la cooperación internacional" (Guerrero y Borgioli, 2018, p.04). La convención presenta tres objetivos principales, los cuales se centran en:

- La armonización del derecho penal nacional en materia de delitos informáticos
- La facilitación de facultades necesarias en el derecho procesal penal interno para la investigación y enjuiciamiento de los ciberdelitos
- El establecimiento de un régimen rápido y efectivo de cooperación internacional en la materia.

Así, se analiza la forma en que debe ejecutarse la extradición de la persona o grupo responsable del ciberataque, los principios básicos de ayuda recíproca, el intercambio de información, y otros aspectos relacionados. Por ejemplo, en el artículo 35 del Título 3 se establece una "red 24/7" para la implementación de un "punto de contacto" con permanente disponibilidad, esto con el objetivo de "estar facultados para responder a las comunicaciones de otros puntos de contacto de manera inmediata, facilitar asesoramiento técnico, preservar datos, recolectar evidencia, proveer información legal y ubicar sospechosos" (Consejo de Europa, 2001, como se citó en Rossi, 2021, p. 50).

Hasta la fecha, se han agregado dos protocolos adicionales a la convención. La primera entró en vigor el 2006 e incluyó "la incriminación de los actos de carácter racista cometidos a través de sistemas informáticos" (Consejo de Europa, 2003). La segunda fue más reciente, ya que entró en vigor el 2021, y se centró en la necesidad de endurecer las normas, sobre todo las que respectan a "la divulgación de registro de nombres, medidas de cooperación con proveedores de servicios para obtener información de usuarios, cooperación inmediata en casos de emergencia, herramientas de asistencia mutua y salvaguardias para la preservación de los derechos humanos en lo digital" (Consejo de Europa, 2022, p.11).

Por otro lado, en el ámbito americano, se establece, en el 2002, La Declaración de Bridgetown, la cual fue aprobada durante el trigésimo segundo período ordinario de sesiones de la Asamblea General de la OEA, destacando la necesidad de adoptar un enfoque multidimensional para abordar los desafíos de seguridad en el hemisferio. Esto debido a que se comienza a reconocer que "las amenazas contemporáneas van más allá de los conflictos militares tradicionales, incluyendo aspectos políticos, económicos, sociales, de salud y ambientales" (Organización de los Estados Americanos [OEA], 2002). De esta manera, se subraya que muchas de estas

amenazas son transnacionales y requieren una cooperación hemisférica efectiva, lo que destaca la importancia de una respuesta integral y coordinada. Asimismo, subraya el compromiso previo de fortalecer la confianza y la seguridad entre los Estados miembros, así como las decisiones tomadas en cumbres y reuniones anteriores sobre la necesidad de revitalizar las instituciones del Sistema interamericano relacionadas con la seguridad hemisférica. Esta Declaración, aunque no aborda específicamente la seguridad en el ciberespacio, es relevante para los Estados de la región porque introduce por primera vez la necesidad de replantear cómo se entiende la seguridad en el hemisferio. Como resultado, se acuerda incluir el enfoque multidimensional como un punto clave en la agenda de la "Conferencia Especial sobre Seguridad", con el fin de proponer recomendaciones y estrategias coordinadas, así como planes de acción integrados, para enfrentar los desafíos hemisféricos.

La Declaración de Bridgetown da pie a que, los días 27 y 28 de octubre del 2003, se lleve a cabo la "Conferencia Especial sobre Ciberseguridad", la cual juntó a diversos países del hemisferio a reflexionar y plantear nuevas estrategias para mejorar la seguridad de la región. En este sentido, surge la Declaración sobre Seguridad en las Américas, en la que se señala "el inicio de una nueva fase en la región, caracterizada por la introducción de un nuevo paradigma multidimensional de seguridad en el hemisferio" (Secretaría de Relaciones Exteriores México, s.f.). Como se menciona dentro de la Declaración (OEA, 2003), se comienzan a incluir diversos aspectos como:

- Considerar a las nuevas amenazas desafíos para la seguridad nacional de los Estados del hemisferio
- Buscar una consolidación de la paz, el desarrollo integral, la justicia social y los valores democráticos
- Promocionar la cooperación entre Estados y la defensa de los Derechos Humanos

De este modo, se comienza a considerar como "nuevas amenazas" al terrorismo, la pobreza extrema, los desastres naturales, la trata de personas, el peligro en el transporte marino y los ataques a la seguridad cibernética. A partir de entonces, esta declaración se convirtió en el marco normativo de base por el cual se comenzó a guiar la OEA en materia de ciberseguridad, lo que "permitió a los países miembros consolidar un entorno colaborativo enfocado en compartir información, mejorar la protección tecnológica y aumentar su capacidad de respuesta ante incidentes

cibernéticos" (Organización de los Estados Americanos & Banco Interamericano de Desarrollo, 2016, como se citó en Bacchi, 2023, p. 47). En este sentido, en el año 2006, se establece a la Junta Interamericana de Defensa (JID) como entidad de la OEA, con la función de prestar a la organización y sus Estados Miembros servicios de asesoramiento técnico, consultivo y de educación sobre temas relacionados con asuntos militares y de defensa en el Hemisferio (Junta Interamericana de Defensa [JID], s.f.).

De esta forma, el Programa de Ciberdefensa de la JID surge en el marco de la creciente necesidad de protección cibernética en el hemisferio occidental, particularmente dentro de la estructura de la OEA. Iniciado formalmente a principios de la década de 2010, nace como una herramienta para proporcionar servicios de asesoramiento técnico y consultivo sobre temas militares y de defensa en el hemisferio. Las áreas clave de este programa incluyen el fortalecimiento de las capacidades nacionales en ciberdefensa, el fomento de la cooperación y el intercambio de información entre países, el impulso de intereses multilaterales, la creación de alianzas estratégicas y el intercambio de conocimientos. Además, apoya la implementación de un marco regional de cooperación en ciberdefensa en las Américas, promoviendo la mejora continua de las estrategias de seguridad cibernética y la resiliencia frente a amenazas globales. (JID, 2020, p. 05-07).

Asimismo, el Foro de Iberoamericano de Defensa Cibernética se establece como otra entidad para la promoción de la cooperación en materia de seguridad digital, el cual no solo facilita el intercambio de conocimientos y mejores prácticas entre los países iberoamericanos, sino que también "fomenta la creación de estrategias conjuntas para hacer frente a las crecientes amenazas cibernéticas" (JID, 2020, p.88).

En Europa, en el 2004, se crea la ENISA (Agencia Europea para la Ciberseguridad) con el objetivo de apoyar la política de seguridad cibernética de la Unión Europea a través de programas de certificación de ciberseguridad y cooperación con los Estados miembros y organismos de la UE para fomentar la confianza en la economía digital, fortalecer la resiliencia de las infraestructuras y garantizar la seguridad de los ciudadanos beneficiando tanto a entidades públicas como al sector privado (Agencia de la Unión Europea para la Ciberseguridad [ENISA], s.f.). Hasta ese entonces, los esfuerzos, principalmente en Europa, se centraron en la protección de redes y sistemas de información como un asunto técnico, más que una prioridad de seguridad nacional e internacional. No obstante, no fue hasta el 2007,

con el ciberataque contra Estonia[11], que esta percepción cambió. Este, considerado como el mayor ataque de DDoS[12] (Denegación de Servicio Distribuida) registrado hasta la fecha, porque tuvo más de un millón de computadoras afectadas dentro del área de la economía, el comercio y las comunicaciones de Estonia a nivel nacional (Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile [CEEAG], 2017, p.52-54).

El ciberataque a Estonia se llevó a cabo en dos fases. La primera, en abril del 2007, se caracterizó por ser llevada a cabo por hacktivistas rusos [13]mediante herramientas de hacking simples y rudimentarias diseñadas para atacar el gobierno, el ministerio de Defensa y los principales partidos políticos de Estonia. De esta manera, la respuesta se limitó a ser nacional, y fue liderada y coordinada por el Equipo Nacional de Respuesta ante Incidentes Informáticos (Estonian CERT), junto con personal experto de los ministerios de Comercio, Comunicaciones, Defensa e Inteligencia (Ganuza, 2011, p.179). No obstante, los ataques cibernéticos no pararon, sino que se complejizaron y sofisticaron, entrando a la segunda fase del ataque. En este sentido, se registraron múltiples ataques durante el mes de mayo de 2007, destacando un aumento significativo[14] en la actividad de ataque en los días posteriores a la reubicación del monumento soviético, lo que reflejó la respuesta de hacktivistas rusos a la situación política en Estonia (Ganuza, 2011, 174-175).

Esta situación puso de manifiesto que la respuesta a los ataques requería un mayor conocimiento sobre ciberdefensa y una mejor coordinación internacional, ya que el ataque se venía realizando desde distintos IPs, por lo que, en mayo del mismo año, Estonia solicita ayuda a la OTAN para anular los botnets[15]. Por consiguiente, con la ayuda de sus aliados, obtuvo apoyo técnico por parte de los observadores de los CERTS, difundió la noticia de que se había consolidado una cooperación internacional para localizar a los ciber criminales, y logró que el número de atacantes y ataques disminuyera (Ganuza, 2011, p.190). Asimismo, se consiguió rastrear que la mayor

[11] Ocurrido en el 2007, fue un ciberataque masivo que afectó servicios críticos, como los gubernamentales y financieros revelando la vulnerabilidad de los Estados ante amenazas cibernéticas y fomentando un cambio en la perspectiva europea sobre la ciberseguridad.
[12] Este ciberataque sobrecarga un servidor o red con tráfico excesivo desde múltiples computadoras, impidiendo que los usuarios legítimos accedan a los servicios.
[13] Los ciberataques fueron impulsados por el descontento de la comunidad rusa en Estonia ante la reubicación de un monumento soviético, lo que llevó a los hacktivistas rusos a atacar las infraestructuras gubernamentales como forma de protesta (Stratcom Centre of Excellence, 2007).
[14] Específicamente, 21 ataques durante el 3 de mayo, 17 durante el 4 de mayo, 31 el 08 de mayo, 58 el 09 de mayo y 01 el 11 de mayo.
[15] Redes de computadoras infectadas con malware que pueden ser controladas remotamente

parte de los ataques y los botnets provenían de Rusia, y algunos de “paraísos legales cibernéticos”, como Egipto, Perú o Vietnam (Ganuza, 2011, p.192).

A raíz de este ataque y casos similares en 2008 en Lituania, Kirguistán y Georgia, se percibió que la OTAN no disponía de un plan de acción en caso de ciberataque. Más aún, ni siquiera disponía de una conceptualización de Ciberdefensa y, como consecuencia, tampoco de una política definida sobre la cuestión (Caro, 2011, p.01-05). Respondiendo a esta necesidad, el 7 de enero de 2008, se firma la Política de Ciber Defensa con “miras a mejorar la capacidad de la OTAN para proteger los sistemas de información y comunicaciones (CIS) de importancia crítica” (Castillo, 2021, p.02). Asimismo, el 28 de octubre de 2008, se establece el Centro de Excelencia de la OTAN de Ciberdefensa Cooperativa especializado en tres ramas: i) asuntos operativos, funcionales y militares; ii) asuntos tecnológicos, académicos y científicos; y iii) asuntos legales. De esta manera, se plantea el objetivo de “dar respuestas y soluciones globales a problemas de seguridad cibernética mediante equipos multidisciplinares” (Ganuza, 2011, p.206).

Durante la década de los 2010, los avances e iniciativas que se habían realizado en materia de ciberseguridad y ciberdefensa se comienzan a consolidar y expandir. En 2010, Naciones Unidas comenzó a promover un enfoque integral de ciberseguridad, reconociendo las ciberamenazas como un riesgo significativo para todos los sectores, por lo que se encargó al Comité de Alto Nivel sobre Gestión y al Comité de Alto Nivel sobre Programas, bajo la supervisión de la UIT y la UNODC, abordar esta cuestión. Esta iniciativa culminó en 2013, con la aprobación de un marco de ciberseguridad y ciberdelincuencia para todo el sistema de la ONU y, en 2014, con un plan de coordinación interna. Aunque estos documentos no se convirtieron en referencias permanentes, establecieron principios fundamentales que siguen guiando los esfuerzos de ciberseguridad dentro del sistema de la ONU (Naciones Unidas, 2021).

Asimismo, en el 2012, la OEA publica la "Declaración Fortalecimiento de la Seguridad Cibernética en las Américas", documento en el que los Estados miembros se comprometieron a implementar la Estrategia Interamericana de Seguridad Cibernética de 2004, así como a continuar estableciendo o fortaleciendo Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT). Además, se acordó participar en la Red de Seguridad Hemisférica de los CSIRT y aumentar el intercambio de información para proteger las infraestructuras críticas y prevenir incidentes de

ciberseguridad. La Declaración enfatiza la importancia de la participación de los CSIRT en la seguridad hemisférica, impulsando el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) para el Fortalecimiento de las Capacidades de Respuesta ante Incidentes Cibernéticos de los CSIRTs. Este programa incluye “evaluaciones de los Estados en materia de ciberseguridad y el desarrollo de estrategias nacionales de ciberseguridad, con el apoyo de mesas redondas de expertos” (Bacchi, 2023, p.49).

En el 2013 se publica el Informe del GGE de la ONU, en el que además de brindar recomendaciones sobre la creación de capacidades para la efectividad de la cooperación mundial en la seguridad de las tecnologías de la información y las comunicaciones (TIC), se reconoce la aplicación del derecho internacional en el ciberespacio, lo que dio las bases para normativas y discusiones futuras (Naciones Unidas, 2013).

Para esos años, la seguridad cibernética ya se había instalado como tema en la agenda de seguridad, llevando, en 2016, a Argentina, Brasil, Chile, Colombia, España, México, Perú y Portugal, a un acuerdo para fomentar la colaboración entre los países iberoamericanos en el ámbito de la ciberseguridad. Su principal objetivo era avanzar en la colaboración en áreas como formación, ejercicios, intercambio de información, investigación, desarrollo e innovación en ciberdefensa. En este sentido, se comenzaron a enfocar en la formación y la realización de ciber ejercicios, como pilares estratégicos en la lucha contra los ciberataques (Lima Costa, 2024). Adicionalmente, se realizaron reuniones ordinarias destinadas a evaluar el avance de las actividades, identificar nuevas oportunidades y compartir los avances en el ámbito cibernético de cada país, centrándose en áreas específicas como la formación de recursos humanos, la elaboración de contenidos curriculares, el intercambio académico, la realización de ciberejercicios, el intercambio de información sobre ciberamenazas y la cooperación en investigación y desarrollo en el campo de la ciberdefensa (Ciberilatam, 2024, p.19-20).

Para el 2017, mediante la Resolución 71/291 de la Asamblea General de Naciones Unidas y en respuesta a la creciente inquietud sobre el uso inapropiado de la tecnología de la información y las comunicaciones (TIC) por parte de los terroristas, particularmente en Internet y las nuevas tecnologías digitales, la organización establece la Oficina de Lucha Contra el Terrorismo (OLCT), la cual comenzará a abordar cuestiones relacionadas con la ciberseguridad y las amenazas híbridas. Para

hacer frente a tal desafío, la oficina desarrolló un Programa de Ciberseguridad y Nuevas Tecnologías, con el objetivo de fortalecer las capacidades de los Estados Miembros y entidades privadas en la prevención y minimización de ciberataques, vinculado en mayor medida a agentes terroristas, además de la restauración de los sistemas afectados en caso de producirse algún ataque (Oficina de Lucha Contra el Terrorismo [OLCT], s.f.).

Finalmente, desde mayo del 2021, se ha venido desarrollando y negociando la creación de algún tratado sobre seguridad cibernética en el seno de la ONU. Una vez aprobado, este sería el primer instrumento vinculante de las Naciones Unidas en la materia y se constituiría como un importante marco jurídico de alcance global para la cooperación internacional en materia de prevención, investigación del cibercrimen y procesamiento penal de los ciberdelincuentes. Sin embargo, hasta la fecha no se ha logrado alcanzar un acuerdo debido a las dudas y reticencias de diversos actores, incluyendo gobiernos y organizaciones civiles, respecto a la extensión del tratado. Las preocupaciones se centran en aspectos como las garantías de derechos humanos, el abordaje de las disparidades en las capacidades de los Estados y la armonización con otros instrumentos legales. Muchos actores temen que un acuerdo podría facilitar la vigilancia estatal de los ciudadanos, comprometiendo así sus libertades fundamentales (Wilkinson, 2023, p.02-03).

En conclusión, la evolución de la ciberseguridad y la ciberdefensa en las instituciones internacionales ha sido un proceso dinámico y multifacético, influenciado por el aumento constante de las amenazas cibernéticas, que se han vuelto más sofisticadas a medida que la tecnología se integra en todos los aspectos de la vida social, económica, política y de defensa. Aunque se han logrado hitos significativos, como la adopción de marcos de cooperación y estándares internacionales, el desafío sigue siendo considerable. La necesidad de una respuesta coordinada ante estas crecientes amenazas es evidente.

Las iniciativas, como la creación de la ENISA, el establecimiento del Centro de Excelencia de Defensa Cibernética Cooperativa de la OTAN en 2008, las resoluciones de la Asamblea General de la ONU, entre otros, reflejan un esfuerzo para fortalecer la seguridad en el ciberespacio a nivel mundial. Es necesario resaltar que estos esfuerzos no solo han proporcionado una base para la cooperación internacional, sino que también han fomentado el desarrollo de habilidades nacionales y regionales con el objetivo de crear un entorno cibernético seguro.

2.2. La Seguridad Digital en el Perú

El Perú no ha sido ajeno al desarrollo de políticas o acciones para el cuidado y la protección del ciberespacio. No obstante, este término es relativamente nuevo, por lo que el presente apartado aborda el desarrollo de las políticas y normativas a nivel nacional que se han llevado a cabo para fomentar un ciberespacio seguro.

En este sentido, el Perú trabaja la ciberseguridad y ciberdefensa bajo el concepto de Seguridad Digital, definido como "la confianza en el entorno digital resultado de la gestión y aplicación de una serie de medidas proactivas y reactivas para hacer a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno" (El peruano, 2018, p.01).

A pesar de que el Perú no cuenta con capacidades cibernéticas cercanas a la de algunos países europeos o de potencias como Estados Unidos o China, el país no se encuentra rezagado en el tema. Según el Índice de Ciberseguridad (UIT, 2020, pp. 26, 28, 67), el Perú se ubica en el puesto 85 de 182 a nivel mundial, y en el puesto 12 de 35 a nivel regional en materia de seguridad cibernética, con una puntuación de 55,67, siendo las "medidas cooperativas" el segundo indicador más alto de su evaluación, obteniendo un puntaje de 13.15 de 20.00.

Como se observó, la preocupación y atención del país a la seguridad en el ciberespacio se puede encontrar a inicios de los 90, en el proceso de modernización del Estado, con la emisión de diversas normativas sobre la regulación del uso de las computadoras y demás dispositivos electrónicos (Guerrero, 2018, p.05). Una de ellas es el Decreto Legislativo "Uso de Tecnologías Avanzadas en Materia de Archivo" (Número 681) publicada en 1991, la cual establece "directrices para el uso de tecnologías avanzadas en el almacenamiento de documentos e información, abarcando tanto los documentos generados de forma convencional como aquellos producidos mediante procedimientos informáticos en computadoras" (Ministerio de Justicia y Derechos Humanos, 1991, p.01).

La normativa centrada en crímenes cibernéticos recién comienza a ser desarrollada, en mayor medida, en los años 2000, cuando se promulgó la Ley N° 27309, la cual incorporó al Código Penal peruano dos nuevos delitos relacionados con la informática: el intrusismo informático y el cracking, estipulando que "los culpables serán sancionados con pena privativa de libertad no menor de tres ni mayor de cinco

años" (Diario El Peruano, 2000). De este modo, se comenzó a reconocer y a penalizar formalmente las actividades ilícitas en el ámbito digital, marcando un primer paso hacia la regulación y protección del ciberespacio a nivel nacional. Posteriormente, en el 2011, se publica una Ley de Protección de Datos Personales (Ley N.° 29733), la cual tiene como objetivo establecer un "marco de protección para regular la disposición y el uso de bases de datos, tanto públicas como privadas, por parte de terceros" (Congreso de la República, 2011). Esta ley, a diferencia de la anterior, buscó garantizar la privacidad y la integridad de los datos personales, estableciendo derechos y obligaciones tanto para los ciudadanos como para las entidades públicas o privadas que gestionan dicha información.

En esta misma línea, durante el 2013, se publicó la Ley de Delitos Informáticos (Ley No. 30096) para "prevenir y sancionar la ciberdelincuencia, las conductas ilícitas que afectan los sistemas y datos informáticos, y otros bienes jurídicos de relevancia penal" (Congreso de la República, 2013). Esta ley resultó de gran importancia, al establecer un marco jurídico más claro para abordar diversos tipos de delitos informáticos. En 2017, las iniciativas de ciberseguridad dieron un paso más con la creación de la Secretaría de Gobierno Digital (SeGDi) y la formulación de la Política Nacional de Ciberseguridad. Estas acciones complementaron y organizaron las leyes ya existentes, coordinando esfuerzos a nivel gubernamental y definiendo estrategias concretas para mejorar la seguridad digital en el país (Presidencia del Consejo de Ministros, 2023).

El desarrollo posterior de este marco incluyó la elaboración del Plan Estratégico Sectorial Multianual (PESEM) 2017-2021, el cual se valió de los avances propuestos por el proyecto fallido de Directiva de la Dirección de Política y Planeamiento Estratégico para la Defensa del Ministerio de Defensa, que delineaba las Políticas del Sector Defensa en Ciberdefensa. Aunque este proyecto no fue aprobado mediante Resolución Ministerial, sirvió de base para cumplir el objetivo estratégico de "garantizar la defensa nacional a través de la protección de la infraestructura crítica del Estado frente a ciberataques" (Castillo, 2021, p.03).

Un año más tarde fue publicada la Ley de Gobierno Digital[16], Decreto Legislativo N° 1412 del 2018, la cual generó un marco de gobernanza con el fin de

[16] Gobierno Digital entendido como el uso estratégico de tecnologías digitales y datos en la Administración Pública. Basado en un ecosistema de actores del sector público, ciudadanos y otros

“gestionar adecuadamente la identidad digital, los servicios digitales, la arquitectura digital, la interoperabilidad, la seguridad digital y los datos” (Poder Ejecutivo, 2018). En este sentido, puso como ente rector a la Presidencia del Consejo de Ministros, la cual se convirtió en la encargada de “supervisar y fiscalizar el cumplimiento del marco normativo, promover la colaboración entre entidades públicas, validar técnicamente proyectos de tecnologías digitales, emitir normas reglamentarias y complementarias, y coordinar esfuerzos para mejorar la prestación de servicios digitales y asegurar la identidad digital” (Poder Ejecutivo, 2018). Asimismo, dentro de su capítulo 4 se aborda todo lo relacionado a la Seguridad Digital, estableciendo un marco integral para la protección y gestión de la seguridad en el entorno digital, definiendo 4 ámbitos de gestión:

- Defensa: Conducido por el Ministerio de Defensa (MINDEF), el cual es el encargado de dirigir, supervisar y evaluar las normas en materia de ciberdefensa.
- Inteligencia: Conducido por la Dirección Nacional de Inteligencia (DINI), la cual emite, supervisa y evalúa las normas en materia de inteligencia y contrainteligencia.
- Justicia: Conducido por el Ministerio de Justicia y Derechos Humanos (MINJUS), el Ministerio del Interior (MININTER), la Policía Nacional del Perú (PNP), el Ministerio Público y el Poder Judicial (PJ), encargado de dirigir, supervisar y evaluar las normas en materia de ciberdelincuencia.
- Institucional: Ámbito donde todas las entidades de la Administración Pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI) fomentando de esta manera la ciberseguridad.

Estos 4 ámbitos son importantes para la Seguridad Digital porque, como mencionó en una de las entrevistas el Comandante Manrique, no operan de manera aislada, sino que interactúan entre sí y de manera continua. Por ende, cada ámbito debe de estar informado sobre las prácticas y medidas que se están llevando a cabo en los demás espacios para poder proteger eficazmente a las instituciones que dependen de ellas.

interesados, que apoyan en la implementación de servicios digitales y contenidos, asegurando el respeto de los derechos de todos en el entorno digital (Poder Ejecutivo, 2018)

A raíz de este capítulo se promulgan diversos decretos y leyes en relación a la Seguridad Digital, siendo uno de ellos el Decreto Supremo 050-2018 (PCM-2018), el cual delimita y especifica de mejor manera este concepto. En este sentido establece que, con la finalidad de contribuir a un Estado más moderno y tomando en cuenta el informe de la OCDE "Recomendaciones sobre gestión de riesgos de seguridad digital para la prosperidad económica y social", la Seguridad Digital es el Estado de confianza[17] en el entorno digital logrado mediante la gestión de medidas proactivas y reactivas[18] frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales (Diario El Peruano, 2018).

Posteriormente, en el 2019, se aprueba la Ley N° 30999, conocida como la Ley de Ciberdefensa, la cual regula las operaciones militares en el ciberespacio para preservar la seguridad nacional, a cargo del Ministerio de Defensa. En este sentido, se encarga de "la protección de la soberanía, los intereses nacionales, los activos críticos nacionales[19] y recursos claves, para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional" (El Peruano, 2019). Es decir, busca salvaguardar la integridad y la funcionalidad de las infraestructuras del país frente a cualquier amenaza cibernética, asegurando así la estabilidad y seguridad del Estado. Por ende, ofrece las siguientes definiciones que complejizan el ámbito de la ciberdefensa (El Peruano, 2019, 02-04):

- Acto Hostil en el Ciberespacio: Definida como cualquier acción realizada en el ciberespacio que comprometa la seguridad nacional, la soberanía, los intereses nacionales o los ACN/RC, otorgando el derecho a ejercer la legítima defensa de acuerdo con las reglas de enfrentamiento establecidas por la autoridad competente.
- Amenaza en el ciberespacio: Cualquier acto o evento, interno o externo, que mediante sistemas o herramientas cibernéticas pueda causar daños a la

[17] Este emerge como "resultado de cuán veraz, predecible, seguro y confiable son las interacciones digitales que se generan entre empresas, individuos o cosas" (Diario El Peruano, 2018).
[18] Abarca "tecnología, políticas, controles, programas de capacitación y sensibilización que tienen por finalidad preservar la conciencialidad, integridad y disponibilidad de la información contenida en el entorno digital" (Diario El Peruano, 2018).
[19] Son los "recursos, infraestructuras y sistemas que son esenciales e imprescindibles para mantener y desarrollar las capacidades nacionales, o que están destinados a cumplir dicho fin" (Diario El Peruano, 2019).

seguridad nacional, la soberanía, los intereses nacionales, o los ACN/RC. También se conoce como ciberamenaza.

- Incidente de seguridad digital: Evento que puede comprometer la confianza, la prosperidad económica, la protección de personas y sus datos personales, así como la información y otros activos de la organización, mediante tecnologías digitales.
- Intención hostil en el ciberespacio: Acción que demuestra la voluntad o preparación para realizar un acto hostil en o mediante el ciberespacio contra la seguridad nacional, la soberanía, los intereses nacionales, o los ACN/RC. Estos actos suelen ser no cinéticos, dificultando su identificación y atribución.
- Riesgo de seguridad digital: Efecto de la incertidumbre en el uso y gestión de tecnologías y datos, debido a amenazas y vulnerabilidades digitales. Puede afectar objetivos económicos y sociales al comprometer la confidencialidad, integridad y disponibilidad de actividades, además de poner en riesgo la privacidad. Involucra tanto entornos físicos como digitales, actividades críticas, personas, organizaciones y procesos organizacionales.

Estas definiciones muestran la categorización que un ataque o incidente en el ciberespacio puede llegar a tener, lo que determinará su tratamiento. En este sentido, dentro del Artículo 5 del Capítulo III se establecen ciertas medidas, divididas en activas y pasivas coo se muestra en la siguiente tabla.

Tabla 2
Medidas pasivas y activas de la Ley de Ciberdefensa

Medidas Pasivas	Medidas Activas
Actividades de prevención, protección y resiliencia del ciberespacio propio y/o asignado.	Actividades de naturaleza proactiva, reactiva o de recuperación.
De aplicación constante y generalizada, abarcando al personal, medios y sistemas propios o asignados.	Involucra el análisis de vulnerabilidades, una labor de detección, evaluación, identificación y reconocimiento de actos hostiles o amenazas en el ciberespacio.
Involucra el monitoreo de redes propias o asignadas, mantenimiento de sistemas informáticos, actualizaciones de seguridad y operativas, establecimiento de políticas, disposiciones, procedimientos y reglas de seguridad institucional, robustecimiento en la infraestructura cibernética propia y la concientización en materia de ciberdefensa, entre otras.	Aplicación de acciones cibernéticas sobre medios o sistemas que constituyen una amenaza, para degradar o neutralizar sus capacidades y formas de acción, a fin de impedir que estas puedan afectar la libertad de acción en el ciberespacio propio, asignado y/o de interés, entre otras.

Fuente: Ley N° 30999, Artículo 5 del Capítulo III (El Peruano, 2019, p.06-07)

De este apartado se desprende el Artículo 6, el cual detalla las capacidades de ciberdefensa de los órganos encargados de esta área dividiéndolos en 4:

- Defensa: Dentro de esta se encuentran las acciones de prevención, protección y resiliencia de las diferentes plataformas tecnológicas o sistemas de información ante amenazas cibernéticas, actos hostiles u otros incidentes de seguridad digital. Por consiguiente, se hace uso de medidas pasivas y activas.
- Explotación: Consiste en la búsqueda, identificación, reconocimiento, vigilancia y seguimiento de ciberamenazas en el ciberespacio. Acá también se hace uso de medidas pasivas y activas.
- Respuesta: Se centra en limitar o negar, temporal o permanentemente, el uso del ciberespacio del objetivo militar mediante la degradación o neutralización de sus sistemas, solo se recurre a medidas activas.
- Investigación Digital: Consiste en el análisis de evidencia digital para determinar su funcionalidad, comportamiento, origen e impacto; así como su explotación futura a través de un proceso de análisis forense digital.

En este sentido, a través de la defensa, se implementan estrategias para proteger y mantener la resiliencia de los sistemas tecnológicos. Mediante la explotación, se monitorizan y se identifican las amenazas emergentes en el ciberespacio. La respuesta se activa para contrarrestar y mitigar amenazas activas, asegurando que se limite o niegue el uso del ciberespacio a actores maliciosos.

Finalmente, la Investigación Digital proporciona una comprensión detallada de los incidentes y amenazas, facilitando la mejora continua de las estrategias y tácticas de ciberdefensa.

En el 2020 se promulga el Decreto De Urgencia 007-2020 que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento. Dentro de este decreto se establece la definición de ciberseguridad, la cual es entendida como la “capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital” (El Peruano, 2020, p.07). Es decir, como las acciones destinadas a garantizar la seguridad y eficiencia de las infraestructuras digitales, protegiéndolas contra amenazas y vulnerabilidades. Estas acciones incluyen, pero no se limitan a, “la implementación de políticas de seguridad, el uso de tecnologías avanzadas para la detección y mitigación de amenazas, la capacitación continua del personal en prácticas seguras y la colaboración con otras entidades y sectores para fortalecer la defensa contra ciberataques” (El Peruano, 2020, p.07).

Los esfuerzos realizados para la creación de un marco legal y normativo en materia de Seguridad Digital se materializaron en el año 2020 con las operaciones de ciberdefensa durante las elecciones congresales. Finalmente, en febrero de este año, se emitió el Reglamento de la Ley de Ciberdefensa mediante el Decreto Supremo 017-2024-PCM. Esta normativa tuvo como objetivo reglamentar el marco normativo contenido en la Ley N° 30999 para “continuar asegurando los activos críticos, los recursos clave, la soberanía y los intereses nacionales en el ciberespacio” (Poder Ejecutivo, 2024). Esto refleja el esfuerzo del país por mejorar la protección de su ciberespacio y adaptarse a los desafíos que surgen en el entorno digital. Sin embargo, todavía hay áreas por mejorar, lo que resalta la necesidad de seguir desarrollando medidas más efectivas para fortalecer la defensa frente a las amenazas cibernéticas.

En conclusión, el Perú no ha sido ajeno a los avances y a la regulación del ámbito cibernético. En su normativa interna, ha pasado de tener una regulación mínima a una más compleja y actualizada, reflejando así su compromiso con la seguridad digital y la protección de sus activos críticos. La creación de entidades especializadas, como la Secretaría de Gobierno Digital y el Comando Operacional de Ciberdefensa, así como la promulgación de leyes como la Ley de Ciberdefensa, demuestran el esfuerzo del país por mantenerse a la vanguardia en este campo.

No obstante, aunque el Perú ha comenzado a desarrollar su normativa de ciberseguridad en los últimos 10 años, lo que muestra avances importantes, el país aún se encuentra en una fase de adaptación y aprendizaje. Dado que el ámbito de la ciberseguridad es altamente dinámico, con amenazas y ataques cada vez más sofisticados, es necesario que las políticas y estrategias no solo se implementen, sino que se revisen y ajusten constantemente para mantenerse al día con estos cambios.

2.3. El Grupo Guacamaya y su proyecto Fuerzas Represivas

Dentro de la región latinoamericana no existe diversidad de grupos hacktivistas, ya que la mayoría de los grupos que roban y filtran información confidencial lo hacen por fines económicos y por una compensación a cambio. En este sentido, Guacamaya es uno de los pocos, por no decir el único, grupo conocido en Latinoamérica que realiza actos ilegales en el ciberespacio para fines sociales. Por este motivo, este último apartado del capítulo realiza una descripción sobre quiénes son, qué buscan, sus implicancias en la región, y su más grande proyecto, llamado “Fuerzas Represivas”.

Guacamaya es un grupo hacktivista centroamericano creado en 2022, cuyo fin es revelar la injusticia que autoridades cometen contra poblaciones vulnerables, el territorio local y contra el planeta en general (Vicens, 2022). Según su propia autodefinición, son “una organización hacktivista comprometida con la privacidad, la libertad de expresión y la justicia en línea” (GuacamayanLeaks, 2022). De esta manera, el eje central por el que se guían es la protección ambiental y la crítica abierta al imperialismo norteamericano por su agresión a los pueblos de América. Tal y como han mencionado en diversas entrevistas, se consideran la representación de todas las personas afectadas ancestralmente por la invasión y el despojo a Abya Yala (término de las naciones indígenas para nombrar el continente americano) y “luchan contra el invasor, colono, neo colono, saqueador extractivista o cualquiera que viole los derechos, pasando por encima de comunidades, culturas milenarias, exterminando bosques, ríos y mares, para acumular lo que consideran riqueza” (La-Lista, 2022).

Lo mencionado queda plasmado en su poema titulado “Resistencia”, por el cual se guían (Enlace hacktivista, s/f). El poema es, básicamente, un llamado a la lucha y la perseverancia de los pueblos indígenas y nativos frente a la opresión y la colonización, de manera que se critica abiertamente la violencia y el saqueo

perpetrado por los colonizadores, mientras se resalta la importancia de la conexión profunda entre el pueblo y su tierra, representada por elementos naturales y símbolos culturales. Según la visión de Enlace Hacktivista, el objetivo de este poema es transmitir un mensaje de optimismo y esperanza, resaltando la capacidad del pueblo para 'florecer de nuevo' y resistir en su lucha por la libertad y la justicia. Esta perspectiva refleja una interpretación de la resiliencia y la determinación del pueblo frente a la adversidad.

El grupo Guacamaya inició sus actividades con ataques dirigidos principalmente a empresas privadas en Brasil, Venezuela y demás países de la región, vinculadas a sectores como el petrolero y minero. Por ejemplo, en Guatemala, en marzo de 2022, hackearon a la minera Compañía Guatemalteca de Níquel (CGN), subsidiaria de Solway Investment Group, revelando documentación dedicada al proyecto minero “Fénix”, donde se revelaron pagos a la Policía guatemalteca que persiguió y detuvo a activistas y periodistas opuestos al proyecto (Calles, 2022). Pronto ampliaron su alcance hacia las instituciones nacionales de defensa de varios países de la región, incluyendo a entidades como la Secretaría de la Defensa Nacional en México (SEDENA), Ministerio del Interior en Perú, Comando Conjunto de las Fuerzas Armadas en Chile, entre otros.

En un comunicado, publicado en septiembre en el sitio web “Enlace Hacktivista", el grupo señaló que los sistemas militares y policiales de México, Perú, El Salvador, Chile y Colombia habían sido objeto de ciberataques pertenecientes a la operación “Fuerzas Represivas”. De esta forma, el grupo mencionó específicamente a instituciones como el Estado Mayor Conjunto de las Fuerzas Armadas de Chile (EMCO), la Secretaría de la Defensa Nacional de México (SEDENA), la Fiscalía General de la Nación y el Comando General de las Fuerzas Militares de Colombia, la Fuerza Armada y la Policía Nacional Civil de El Salvador, el Ejército del Perú (EP) y el Comando Conjunto de las Fuerzas Armadas del Perú (CCFFAA).

La operación “Fuerzas Represivas” se habría llevado a cabo a través de una vulnerabilidad activa denominada “ProxyShell”, la cual afecta a los servidores Exchange de Microsoft en sus versiones 2013, 2016 y 2019. Esta vulnerabilidad permite la ejecución de código remoto y la falsificación de solicitudes de acceso desde el lado del servidor, aprovechando un conjunto de debilidades de seguridad en el servidor de correo. Es relevante mencionar que, desde el año 2021, esta vulnerabilidad era conocida y que Microsoft lanzó las actualizaciones de seguridad

correspondientes en abril y mayo de ese mismo año (Centro Nacional de Seguridad Digital, 2020, p.04-05).

El Estado Mayor Conjunto de Chile fue el primer objetivo del ataque, experimentando una filtración masiva de datos sensibles para la seguridad nacional, lo que incluyó la exposición de correos electrónicos enviados y recibidos entre 2012 y mayo de 2022 del EMCO, institución chilena que desempeña un papel importante en la inteligencia, operaciones y logística para la defensa nacional. El ataque incluyó la filtración de más de 400 mil mensajes de correo electrónico, algunos de los cuales estaban marcados como “reservado”, “secreto” y “ultra secreto”, porque abarcaban áreas críticas de defensa, como estrategias de ciberseguridad, sistemas de monitoreo de comunicaciones satelitales en las fronteras, y programas para la gestión de bases de datos de inteligencia (Ciper Chile, 2022).

En septiembre, se llevó a cabo un incidente destacado del proyecto hacktivista, en el cual se sustrajo información documental del SEDENA, así como 4,1 millones de correos electrónicos que abarcaban el período de 2016 a 2022. La filtración incluye comunicaciones entre el Secretario de la Defensa Nacional y el Secretario de Marina, información sobre el “Culiacanazo”, datos sobre la salud del presidente Andrés Manuel López Obrador, y contratos para la construcción del Tren Maya y el Aeropuerto Internacional de Tulum.

A partir de estas filtraciones, se conocieron varias revelaciones de impacto, incluyendo la vigilancia por parte del ejército mejicano de grupos feministas, los abusos sexuales al interior del ejército y los bloqueos para que las víctimas no denuncien, el espionaje a periodistas por medio del uso del software israelí Pegasus, y el papel del ejército en el caso Ayotzinapa[20] (Abi-Habib, 2022).

En octubre del mismo año se produjo un ciberataque similar en Perú, que afectó principalmente al Comando Conjunto de las Fuerzas Armadas y al Ejército peruano. En esta acción, Guacamaya accedió a 283 mil correos electrónicos de documentación militar. Estos documentos revelaron que el Perú tenía conocimiento sobre el armamento bélico de Chile. Además, se descubrió que hubo seguimiento de candidatos de izquierda durante las Elecciones Regionales y Municipales de 2022, especialmente a organizaciones como Patria Roja, y a sus miembros, como Vladimiro

[20] El caso Ayotzinapa, ocurrido en 2014, involucró la desaparición de 43 estudiantes en Guerrero, México. Las filtraciones revelaron información sobre la posible participación y omisión del ejército en los hechos (Comisión para la Verdad y Acceso a la Justicia en el Caso Ayotzinapa, s.f.)

Vegas. Los correos electrónicos también sugieren que el Ejército considera a estos partidos, así como al Frente Amplio y a Tierra y Libertad, como organizaciones de fachada de Sendero Luminoso (Infobae, 2023).

No obstante, Andrés Gómez de la Torre (exdirector de la Escuela Nacional de Inteligencia de la Dirección Nacional de Inteligencia) calificó el ataque a Perú como de "bajo ratio", puesto que, a diferencia de los demás países, la cantidad de documentos publicados es relativamente baja y principalmente serían "planes de carácter defensivo y no ofensivo" ante una eventual amenaza, por lo que no tendrían potencial de afectar las relaciones internacionales (RPP, 2022).

Luego de estos ataques, el grupo no ha tenido actividad reciente dentro de los últimos dos años. En este sentido, no han tenido publicaciones o mayores hackeos reportados en ningún sector específico. Esta pausa podría indicar diversas posibilidades, como una reestructuración interna, un cambio de estrategia o, incluso, una disolución del grupo. No obstante, esto no implica su desaparición, ya que los grupos hacktivistas pueden reactivarse o surgir nuevos en cualquier momento, debido a la naturaleza dinámica del entorno cibernético y a las diversas motivaciones que pueden impulsar estos actos.

Capítulo III: Recojo de información

En este capítulo se presenta la información recolectada de modo sistematizado y descriptivo, en función de las variables de estudio. Como se ha descrito en la sección metodológica, la información presentada aquí surgió del análisis de fuentes documentales y entrevistas realizadas, y será analizada en mayor profundidad en el Capítulo 4.

3.1. Participación del Perú en instituciones internacionales en materia de ciberseguridad y ciberdefensa

En esta sección, se recopiló información de diversas instituciones internacionales[21] relevantes en los campos de ciberseguridad y ciberdefensa, seleccionando aquellas con mayor presencia tanto a nivel global como regional. De esta manera, se distinguió tres tipos de relaciones que el Perú posee con estas instituciones. La primera se caracteriza por ser formal, lo que incluye su membresía y acuerdos suscritos. La segunda se caracteriza por una colaboración e interacción bilateral con instituciones que, aunque no son de membresía oficial, permiten el intercambio de información y recursos en materia de seguridad digital. Finalmente, la tercera corresponde a la ausencia de participación formal o colaboración bilateral, donde el Perú no mantiene ningún vínculo, ya sea por falta de alineación estratégica, limitaciones geográficas o prioridades nacionales diferentes.

Este enfoque permite no solo identificar las instituciones en las que el Perú participa de manera oficial, sino también su interacción en casos donde no se le reconoce como un miembro pleno. Esta información es importante para entender la inserción del Perú en el contexto internacional de la ciberseguridad y su compromiso con el desarrollo de la seguridad digital.

[21] Las instituciones, entendidas como reglas formales e informales que moldean el comportamiento de los Estados para facilitar la cooperación internacional (Keohane, 1984), incluyen organizaciones intergubernamentales, regímenes internacionales y convenciones, actuando como mecanismos normativos para responder a amenazas transnacionales como los ciberataques (Lallande, 2021; Guiora, 2018; Valencia, 2015)

3.1.1. Participación[22] formal del Perú en Instituciones Internacionales

En esta sección se incluyen las organizaciones y marcos en los que el Perú es miembro oficial o ha firmado acuerdos relevantes. Estas instituciones son espacios formales de cooperación donde la participación del país está regulada mediante tratados, normas o convenios específicos.

3.1.1.1. Convenio de Budapest sobre el Ciberdelito

Este convenio es el único instrumento internacional vinculante en materia de ciberdelitos, de manera que orienta a los países en la creación de leyes nacionales contra delitos cibernéticos y establece un marco para la cooperación internacional entre los Estados miembros. Además, es el primer tratado internacional que aborda delitos en Internet como “derechos de autor, fraude informático, pornografía infantil y violaciones de la seguridad de la red” (Consejo de Europa, 2001). De esta forma, el Convenio de Budapest tiene tres objetivos principales: crear un marco común de derecho penal sustantivo, estandarizar los métodos procesales y la informática forense, e impulsar la cooperación internacional.

La importancia del Convenio de Budapest radica en que brinda herramientas de cooperación con los demás países suscriptores y organismos internacionales para hacer frente a la ciberdelincuencia. Por ejemplo, se encuentran las solicitudes de asistencia mutua a través de medios de comunicación rápidos o el establecimiento de la Red 24/7 (Consejo de Europa, 2001). Así, facilita la rápida remisión de solicitudes formuladas por operadores jurídicos a nivel nacional, como jueces o fiscales, hacia los Estados Parte del Convenio como Estados Unidos de América, Italia, España, Japón, Canadá, Israel, Argentina, Chile, Costa Rica, Paraguay, República Dominicana, Panamá, Colombia, entre otros (Ministerio Público Fiscalía de la Nación, 2020). Además, es el único convenio encontrado para abordar el tema de la extradición mediante la cooperación internacional.

A pesar de que el Convenio fue promulgado el 2001, el Perú recién comienza a dar los primeros pasos para su adhesión con la Comisión de Defensa liderada por

[22] Es importante resaltar que la definición de "participación" se detalla en el apartado de metodología y operacionalización de variables. En este contexto, se refiere a la adhesión formal del Perú a instituciones internacionales que se dedican a promover la ciberseguridad y la ciberdefensa.

el Congresista Jorge del Castillo en el año 2011. En este sentido, se empezó a averiguar el estado en el que se encontraba el Convenio. No obstante, fue recién en el año 2018, con el Grupo de Trabajo de Ciberseguridad y Ciberdefensa, que el tema entró en la agenda del Congreso, y fue gracias a la presión de este grupo que el Perú finalmente lo adoptó en el 2019 (CISObeat, 2019) mediante la resolución Legislativa N°30913.

La adhesión del Perú al Convenio involucró la modificación de algunas leyes promulgadas. En este sentido, se revisó el Código Penal y Procesal del Delito y se emitió la Ley N°30171, donde se modificó los artículos 2; 3; 4; 5; 7; 8 y 10 de la Ley N°30096 acerca de Delitos Informáticos. Asimismo, involucró la creación normativa de peritaje forense o informática y el inicio del desarrollo de la Política Nacional de Ciberseguridad publicada en el 2019.

3.1.1.2. International Telecommunication Union (ITU)

Es una agencia especializada de las Naciones Unidas que se dedica a la regulación y estandarización de las telecomunicaciones y las tecnologías de la información. Su misión principal es coordinar el uso global del espectro radioeléctrico y las órbitas de satélite, así como establecer estándares técnicos que aseguren la interoperabilidad y la seguridad de las redes y servicios de telecomunicaciones en todo el mundo (United Nations Office at Geneva, s.f.).

El Perú es miembro de la UIT desde la aprobación de sus instrumentos de Constitución y Convenio Marco, junto con sus enmiendas, mediante la Resolución Legislativa N.º 26362 del 29 de septiembre de 1994. Con esta resolución, que ratificó los acuerdos adoptados en Ginebra en 1992, el Perú se incorporó oficialmente a la UIT, participando desde entonces en la formulación de políticas y decisiones globales en telecomunicaciones (Congreso de la República, 2002). En este sentido, el Perú se comprometió a participar activamente en las conferencias y reuniones, ejercer su derecho a voto en decisiones clave, y contribuir al desarrollo de las telecomunicaciones a nivel global y regional, según lo establecido en la Constitución y el Convenio de la UIT adoptados en Ginebra en 1992 (ratificados por el Perú mediante la Resolución Legislativa Nº 26362 en 1994).

3.1.1.3. Organización Internacional de Policía Criminal (INTERPOL)

Es una entidad intergubernamental que reúne a 196 países miembros y su misión es facilitar la colaboración entre las fuerzas policiales de estos países para promover la seguridad global mediante el intercambio y acceso a información sobre delitos y delincuentes. Todos los países miembros están conectados a través del sistema de comunicación I-24/7, un medio seguro que permite la comunicación entre ellos y con la Secretaría General de INTERPOL. (Organización Internacional de Policía Criminal [INTERPOL], s.f.-a). Los conocimientos especializados de INTERPOL respaldan las iniciativas nacionales contra la delincuencia en cuatro áreas prioritarias: terrorismo, ciberdelincuencia, delincuencia organizada y delincuencia financiera y corrupción. En el ámbito de la ciberseguridad y ciberdefensa, INTERPOL cuenta con divisiones especializadas como el Cybercrime Directorate y el INTERPOL Global Complex for Innovation (IGCI).

El Centro de Innovación de INTERPOL (IGCI) se organiza en cuatro laboratorios temáticos. El primer laboratorio es el de Inteligencia Artificial Responsable, el cual facilita la concienciación general sobre inteligencia artificial (IA), el intercambio de conocimientos y la colaboración entre expertos, con un enfoque en el uso responsable de esta tecnología. El segundo es el Laboratorio de Ciberespacio y Nuevas Tecnologías, el cual evalúa las principales formas de interrumpir, predecir e investigar amenazas emergentes en el ciberespacio. El tercero es el laboratorio de Forense Digital, el cual ofrece asistencia operativa en investigaciones forenses digitales, abarcando dispositivos móviles, sistemas aéreos no tripulados y equipos a bordo de embarcaciones incautadas mediante su proyecto “LEADER”. Finalmente, el laboratorio de Futuro y Prospectiva dedicado a identificar y analizar desarrollos globales en tecnología, estrategia y políticas (Interpol, s.f.-b).

El Perú se unió a INTERPOL tras la firma de su Estatuto en 1949, lo que le permite participar en una red internacional dedicada a la cooperación policial. A través de su Oficina Central Nacional (OCN), el país actúa como enlace entre los organismos nacionales de aplicación de la ley, otros países miembros y la Secretaría General de INTERPOL. Utilizando el sistema I-24/7, una red mundial de comunicación policial segura, la OCN facilita el intercambio de información vital en investigaciones criminales. Es fundamental resaltar que las OCN son el eje central de INTERPOL, ya que no solo buscan información en otras OCN para asistir en la investigación de delitos

y delincuentes en sus respectivos países, sino que también promueven la cooperación internacional en la lucha contra la ciberdelincuencia (INTERPOL, s.f.-c).

3.1.1.4. Organización de los Estados Americanos (OEA)

El Perú, como miembro activo de la OEA desde la firma de su Carta en 1948, ha desempeñado un papel significativo en el fortalecimiento de la ciberseguridad en la región. Este compromiso se refleja en diversas iniciativas que abarcan desde la suscripción de declaraciones clave hasta su participación en conferencias hemisféricas y el trabajo colaborativo con entidades especializadas.

En primer lugar, el Perú ha firmado importantes declaraciones de la OEA en materia de ciberseguridad, como la Declaración sobre Seguridad en las Américas y la Declaración de Bridgetown, adoptadas en 2002. Estas declaraciones introdujeron un enfoque multidimensional de la seguridad, influyendo en la "Política Nacional Multisectorial de Seguridad y Defensa Nacional al 2030", que redefinió las amenazas tradicionales para incluir los ataques cibernéticos como un riesgo para la seguridad nacional. Según el Ministerio de Defensa (Mindef), “el concepto de las amenazas tradicionales debe ampliarse y considerar también a los ataques cibernéticos” (Mindef, 2022, p.07). Asimismo, estas iniciativas “otorgaron nuevos roles a las Fuerzas Armadas en la defensa cibernética del país” (Álvarez, 2020, p.52).

Además, el Perú participó en la I Conferencia del Hemisferio Occidental sobre Ciberdefensa, organizada en 2019 por la Junta Interamericana de Defensa (JID). Este evento reunió a 170 representantes de alto nivel de 25 países, incluyendo autoridades militares, gubernamentales, académicas y del sector privado. La conferencia abordó temas como la conciencia de amenazas, la educación y capacitación en ciberseguridad, la protección de infraestructura crítica, y la colaboración entre sectores público y privado. Tras el éxito de esta edición, se llevó a cabo una segunda conferencia en 2020, que destacó la importancia de establecer un marco hemisférico de ciberdefensa. Entre las prioridades identificadas estuvieron “la mejora del entrenamiento cibernético, el intercambio de información no clasificada, y el fortalecimiento de instituciones y respuestas ante amenazas cibernéticas” (OEA, 2019, p.13-15).

Finalmente, el Perú ha trabajado activamente con entidades de la OEA como la JID, el Comité Interamericano contra el Terrorismo (CICTE) y el Foro

Iberoamericano de Ciberdefensa. Estas colaboraciones han permitido al país compartir experiencias, lecciones aprendidas y soluciones consensuadas con otros miembros, promoviendo un ciberespacio más seguro. Además, estas acciones facilitan la creación de redes de cooperación regional, esenciales en un entorno digital interconectado, y alinean al Perú con las mejores prácticas internacionales en ciberseguridad (Comando Conjunto de las Fuerzas Armadas, 2020).

3.1.1.5. El Foro Global de Experiencia en Ciberseguridad (GFCE)

Es una plataforma central para la cooperación internacional en el fortalecimiento de la ciberseguridad. Esta organización reúne a más de 200 miembros y socios, incluidos gobiernos, organizaciones internacionales, empresas y académicos de todas las regiones del mundo. Los miembros del GFCE están conformados por países, organizaciones intergubernamentales, organizaciones internacionales y empresas privadas que tienen el compromiso y los recursos para contribuir a la construcción de capacidades cibernéticas. El GFCE se organiza en grupos de trabajo, los cuales actúan como la plataforma global de referencia para que organizaciones e individuos aprendan, compartan y discutan temas de interés común, así como buenas prácticas relacionadas con la construcción de capacidades cibernéticas globales. Los grupos de trabajo, establecidos en 2018, se basan en los cinco temas clave identificados en el Comunicado de Delhi y un sexto tema sobre la integración de género e inclusividad, los cuales incluyen la Política y Estrategia de Ciberseguridad, la Gestión de Incidentes Cibernéticos y Protección de Infraestructuras Críticas, el Ciberdelito, la Cultura y Habilidades en Ciberseguridad, y las Tecnologías Emergentes (Global Forum on Cyber Expertise [GFCE], s.f.).

En los últimos ocho años, el GFCE ha crecido, convirtiéndose en una plataforma global de múltiples partes interesadas que promueve la transparencia y la conciencia sobre las actividades de construcción de capacidades cibernéticas. Esta evolución ha fomentado una mejor coordinación, colaboración y asociaciones entre los miembros. Para mejorar su coordinación, el GFCE se centra en reforzar un enfoque basado en la demanda mediante la expansión con enlaces y oficinas regionales, las prioridades principales incluyen fomentar la inclusividad en la red del GFCE, empoderar a los centros regionales en África, América Latina, el Caribe, el Pacífico y el Sudeste Asiático, establecer una agenda global, aumentar el intercambio

de información y liderar esfuerzos para integrar la perspectiva de género en la construcción de capacidades cibernéticas (GFCE, s.f.). Perú ha sido miembro del GFCE desde 2016, lo que le ha permitido participar en esta plataforma global para mejores prácticas en ciberseguridad como el Americas and Caribbean regional meeting en el año 2021.

3.1.2. Colaboración externa o bilateral

Se refiere a la interacción del Perú con instituciones internacionales sin ser miembro oficial, mediante acuerdos específicos o intercambios de información, asistencia técnica o cooperación en proyectos puntuales en materia de ciberseguridad. Estas relaciones permiten al país beneficiarse del conocimiento y recursos compartidos sin los compromisos formales de la membresía.

3.1.2.1. La Organización del Tratado del Atlántico Norte (OTAN)

Es una alianza militar intergubernamental creada para la defensa mutua entre países europeos y América del Norte, promoviendo la seguridad y cooperación internacional. Sus miembros son 30 países, incluyendo Estados Unidos, Canadá, países de Europa Occidental y Europa del Este (Organización del Tratado del Atlántico Norte [OTAN], s.f.).

Centrada inicialmente en la defensa durante la Guerra Fría, la OTAN mostraba poco interés en relaciones con Estados no miembros, especialmente de América Latina. No obstante, luego del fin de la misma y a partir de diversos sucesos como el atentado del 11 de septiembre y el surgimiento de nuevos fenómenos globales como la ciberdelincuencia y el cambio climático, la OTAN notó la “necesidad de un mayor enfoque global en el relacionamiento de la Organización con terceros Estados, por lo que se ha acercado a Asia, África, Oceanía y América” (Jimenez, 2022, p.35-40).

Perú comenzó a relacionarse con la OTAN desde 2019, una relación que se intensificó con el comunicado de la Cumbre de Bruselas de 2021, la cual enfatizó que, con el fin de promover las capacidades de la OTAN, la organización buscará nuevos interlocutores en regiones como América Latina. En este sentido, “a pesar de no ser miembro, puede aportar al Centro de Excelencia en Ciberdefensa Cooperativa

(CCDCOE) y al Comité Directivo como participante contribuyente" (Jimenez, 2022, p.161).

La OTAN representa una organización importante a considerar porque "representa el máximo referente mundial en ciberdefensa que sirve como modelo para que los Estados, incluido el Perú, puedan proteger sus infraestructuras críticas y desarrollar modelos para operaciones cibernéticas" (Oficial Freitas, O., comunicación personal, 06 de mayo del 2024). En este sentido, la participación y colaboración con la OTAN en temas de ciberdefensa y ciberseguridad permite al Perú adoptar prácticas y estándares internacionales que fortalezcan su seguridad nacional y regional en el ciberespacio.

3.1.2.2. La Asia Pacific Computer Emergency Response Team (APCERT)

Es una organización que agrupa a los Equipos de Respuesta a Emergencias Informáticas (CERT) y a los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) en la región de Asia-Pacífico. Por ello, tiene como misión crear un ciberespacio seguro, limpio y confiable en la región a través de la colaboración y cooperación global. De acuerdo con lo citado en Chacha (2019), entre los principales objetivos del APCERT se encuentran "fomentar la cooperación en seguridad informática, compartir conocimientos técnicos sobre amenazas como virus, impulsar proyectos colaborativos de investigación y desarrollo, asistir a otros equipos de respuesta y proporcionar recomendaciones legales para gestionar la seguridad informática a nivel transfronterizo" (Asia Pacific Computer Emergency Response Team [APCERT], 2003, como se citó en Chacha, 2019, p. 17).

Desde 2003, ha estado publicando informes anuales que proporcionan análisis detallados de incidentes de seguridad ocurridos en la región, identifican tendencias emergentes en el panorama de amenazas cibernéticas y ofrecen recomendaciones específicas para mejorar la ciberseguridad (APCERT, s.f.). Perú no es miembro y no se ha adherido formalmente, pero se encontró que APCERT participa en los foros intra-gubernamentales como APEC, del cual Perú sí es parte. En este sentido, a través de estos foros, APCERT ayuda a mejorar la ciberseguridad en la región de Asia-Pacífico, beneficiando indirectamente a países no miembros como Perú al compartir conocimientos, mejores prácticas y recomendaciones estratégicas para enfrentar amenazas cibernéticas (APCERT, 2003).

3.1.3. Ausencia de colaboración y participación

Hace referencia a aquellos casos en los que el Perú no mantiene ningún vínculo formal ni cooperativo con determinadas instituciones. En estos casos, el país no participa ni colabora activamente, lo que refleja un menor grado de integración o interés en los temas abordados por dichas instituciones.

3.1.3.1. La Agencia de la Unión Europea para la Ciberseguridad (ENISA)

ENISA, establecida en 2004, es la entidad encargada de promover un nivel elevado y uniforme de ciberseguridad dentro de la Unión Europea. Para ello, “apoya el desarrollo de políticas, promueve esquemas de certificación en TIC, coopera con Estados Miembros y organismos de la UE, y fortalece la preparación ante amenazas cibernéticas mediante acciones de sensibilización, creación de capacidades e intercambio de información clave” (Parlamento Europeo y Consejo de la Unión Europea, 2019).

La normativa que rige a ENISA es el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de la UE del 17 de abril de 2019 (Ley de Ciberseguridad), que deroga el Reglamento (UE) Nº 526/2013. De esta manera, ENISA se compromete a asistir a los Estados Miembros en mejorar la prevención, detección y capacidad de respuesta ante amenazas e incidentes cibernéticos, proporcionando conocimientos y experiencia. Esto incluye el desarrollo de CSIRTs nacionales, estrategias nacionales sobre la seguridad de sistemas de red e información, y estrategias de la Unión en ciberseguridad, promoviendo su difusión y monitoreando su implementación. Además, organiza ejercicios de ciberseguridad regularmente, al menos cada dos años, y formula recomendaciones políticas basadas en la evaluación de estos ejercicios y las lecciones aprendidas. Finalmente, ENISA contribuye a los esfuerzos de la Unión para cooperar con terceros países y organizaciones internacionales, promoviendo la cooperación internacional en cuestiones de ciberseguridad (European Union, 2019).

Tras una revisión de las fuentes disponibles y de los registros pertinentes, no se han encontrado vínculos formales entre ENISA y Perú, por lo que no se ha identificado ninguna conexión directa o relevante con este país. La ausencia de

vínculos puede deberse a la falta de actividades conjuntas documentadas, proyectos compartidos o colaboraciones formales entre las entidades involucradas.

3.1.3.2. La Agencia de Implementación de la Comunidad del Caribe (CARICOM) para la Criminalidad y la Seguridad (IMPACS)

Fue establecida en julio de 2006 durante la Vigésima Séptima Reunión de la Conferencia de Jefes de Gobierno en Bird Rock, St. Kitts y Nevis. Su creación respondió a la necesidad de gestionar y ejecutar una nueva Arquitectura Regional destinada a abordar la agenda de acción de CARICOM en materia de criminalidad y seguridad.

En este encuentro, los Jefes de Gobierno firmaron un Acuerdo Inter-Gubernamental que estableció a IMPACS como una entidad legal con responsabilidades directas en investigación, monitoreo y evaluación, análisis y preparación de documentos y reportes, así como en el desarrollo e implementación de proyectos relacionados con la agenda regional de criminalidad y seguridad (Agencia de Implementación de la Comunidad del Caribe para la Criminalidad y la Seguridad [CARICOM IMPACS], s.f.).

IMPACS se compromete a mejorar la seguridad en la región del Caribe a través de una amplia gama de proyectos e iniciativas. Su programa insignia, la Estrategia de Criminalidad y Seguridad de CARICOM, se enfoca en fortalecer la aplicación de la ley, la seguridad fronteriza y el intercambio de inteligencia. Además, lidera el "Caribbean Citizen Security Toolkit", que proporciona formación y recursos para la prevención del crimen basada en la comunidad.

El Sistema de Seguridad Regional coordina ejercicios militares conjuntos y patrullajes para responder a amenazas. También trabaja en iniciativas como la lucha contra el extremismo violento, la ciberseguridad y la seguridad marítima (CARICOM IMPACS, s.f.). No obstante, no se ha encontrado una relación directa entre Perú y esta organización hasta el momento.

3.1.3.3. El Foro Africano de Equipos de Respuesta a Incidentes Informáticos (AfricaCERT)

Este tiene como misión proponer soluciones a los desafíos de Internet de África. Entre sus objetivos principales se encuentra coordinar la cooperación entre los CSIRT,

facilitando la colaboración entre los equipos de respuesta a incidentes de seguridad informática en el continente. De esta manera, AfricaCERT asiste a los países africanos en el establecimiento de CSIRT, proporcionando experiencia y asesoramiento en la formulación de iniciativas, programas y proyectos destinados a la creación de estos equipos. Además, fomenta y apoya programas de educación y divulgación en seguridad informática, ayudando a sus miembros a adquirir las habilidades técnicas, el conocimiento y la experiencia necesarios para llevar a cabo respuestas efectivas a emergencias informáticas (Foro Africano de Equipos de Respuesta a Incidentes Informáticos [AfricaCERT], s.f.).

Otro objetivo importante de AfricaCERT es fortalecer las relaciones entre los CSIRT en África con otros actores globales, construyendo cooperación, confianza y colaboración para una gestión efectiva de incidentes de seguridad. Para ello, fomenta el intercambio de información en seguridad informática, compartiendo hallazgos de incidentes reportados y estudios de caso para identificar rápidamente vulnerabilidades y neutralizar sus riesgos. Los miembros de AfricaCERT también desarrollan conjuntamente medidas para abordar incidentes de seguridad y emergencias a gran escala. Finalmente, AfricaCERT promueve la investigación tecnológica colaborativa, el desarrollo y la innovación en el campo de la seguridad informática. Con estos objetivos, AfricaCERT se dedica a fortalecer la capacidad de respuesta a incidentes de seguridad informática en África y a mejorar la preparación cibernética, fomentando la cooperación y el intercambio de conocimientos entre los CSIRT y otras partes interesadas a nivel mundial (AfricaCERT, 2023, p.02).

Respecto a su relación con Perú, no se ha encontrado ninguna relación directa, lo que indica que hasta el momento no existen colaboraciones o iniciativas conjuntas entre el país sudamericano y el foro africano de equipos de respuesta a incidentes informáticos.

3.1.3.4. La Agencia de Seguridad Nacional/Servicio Central de Seguridad (NSA/CSS)

Como parte del Departamento de Defensa de los EE. UU., actúa como una agencia de apoyo en combate. Un aspecto importante de su labor es colaborar con los miembros del servicio militar en todo el mundo. Por ejemplo, en años anteriores, analistas, lingüistas, ingenieros y otros profesionales de la NSA se despliegan en

Afganistán y otras áreas para ofrecer apoyo de SIGINT y ciberseguridad a los combatientes en las líneas del frente, mientras que su personal de ciberseguridad, junto con productos y servicios especializados, asegura que las comunicaciones y datos militares permanezcan protegidos y fuera del alcance de los adversarios (Agencia de Seguridad Nacional [NSA/CSS], s.f.).

El tema de ciberseguridad lo trabaja el Centro de Colaboración en Ciberseguridad de la NSA (CCC) que colabora con la industria, agencias gubernamentales y socios internacionales para fortalecer la Base Industrial de Defensa de EE. UU., operacionalizar los conocimientos únicos de la NSA sobre amenazas cibernéticas de estados-nación, desarrollar conjuntamente guías de mitigación para actividades emergentes y desafíos crónicos de ciberseguridad, y asegurar tecnologías emergentes (NSA/CSS, s.f.).

A pesar del amplio alcance y las múltiples colaboraciones de la NSA a nivel internacional, no se encontró información que demuestre que Perú colabora directamente con la NSA. Esta falta de evidencia puede deberse a varios factores, como la confidencialidad de las relaciones en seguridad nacional, la ausencia de acuerdos formales de colaboración, o la posibilidad de que cualquier cooperación existente no haya sido divulgada públicamente. La NSA, conocida por la naturaleza reservada de sus operaciones, podría tener acuerdos bilaterales o multilaterales que no se revelan públicamente. Sin embargo, con la información disponible, no hay datos que respalden una colaboración explícita entre Perú y la NSA en temas de inteligencia de señales o ciberseguridad.

3.1.3.5. El Centro de Seguridad de las Comunicaciones (CSE) de Canadá

Nació durante la Segunda Guerra Mundial, y fue fundado en 1946 como la agencia de inteligencia de señales y seguridad de comunicaciones de Canadá. Desde su fundación, CSE mantiene numerosas asociaciones y relaciones con organizaciones tanto en Canadá como en todo el mundo, sobre todo con Estados Unidos, el Reino Unido, Australia y Nueva Zelanda, conocidos colectivamente como los socios de los "Cinco Ojos" (Centro de Seguridad de las Comunicaciones [CSE], s.f.).

La ciberseguridad es una parte clave del mandato de CSE, por lo que usan su experiencia técnica para proteger la información y los sistemas de los que dependen los canadienses diariamente. A través del Centro Canadiense para la Ciberseguridad del CSE, se defienden las redes del Gobierno de Canadá y se asesora a otros niveles

de gobierno y operadores de infraestructuras críticas como bancos y compañías de telecomunicaciones. Asimismo, colabora estrechamente con departamentos gubernamentales, provincias, territorios, municipios, infraestructuras críticas, negocios canadienses, académicos y socios internacionales para elevar el nivel de ciberseguridad (CSE, s.f.).

Las operaciones cibernéticas activas permiten al CSE tomar medidas en línea para interrumpir las capacidades de amenazas como grupos terroristas extranjeros, ciberdelincuentes, agencias de inteligencia hostiles y hackers patrocinados por estados. Por ejemplo, el CSE podría deshabilitar dispositivos de comunicación utilizados por un grupo terrorista extranjero para planificar ataques. Las amenazas que se interrumpen deben estar relacionadas con asuntos internacionales, defensa o seguridad. Cabe resaltar que todas las actividades del CSE están sujetas a revisión por parte de la Agencia de Revisión de la Seguridad Nacional y la Inteligencia (NSIRA) y el Comité de Parlamentarios de Seguridad Nacional e Inteligencia (NSICOP) (CSE, s.f.).

No obstante, al igual que con la NSA, no se ha encontrado información que demuestre una colaboración directa entre Perú y el CSE. Esta ausencia de evidencia puede deberse a varios factores, como la falta de acuerdos formales de colaboración entre ambos países en el ámbito de la inteligencia y la ciberseguridad.

En resumen, el Perú participa activamente en varias instituciones internacionales relacionadas con la ciberseguridad, consolidando su presencia en plataformas orientadas a la cooperación y el fortalecimiento de capacidades en este ámbito. Entre las más relevantes se encuentran la OEA, el GFCE y el Convenio de Budapest, donde el país ha colaborado en el desarrollo de marcos regulatorios, intercambio de buenas prácticas y fortalecimiento de competencias cibernéticas.

Asimismo, instituciones como el CICTE y la JID, vinculadas a la OEA, han sido espacios importantes para el Perú en la búsqueda de mejorar sus capacidades en ciberdefensa y seguridad. A través de su participación, ha contribuido al desarrollo de iniciativas regionales en áreas clave como la gestión de incidentes, la capacitación cibernética y la protección de infraestructuras críticas.

No obstante, la participación del Perú no abarca todos los foros internacionales existentes en el ámbito de la ciberseguridad. Su ausencia en organismos como la NSA/CSS, CARICOM IMPACS y APCERT puede responder a limitaciones geográficas. Estas restricciones, aunque razonables, limitan el acceso del Perú a

ciertas iniciativas que podrían resultar valiosas para abordar amenazas compartidas, especialmente considerando el carácter transnacional de los ciberataques.

En términos de beneficios, la participación del Perú en estas plataformas internacionales le ha permitido fortalecer su infraestructura cibernética, acceder a recursos técnicos y financieros, y colaborar en el desarrollo de normativas y políticas de seguridad digital. Sin embargo, algunos ámbitos de la ciberdefensa permanecen desatendidos. Por ejemplo, la integración de sectores como el sector privado y la sociedad civil en estrategias nacionales de ciberseguridad es aún limitada.

En balance, la participación internacional del Perú ha contribuido a fortalecer su ciberseguridad, pero la información recolectada también evidencia áreas de oportunidad. En un contexto global donde las amenazas cibernéticas no reconocen fronteras, se hace necesario que el Perú siga expandiendo su compromiso con plataformas internacionales, identificando y cerrando las brechas existentes para consolidar una respuesta integral a los desafíos del entorno digital.

3.2. Mecanismos de cooperación

Este apartado contiene las acciones concretas de cooperación que la participación en instituciones le ha brindado al Perú.

3.2.1. Consultas realizadas por el Perú para el desarrollo o actualización de normativas

3.2.1.1. Apoyo de la OEA para la redacción del documento sobre la Estrategia Nacional de Ciberseguridad

En abril de 2015, se llevó a cabo en Lima, una Mesa de Discusión para el Desarrollo de una Estrategia Nacional de Seguridad Cibernética, auspiciada por el Comité Interamericano contra el Terrorismo (CICTE) de la Organización de Estados Americanos (OEA), el gobierno de Canadá y la Oficina Nacional de Gobierno Electrónico y Estadística (OEA, 2015, p.01). Este evento contó con la participación de profesionales de la Dirección General de Política y Estrategia de la SEDENA y se enmarcó en las políticas nacionales de Modernización del Estado y de Gobierno Electrónico, aprobadas por el Estado Peruano en 2013, con el objetivo de “garantizar

la integridad, confidencialidad y disponibilidad de la información en la administración pública, así como de articular los temas de ciberseguridad en el Estado" (Perú, 2015, p. 02).

Asimismo, a través del Programa de Seguridad Cibernética de la JID, el Perú recibió asistencia técnica mediante capacitaciones, mesas redondas sobre políticas, ejercicios de gestión de crisis e intercambio de mejores prácticas en el uso de tecnologías de la información y la comunicación. También, dicha asistencia contribuyó a la elaboración del Documento de Trabajo de la Estrategia Nacional de Seguridad y Confianza Digital 2021-2026, publicado en 2021. Este documento recoge sugerencias y aportes provenientes de diversas mesas de discusión y expertos en el campo, incluyendo los de la OEA. Si bien este documento no constituye una Estrategia Nacional oficial, representa un paso importante hacia la conformación de dicha estrategia (El Peruano, 2021).

Además de este caso, no se encontraron otras solicitudes o consultas realizadas por Perú a instituciones internacionales para el desarrollo o actualización de normativas específicas de seguridad cibernética.

3.2.2. Programas de capacitación y ejercicios conjuntos en los que el Perú ha participado

3.2.2.1. Programa de Ciberdefensa De La Junta Interamericana de Defensa (JID):

El Programa es una iniciativa de la OEA destinada a promover la seguridad y defensa en el ciberespacio. A través de esta plataforma, Perú se involucra en actividades que abarcan desde la prevención hasta la respuesta ante ciberataques, así como la recuperación de sistemas afectados. Esto se lleva a cabo mediante entrenamientos, ejercicios conjuntos y capacitaciones dirigidas a las autoridades pertinentes.

El Programa establece una Guía de Ciberdefensa que proporciona lineamientos para implementar una defensa militar efectiva en el ámbito cibernético. Los entrenamientos en ciberdefensa se extienden por 40 horas, divididas en 16 horas para legisladores y responsables de la toma de decisiones, y 24 horas para

autoridades técnicas. Además, se ofrece acceso al Cyber Range [23]durante un año para garantizar una formación continua y proporcionar asistencia en la resolución de consultas. Como parte del programa, se realizan simulaciones de crisis que involucran dos ejercicios de ocho horas cada uno. Estos ejercicios permiten a los responsables de la toma de decisiones y las autoridades técnicas aplicar los conocimientos adquiridos durante los entrenamientos anteriores. En 2021, solo Argentina, México y Colombia completaron estas simulaciones, mientras que Perú no logró finalizarlas y quedó pendiente (Junta Interamericana de Defensa [JID], 2021), lo que sugiere brechas en su nivel de preparación para enfrentar ciberamenazas de manera integral.

3.2.2.2. Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la OEA

El Comité Interamericano contra el Terrorismo (CICTE) busca promover y desarrollar la cooperación entre los Estados Miembros de la OEA para prevenir, combatir y eliminar el terrorismo. En el ámbito de la ciberseguridad, el CICTE apoya la creación de CSIRTs (Equipos de Respuesta a Incidentes de Seguridad Informática) y fomenta una red hemisférica 24/7 para divulgar rápidamente información sobre seguridad cibernética (Moreno, s.f.). Entre sus actividades se incluyen talleres y conferencias hemisféricas sobre seguridad cibernética, cursos básicos y avanzados sobre la creación y manejo de CSIRTs, y el fortalecimiento de alianzas con organizaciones nacionales, regionales, internacionales y el sector privado (Moreno, s.f.).

En 2023, Perú se unió al CSIRTAmericas (red que impulsa el Programa de Ciberseguridad del CICTE) incorporando el Centro Nacional de Seguridad Digital (CNSD) a la red de Equipos de Respuesta ante Incidentes Cibernéticos Gubernamentales de los Estados Miembros de la OEA. Cabe resaltar que aunque esta incorporación ocurrió después del ataque del grupo Guacamaya, es relevante mencionarla porque representa un paso hacia la mejora de las capacidades nacionales en ciberseguridad. En este sentido, permite al Perú acceder a asistencia técnica y capacitación continua, así como coordinar acciones con equipos internacionales, lo que contribuye a la preparación del país frente a futuros incidentes

[23] Entorno digital diseñado para la formación, evaluación e investigación en ciberseguridad, capaz de replicar redes y simular ciberataques reales.

y refuerza su alineación con la Política Nacional de Transformación Digital, como lo mencionó Alain Dongo, secretario de Gobierno y Transformación Digital de la PCM (Gestión, 2023).

3.2.2.3. Taller 4 - Red 24/7 del Convenio de Budapest

La reunión de la Red 24/7 del Convenio de Budapest llevada a cabo el 8 de noviembre de 2020 se desarrolló en un contexto de creciente sofisticación de la ciberdelincuencia y la necesidad de cooperación internacional. Desde 2017, “estos encuentros buscan fortalecer la eficacia de la Red, promover el intercambio de prácticas, procedimientos y herramientas entre puntos de contacto, y mejorar la tramitación de solicitudes transfronterizas” (Council of Europe, 2022).

El taller presentó el marco y las prácticas de varios países de la región, fomentando debates sobre las necesidades nacionales para integrar de manera fluida las nuevas responsabilidades del POC 24/7. De igual manera, el evento incluyó observaciones introductorias y objetivos del taller, una actualización sobre el funcionamiento de la Red 24/7, una mesa redonda sobre prácticas actuales de cooperación en emergencias, una sesión de preguntas y respuestas, y conclusiones con perspectivas de futuro (Council of Europe, 2022).

Entre los participantes[24] se contó con expertos de alto nivel de Chile, República Dominicana y Perú, lo que permitió el intercambio de experiencias y buenas prácticas en cooperación judicial y ciberseguridad (Centro de Estudios Internacionales Gilberto Bosques, 2022). Estas intervenciones permitieron intercambiar experiencias y enfoques nacionales, destacando la importancia de la cooperación internacional en la lucha contra la ciberdelincuencia. Se discutieron estrategias para mejorar la respuesta rápida y efectiva a incidentes cibernéticos, así como la integración de mejores prácticas y tecnologías avanzadas para fortalecer la seguridad cibernética a nivel regional y global.

[24] Entre los oradores destacados estuvieron Antonio Segovia Arancibia, Director de la Unidad de Cooperación Internacional y Extradición del Ministerio Público de Chile; Armando Díaz, Encargado del Departamento de Ciberseguridad de la Procuraduría General de la República y Miembro de la unidad de Puntos de Contacto 24/7 DICAT/PGR de la República Dominicana; y Lizet Nancy Rodríguez Rocha, Fiscal Provincial Adjunta de la Unidad de Cooperación Judicial Internacional y Extradiciones del Ministerio Público de Perú.per

3.2.2.4. Ejercicio Conjunto del Foro Iberoamericano de Ciberdefensa

Perú participó en el V Ejercicio Conjunto del Foro Iberoamericano de Ciberdefensa en Bogotá, Colombia, según la Resolución Ministerial Nº 0600-2021. La autorización incluyó a personal militar[25] de distintas ramas de las Fuerzas Armadas, y la participación fue financiada con recursos del Presupuesto Institucional del Año Fiscal 2021, aprobado por el Comando Conjunto de las Fuerzas Armadas. Esta misión requirió una inversión mínima por parte del Estado Peruano (Ministerio de Defensa [Mindef], 2021).

Durante su participación en el Foro Iberoamericano de Ciberdefensa en 2021, la delegación peruana obtuvo el tercer lugar entre doce países. El ejercicio permitió evaluar capacidades nacionales de respuesta ante amenazas digitales que afectan tanto a la población civil como a la militar. Además del reconocimiento, esta experiencia promovió la cooperación internacional, el fortalecimiento de las infraestructuras críticas y la mejora de estrategias frente a incidentes cibernéticos (Comando Conjunto de las Fuerzas Armadas, 2021).

3.2.2.5. Programa Generar Integridad de la OTAN

El programa Generar Integridad (GI) apoya a los países aliados y socios de la OTAN en la promoción de la buena gobernanza y la implementación de los principios de integridad, transparencia y rendición de cuentas en el sector de defensa y seguridad (OTAN, 2022). En marzo de 2021, “la OTAN invitó a Perú a unirse a este programa, y el 15 de septiembre de 2021, los Aliados de la OTAN aprobaron su incorporación, de manera que los ministerios peruanos involucrados son Defensa, Interior y Relaciones Exteriores” (Jimenez, 2022, p.47).

El programa contribuye a las tareas fundamentales de la OTAN: defensa colectiva, gestión de crisis y seguridad cooperativa, y está diseñado según las necesidades de cada Estado participante. De esta forma, el Perú es participante de sus cursos en liderazgo de ciberdefensa, uno de ellos se dio entre el 7 y el 11 de noviembre del 2022, donde cerca de 70 personas influyentes del sector de defensa y

[25] El personal autorizado incluyó al General de Brigada EP Ángel Augusto Sosa Guevara, al Capitán EP César Iván Márquez Orihuela, al Teniente Primero AP Ramón Mijail Jauregui Iparraguirre y al Teniente FAP Kenny Keith Meza Chalco. El costo total fue de US$ 6968.00.

seguridad participaron. Durante la semana de actividades, los asistentes recibieron formación sobre el papel de las personas influyentes en promover reformas para la integridad y la buena gobernanza. Aprendieron a adoptar estos principios en las operaciones y misiones de defensa, destacando su carácter transversal. Las sesiones incluyeron una variedad de formatos didácticos, como sesiones plenarias, ejercicios prácticos, actividades de representación y mesas redondas, lo que facilitó un valioso intercambio de conocimientos y experiencias (OTAN, 2022).

En gran medida, las instituciones internacionales ofrecen mecanismos de cooperación que se centran en ejercicios conjuntos y programas técnicos de capacitación. Este enfoque resalta la importancia crítica de mantenerse actualizado con las técnicas y procedimientos necesarios para protegerse en el ámbito cibernético. Para el Perú, es crucial adoptar estas prácticas y posteriormente fortalecerlas mediante alianzas estratégicas con países líderes en esta área (Comandante Ojeda, D., comunicación personal, 06 de mayo del 2024).

3.2.3. Fondos recibidos por el Perú a través de iniciativas internacionales de ciberseguridad y ciberdefensa

La investigación no identificó financiamiento significativo proveniente de instituciones internacionales en temas de ciberseguridad y ciberdefensa. Apenas se halló evidencia de un gasto relacionado con la participación del Perú en la "I Conferencia de Ciberdefensa en el Hemisferio Occidental", realizada en Bogotá los días 14 y 15 de mayo de 2019. Este viaje fue autorizado mediante la Resolución Ministerial N° 041-2019/DP-JID-OEA del 05 de febrero de 2019 y el Informe Técnico N° 156-2019-MINDEF/VPD/DIGRIN/e del 22 de abril de 2019. La Comisión estuvo integrada por tres altos representantes[26] del sector defensa, asignados para coordinar esta misión

El propósito de este viaje fue permitir a los participantes conocer y verificar las herramientas y medios que pueden implementarse para operaciones en el ciberespacio en territorio nacional. Además, se buscó establecer vínculos y estrechar

[26] Los integrantes fueron: el General de Ejército César Augusto Astudillo Salcedo, Jefe del Comando Conjunto de las Fuerzas Armadas; el Mayor General FAP Augusto Alberto García Calderón Sandoval, Jefe de la 6ta DIEMFA; y el General de Brigada EP Juan Carlos Lescano Albán, Director General de Política y Estrategia del Ministerio de Defensa.

la cooperación con representantes de países que cuentan con capacidades en ciberdefensa. La financiación de los gastos relacionados con el transporte aéreo, alojamiento y alimentación para estos representantes fue asumida por la "Fundación Interamericana de Defensa", sin ocasionar ningún costo al Tesoro Público peruano como se refleja en la Resolución Ministerial 0573-2019 (Mindef, 2019).

Al respecto, es necesario resaltar que este fue el único monto que se encontró hasta el 2022. Esto se debe a que la financiación en instituciones no es muy común y si existe se limita a ser para cubrir cursos de capacitación o asistencia a conferencias, pero no para construir o implementar un centro de ciberdefensa, porque esa responsabilidad recae en el Estado por lo que se debe usar recursos estatales (Oficial Freitas, O., comunicación personal, 06 de mayo del 2024).

3.3. Respuesta del Estado peruano frente al ataque de Guacamaya

Los productos informáticos [27]nunca son perfectos; todos tienen vulnerabilidades, por lo que sus creadores están obligados a comunicar a los compradores sobre las actualizaciones y posibles fallos de seguridad. Por ejemplo, al adquirir licencias de plataformas digitales de grandes corporaciones, como las utilizadas para correos electrónicos, se espera que el producto, como Windows, informe sobre actualizaciones y vulnerabilidades.

Guacamaya explotó una vulnerabilidad en los correos de Windows para acceder a la información de los correos electrónicos de las Fuerzas Armadas del Perú. La filtración de información incluyó presentaciones, mensajes y archivos de PowerPoint, entre otros. Sin embargo, esta filtración se limitó a una muestra específica de información administrativa, la cual fue posteriormente publicada en la dark web con el anuncio de que se trataba de información relacionada con el Perú.

Según un comandante del Comando Conjunto de las Fuerzas Armadas del Perú (entrevista personal, 06 de mayo del 2024), los correos electrónicos se utilizan principalmente para intercambiar información de rutina, y no suelen contener datos confidenciales, ya que existen políticas de seguridad estrictas al respecto. Por ello, la información filtrada no era confidencial, como habían anunciado diversos medios, como La Encerrona, sino más bien de naturaleza administrativa. Además, no se pudo

[27] Dispositivos y software diseñados para procesar, almacenar, y comunicar información digitalmente

confirmar que esta información filtrada proviniera del Comando Conjunto, lo que cuestiona aún más la relevancia y autenticidad de la información divulgada.

3.3.1. Tiempo promedio de detección del ataque

El 2 de marzo de 2021, Microsoft emitió un comunicado destinado a abordar la identificación de diversas vulnerabilidades dentro del servidor Microsoft Exchange Server, el cual es una infraestructura desarrollada por Microsoft destinada a la gestión de correo, calendario y colaboración (Microsoft, 2021). En este sentido, se expusieron 3 vulnerabilidades: la CVE-2021-34473[28], CVE-2021-34523[29] y la CVE-2021-31207[30], lo que Microsoft en conjunto pasó a llamar ProxyShell, la cual habilita el acceso a las direcciones de correo electrónico empresarial y facilita la instalación de software externo para asegurar la continuidad de presencia en el entorno de la víctima (Tenable, 2023). Esto indica que la vulnerabilidad ya había sido expuesta por Microsoft a los usuarios del programa desde febrero de 2021, incluyendo el Perú.

Antes de la filtración de la información robada, la DINI (Dirección Nacional de Inteligencia del Perú) reportó la amenaza cibernética en la "Alerta Integrada de Seguridad Digital N. 260-2022-CSN"[31], informando a los responsables de la Seguridad Digital sobre riesgos que podrían llegar a afectar la continuidad de los servicios informáticos. De esta manera, brindó recomendaciones como intensificar las medidas y actividades de ciberseguridad para prevenir incidentes, mantener un monitoreo activo con herramientas como WAF, FIREWALL, IPS, IDS, y actualizar las firmas de detección de amenazas; asimismo, monitorear constantemente las nuevas vulnerabilidades y aplicar los parches y actualizaciones de seguridad proporcionados por los proveedores. Dentro de esta Alerta, la DINI también aseguró que la vulnerabilidad y los parches para ProxyShell era conocida desde el 2021, por lo que se encontraba trabajando en la recopilación de información para detectar estos

[28] Esta vulnerabilidad en Microsoft Exchange permite a un atacante ejecutar código desde una ubicación remota, lo que facilita el control total sobre el sistema afectado

[29] En esta vulnerabilidad, hay un problema con la validación del token de acceso antes de ejecutar PowerShell. Esto significa que un atacante puede aprovechar esta falla para obtener acceso como usuario NT AUTHORITY\SYSTEM, que tiene privilegios de administrador en el sistema afectado.

[30] En esta vulnerabilidad hay un problema en el manejo de la exportación del buzón en Microsoft Exchange por la falta de validación adecuada de los datos ingresados por el usuario y en la carga de archivos.

[31] Análisis técnico periódico hecho por el CCFFAA, el Ejército del Perú, La Marina de Guerra del Perú, la Fuerza Aérea, la DINI, la PNP, la Asociación de Bancos del Perú y el CNSD de la Secretaría Digital

ataques y mitigar sus efectos, que responden a la exfiltración de datos, inoperatividad del servicio y pérdida de datos, lo que afecta la imagen institucional y la integridad, confidencialidad y disponibilidad de los activos digitales (CNSD, 2022).

La Alerta de Seguridad proporcionada por la DINI no evitó que en octubre del 2022 la información fuera filtrada. De esta manera, existió un intercambio de información y conversaciones con Chile y México (países que también fueron víctimas de Guacamaya), y Costa Rica (país que había sido afectado y paralizado por el grupo hacker Conti), con el objetivo de analizar las soluciones disponibles en el mercado más efectivas para eliminar la amenaza e identificar las vulnerabilidades que afectaban cada sistema, además de discutir medidas para mitigar el impacto del ataque, fortalecer la infraestructura cibernética y evitar futuros incidentes relacionados con Guacamaya (Oficial Freitas, O., comunicación personal, 06 de mayo del 2024).

Además, se hizo uso de la Malware Information Sharing Platform (MISP). Esta es una plataforma de inteligencia diseñada para compartir, almacenar y correlacionar amenazas informáticas actuales para mejorar las contramedidas contra ataques y establecer acciones preventivas y de detección (MISP Project, s.f.). En la región, el uso de las MISP se encuentra conectada y fomentada por la OEA, por lo que se recopila información sobre ataques detectados dentro de los países conectados a la plataforma, la cual luego se envía a Microsoft Windows u otros fabricantes de software para que desarrollen parches de seguridad (Comandante Ojeda, D., comunicación personal, 06 de mayo del 2024). El Perú es parte de esta plataforma desde el 2020 y se encuentra conectada a través de Secretaria General del Gobierno Digital, por lo que fue de ayuda para la identificación del grupo y cómo había estado trabajando en demás países para el robo de su información (Oficial Freitas, O., comunicación personal, 06 de mayo del 2024).

De manera que se recopila información sobre ataques detectados dentro de los países conectados a la plataforma, la cual luego se envía a Microsoft Windows u otros fabricantes de software para que desarrollen parches de seguridad. Estos parches son luego compartidos en la plataforma para su implementación. Finalmente, la red 24/7 también fue parte del proceso de identificación de Guacamaya. Esta es una red operativa continua y sin interrupciones con personal siempre disponible para la detección de anomalías.

Entonces, se puede decir que el tiempo de detección de la amenaza y la vulnerabilidad de Microsoft fue temprana pero el tiempo de respuesta para enfrentar

la amenaza evitando que se convierta en un ciberataque fue insuficiente. La falta de aplicación de parches y medidas de seguridad adecuadas permitió que las vulnerabilidades fueran explotadas, resultando en filtraciones de información en 2022. Cabe resaltar que esta falta de aplicación de actualizaciones y parches no solo fue por parte del Perú, el informe presentado por la multinacional rusa de ciberseguridad Kaspersky (2022) demuestra que esta acción también se repitió en países como Chile y México.

3.3.2. Número de equipos de respuesta activados ante el ataque

Respecto a las acciones frente al hackeo al sistema de defensa nacional, Gómez de la Torre enfatizó la necesidad de "determinar la profundidad de la penetración efectuada por estos hackers" (RPP, 2023). Señaló que se había previsto convocar una reunión del Consejo de Seguridad y Defensa Nacional con todos los actores relevantes de defensa, interior y relaciones internacionales para evaluar detalladamente el alcance de los hechos. Asimismo, mencionó que podría haberse requerido una supervisión conjunta de las comisiones parlamentarias de Defensa Nacional, Orden Interno e Inteligencia, en sesiones reservadas, con el fin de investigar la magnitud de la intrusión y definir medidas correctivas que evitaran futuras filtraciones.

En ese sentido, como primera medida, se aisló el software y equipos afectados para realizar un análisis forense. Esto implicó investigar el hardware, aislarlo y analizarlo en busca de vulnerabilidades, así como identificar posibles vectores de ataque. La recopilación de pruebas digitales implicó trasladar dispositivos que podrían contener evidencia a un entorno controlado, como un laboratorio, para su adquisición y análisis. De esta manera, fue analizado en dos niveles: hardware y software especializado. El análisis a nivel de hardware se realizó con dispositivos especializados que aseguró la extracción segura de datos digitales. Por otro lado, el análisis a nivel de software implicó el uso de sistemas informáticos operados por personal pericial, empleando herramientas especializadas para garantizar la precisión y fiabilidad en la extracción y análisis de datos digitales. Estos procesos fueron fundamentales para asegurar la integridad de la evidencia digital en cualquier procedimientos legal e investigativos (Ministerio Público, 2020).

Al respecto, ese mismo mes, el ministro del interior de ese entonces, Daniel Barragán, comentó que la investigación forense (La República, 2022) revelaba que la información filtrada no era sensible, y que los correos electrónicos revelados no tenían ningún valor para el Estado Peruano. Asimismo, en una entrevista para RPP, el ex director de la Escuela Nacional de Inteligencia de la DINI, Andrés Gomez de la Torre, mencionó que el tenor de los documentos filtrados no era preocupante (RPP, 2022). Asimismo, el equipo responsable de la tarea aplicó el parche y las actualizaciones correspondientes para el malware identificado, asegurando de esta manera que todos los sistemas y dispositivos afectados estuvieran protegidos contra posibles vulnerabilidades adicionales (Oficial Freitas, O., comunicación personal, 19 de junio del 2024).

En este contexto, los equipos de respuesta frente al malware pueden ser clasificados en dos grupos distintos. El primero estuvo compuesto exclusivamente por equipos dedicados a la investigación de los efectos en el software y hardware afectados. Este grupo se enfocó en analizar y comprender los impactos del malware en los sistemas tecnológicos. Por otro lado, el segundo grupo estuvo formado por equipos especializados en la corrección de las vulnerabilidades expuestas. Estos equipos trabajaron activamente para implementar soluciones y medidas correctivas destinadas a mitigar y resolver las vulnerabilidades detectadas.

3.3.3. Mejoras implementadas en sistemas de monitoreo y alerta

Una vez restablecidos los sistemas y operadores, se llevaron a cabo medidas correctivas para evitar que otro ciberataque de este tipo pueda volver a suceder. De esta manera, para el fortalecimiento de la Seguridad Digital del Comando Conjunto de las Fuerzas Armadas, se compraron nuevos ordenadores, se actualizaron los componentes para proporcionar una seguridad perimetral al entorno digital de la organización, y se instaló un mayor monitoreo en la Red 24/7. Como resultado, el Comando Conjunto ahora cuenta con una ciberseguridad mejorada para su propia red (Oficial Freitas, O., comunicación personal, 19 de junio del 2024).

Asimismo, según lo comentado por los entrevistados (6 de mayo del 2024), el ataque demostró su eficacia al generar una reacción inmediata y natural frente al golpe recibido. En esta ocasión, la respuesta no se centró en la búsqueda y aprehensión de culpables, sino que se enfocó en reforzar la seguridad digital del Comando Conjunto,

lo que puso de manifiesto que el ataque representó una oportunidad para fortalecer las defensas y mejorar la seguridad en general.

En este sentido, la respuesta del Perú se caracterizó principalmente por ser defensiva en lugar de ofensiva. Se enfocó en proteger activamente los sistemas y responder a los incidentes para minimizar el impacto, en lugar de realizar acciones más proactivas dirigidas a los adversarios para prevenir futuros ataques y disuadir amenazas.

Capítulo IV: Análisis de la información

Este capítulo analiza la información recopilada en el capítulo anterior. Se aborda la relación entre la participación del Perú en instituciones internacionales de ciberseguridad y ciberdefensa y los mecanismos de cooperación que estas ofrecen; para luego examinar cómo dicha participación y los mecanismos se vinculan con la respuesta que el país implementó frente al ataque del Grupo Guacamaya, evaluando tanto sus fortalezas como sus limitaciones.

La falta de participación de Perú en algunas de las principales instituciones de ciberseguridad y ciberdefensa, como ENISA, CSE, NSA, CARICOM IMPACS y Africa CERT, puede deberse a diversos factores como el geográfico, ya que estas instituciones se centran en regiones específicas, como Europa, Norteamérica, el Caribe o África, y Perú no forma parte de dichas áreas de influencia; el técnico, porque el país podría enfrentar limitaciones en infraestructura tecnológica o en recursos humanos especializados que dificulten su integración; y el estratégico, porque podría responder a una decisión de priorizar relaciones más específicas o relevantes para sus necesidades y capacidades nacionales.

En este sentido, Perú puede haber optado por involucrarse de manera más selectiva con instituciones cuya colaboración ofrezca mayores beneficios estratégicos, técnicos o de capacitación, en lugar de expandir su participación a una mayor cantidad de organismos sin un impacto directo en el desarrollo de sus habilidades en ciberseguridad y ciberdefensa. Un ejemplo de este comportamiento es el esfuerzo de Perú por mantener contacto con instituciones como la OTAN, la cual, a pesar de estar centrada principalmente en Europa y encontrarse geográficamente alejada, representa un referente global en ciberseguridad y ciberdefensa. Como lo indica el Oficial Freitas (comunicación personal, 06 de mayo de 2024), la clave para el Perú radica en adoptar las mejores prácticas internacionales en ciberseguridad y fortalecerlas mediante alianzas estratégicas con países líderes en la materia. Esta aproximación, enfocada quizá en la calidad sobre la cantidad, busca optimizar los recursos disponibles, asegurando que las colaboraciones sean más efectivas y contribuyan a la construcción de una infraestructura de ciberdefensa más sólida y adaptada a las necesidades del país.

No obstante, esto no significa que Perú no pueda colaborar o buscar futuras oportunidades de cooperación con estas instituciones. De hecho, representan

espacios estratégicos a explorar a medida que el país fortalece su posición en el ámbito internacional de la ciberseguridad y ciberdefensa. La participación en estas organizaciones, aunque limitada en la actualidad, podría abrir puertas para colaborar en proyectos específicos que contribuyan al desarrollo de una seguridad digital más sólida.

Respecto a las instituciones en las que el Perú forma parte, este es miembro formal de cinco de estas, lo que implica su aceptación de ciertas normas y estándares en materia de ciberseguridad y ciberdefensa, así como la oportunidad de participar en programas de cooperación y capacitación; y colabora de manera bilateral, sin un compromiso formal de membresía, con otras dos instituciones. En este punto es necesario resaltar que a pesar de que las instituciones internacionales mencionadas en el capítulo III abordan de manera general el campo de la ciberseguridad y la ciberdefensa, cada una se enfoca en aspectos específicos y, por lo tanto, establece vínculos con distintos sectores del gobierno. Por ejemplo, la Policía Nacional del Perú (PNP) tiene una mayor relación con INTERPOL, mientras que la Unión Internacional de Telecomunicaciones (UIT) trabaja estrechamente con la Secretaría General del Gobierno Digital. De esta forma se pasará a analizar solo las que se encuentran directamente relacionadas al caso de estudio.

Asimismo, otro punto a resaltar es que las instituciones no sustituyen la labor de los Estados; más bien, facilitan la cooperación internacional mediante reglas y normas que influyen en el comportamiento y la toma de decisiones dentro del sistema internacional (Prado, 2017, p. 373). En otras palabras, las instituciones actúan como medios que reducen la incertidumbre, promueven la transparencia, y establecen un marco común para coordinar acciones y resolver problemas colectivos, fortaleciendo así la gobernanza en ciberseguridad y ciberdefensa. De esta forma, las instituciones internacionales juegan un papel al conectar a los Estados con empresas privadas y otras entidades especializadas en el campo, que mediante sus programas ofrecen enfoques diversos y reúnen a una variedad de expertos.

Este entorno de colaboración no solo facilita el intercambio de conocimientos y el desarrollo de tecnologías avanzadas, sino que también fomenta métodos de interconexión a través de plataformas diseñadas para explorar el ciberespacio, monitorear foros de dark web o deep web, y compartir incidentes de seguridad experimentados. Estas acciones permiten detectar amenazas emergentes y divulgarlas a la comunidad internacional, promoviendo una vigilancia más efectiva y

fortaleciendo la cooperación con proveedores de servicios (Oficial Freitas, O., comunicación personal, 06 de mayo del 2024).

La OEA ha sido una de las instituciones más recurrentes en el apoyo a Perú en el ámbito de la ciberseguridad, desempeñando un papel en el fortalecimiento de la infraestructura digital del país. Entre los programas más destacados en los que Perú ha participado se encuentran el Programa de Ciberdefensa de la Junta Interamericana de Defensa (JID) y el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE), los cuales han proporcionado a los funcionarios peruanos la oportunidad de fortalecer sus habilidades técnicas y operativas frente a las amenazas cibernéticas. Asimismo, le ha brindado asistencia para la redacción del documento sobre la Estrategia Nacional de Ciberseguridad.

Por otro lado el Convenio de Budapest también ha sido una institución presente en el desarrollo de una seguridad digital en el Perú. Su importancia se refleja en su contribución al fortalecimiento de la cooperación internacional en la lucha contra la ciberdelincuencia. A través de mecanismos como la Red 24/7, el convenio facilita la rápida remisión de solicitudes de asistencia mutua entre los países suscriptores, incluidos Estados Unidos, España, Japón y varios países latinoamericanos. Además, este instrumento aborda cuestiones importantes como la extradición, una herramienta en la persecución de ciberdelincuentes internacionales. A pesar de que el Convenio fue promulgado en 2001 y Perú recién se adhirió formalmente el 2019, este ha cumplido con los estándares solicitados, por lo que su implementación ha permitido al país avanzar en la modernización de su marco legal y en la mejora de su infraestructura de ciberseguridad.

En este contexto, es fundamental diferenciar entre las recomendaciones y las obligaciones que surgen del compromiso formal con las instituciones internacionales. Las recomendaciones, al no tener carácter vinculante, no implican una obligación legal para el Estado, aunque sí pueden influir en la toma de decisiones o en la adopción de buenas prácticas. A pesar de que las recomendaciones son herramientas importantes para guiar la mejora en la ciberseguridad y ciberdefensa, su implementación queda a la discreción del Estado, sin que exista una obligación formal de seguirlas. Por otro lado, las obligaciones derivadas de un compromiso formal, como la adhesión a tratados o convenios internacionales, requieren que el Estado cumpla con medidas específicas que suelen estar claramente definidas en los acuerdos suscritos. Un claro ejemplo de esto es la incorporación de modificaciones en la legislación nacional, como

las que se dieron en la Ley N° 30096, particularmente en el artículo N° 230 del Código Procesal Penal, tras el ingreso de Perú al Convenio de Budapest incorporando medidas que antes no estaban contempladas, como la clonación de datos. Esto demuestra cómo un compromiso formal con una institución internacional puede traducirse en obligaciones que afectan directamente la legislación interna del país, adaptándola a estándares y marcos legales internacionales en ciberseguridad y ciberdelitos (Guerrero, 2018, p.08-09).

Otra observación acerca de la participación en instituciones internacionales es que la mayor parte de los mecanismos de cooperación proporcionados por estas se centran principalmente en la capacitación y asistencia técnica, ya que estos programas están diseñados para fortalecer las habilidades operativas y estratégicas del personal encargado de la ciberseguridad y ciberdefensa, a través de entrenamientos especializados, talleres y ejercicios conjuntos. Por lo tanto, se detectó que el financiamiento no es un componente tan prevalente en los mecanismos de cooperación. Esta tendencia refleja un enfoque orientado a la formación y a la colaboración técnica, más que a la inversión económica directa. Además, el financiamiento necesario para el desarrollo de infraestructuras y la implementación de proyectos específicos de ciberseguridad debe ser asumido principalmente por el propio Estado, que es el responsable de garantizar los recursos y la inversión en este ámbito para fortalecer la infraestructura digital y proteger sus sistemas ante las crecientes amenazas cibernéticas.

Finalmente, se encontró que los mecanismos de cooperación del Perú en ciberseguridad se obtienen tanto a través de una adhesión formal a instituciones internacionales como mediante colaboraciones bilaterales o externas, siendo estas últimas más limitadas. Es importante reconocer esta distinción, ya que estos mecanismos no se restringen únicamente a la adhesión formal, sino que también pueden ser alcanzados mediante otros enfoques más flexibles, como las colaboraciones bilaterales. Este tipo de interacción permite a los países compartir información, experiencias y buenas prácticas sin la necesidad de suscribir tratados formales ni estar sujetos a una membresía institucional rígida. De hecho, las redes de trabajo ad hoc, los foros de diálogo y las alianzas estratégicas ofrecen un espacio valioso para la cooperación, adaptándose a necesidades específicas y generando resultados concretos sin los trámites y restricciones de un marco institucional más formal.

Cabe resaltar que no se trata de decir que uno de estos enfoques sea superior al otro, sino de reconocer que ambos se complementan en el ámbito de la ciberseguridad. En un entorno tan incierto y complejo como el ciberespacio, lo que realmente importa es la capacidad de adaptación y la flexibilidad estratégica. La adhesión formal a instituciones internacionales y las colaboraciones bilaterales no deben considerarse opciones excluyentes, sino herramientas que, al combinarse, pueden generar una respuesta más sólida y flexible ante las amenazas cibernéticas. Cada enfoque tiene sus ventajas, y su integración estratégica permite optimizar los esfuerzos de cooperación y mejorar la resiliencia digital del país. La clave está en aprovechar de manera efectiva ambos mecanismos según las circunstancias y los objetivos específicos, para enfrentar de forma más eficaz los desafíos que presenta la seguridad en el ciberespacio.

En el caso específico del ciberataque de Guacamaya en 2022, se identificaron mecanismos de cooperación que fueron tanto formales, a través de la adhesión de Perú a instituciones internacionales como la Organización de Estados Americanos (OEA) y el Convenio de Budapest, como mediante la colaboración bilateral con países vecinos, sin involucrar directamente a otras instituciones internacionales. La participación de Perú en estas instituciones fue resaltante, ya que le permitió acceder a herramientas como la Malware Information Sharing Platform (MISP) y la Red 24/7, que jugaron un papel importante en la coordinación de la respuesta ante el ataque. Estas plataformas facilitaron el intercambio de información sobre amenazas y vulnerabilidades, permitiendo a Perú mejorar sus habilidades de detección y mitigación frente a los ciberataques. Además, la participación en estos instituciones no solo permitió el acceso a herramientas tecnológicas, sino también el fortalecimiento de sus habilidades tecnológicas mediante las capacitaciones realizadas. Los ejercicios conjuntos y talleres proporcionados ofrecieron a los equipos de ciberseguridad peruanos una formación práctica, enfocada en situaciones reales de ciberdefensa.

Por otro lado, la colaboración bilateral con países vecinos como Chile, México y Costa Rica jugó un rol complementario.Estos países, que también fueron afectados por el ataque de Guacamaya, compartieron información clave sobre las tácticas utilizadas por los atacantes, lo que contribuyó a una mejor comprensión de las vulnerabilidades explotadas. Además, el análisis conjunto de los datos permitió desarrollar soluciones coordinadas para contrarrestar el ataque.

Ahora bien, la respuesta hacia Guacamaya puede analizarse desde dos perspectivas: la primera centrada en la gestión de la vulnerabilidad explotada y la segunda focalizada en la falta de acción contra la amenaza que representaba el grupo en sí. Dentro de la primera perspectiva destaca el hecho de que se pudo eliminar la vulnerabilidad del software, identificar al grupo y aplicar el parche para evitar futuros ataques en el mismo servidor, por lo que el país demostró una respuesta adecuada, implementando medidas de ciberseguridad y actualizando sus protocolos para incidentes con ayuda de los mecanismos de cooperación proporcionados por las instituciones internacionales y el dialogo bilateral. No obstante, dentro de la segunda perspectiva se enfatiza una respuesta limitada en cuanto a la neutralización de la amenaza que representaba el grupo en sí. En este sentido, no se tomaron acciones contundentes para mitigar o desarticular a Guacamaya, ya que no se promovieron solicitudes de extradición ni se inició un proceso judicial para capturar a los responsables, permitiendo que el grupo mantuviera su operatividad en el ciberespacio.

Cabe resaltar que este patrón de inacción no fue exclusivo de Perú, sino que se replicó en otros países de la región que también fueron víctimas del ataque y que no implementaron medidas para detener al grupo. A pesar de que Guacamaya ha reducido su actividad, la falta de acciones concretas para contenerlo deja abierta la posibilidad de que resurjan operaciones similares en el futuro, lo que representa un riesgo para la seguridad regional. Si bien la información filtrada en el caso peruano era mayormente administrativa y no confidencial, la ausencia de medidas efectivas contra estos actores en la dark web podría alentar a otros grupos maliciosos a continuar explotando el ciberespacio, incrementando la vulnerabilidad de los países de la región.

De esta manera, la presente investigación califica la respuesta del Perú según la segunda perspectiva, ya que la estrategia adoptada estuvo basada en una defensa netamente pasiva, lo cual no cumple con lo dispuesto en el Artículo 5 del Capítulo III de la Ley de Ciberdefensa, que establece medidas tanto activas como pasivas para enfrentar ciberataques. En este contexto, aunque se implementaron medidas como la supervisión e identificación de amenazas, se omitieron tareas esenciales de mantenimiento y actualización de los sistemas informáticos. Asimismo, si bien se realizaron análisis de vulnerabilidades, detección y evaluación del ataque, no se tomaron acciones decisivas para degradar o neutralizar las capacidades operativas de Guacamaya, lo que permitió que el grupo continuara operando en el ciberespacio

sin restricciones, lo que expuso al país a riesgos adicionales. En consecuencia, se demuestra que la respuesta no cumplió con lo establecido por la Ley de Ciberdefensa Nacional y fue, por lo tanto, incompleta.

Esto se puede deber a diversas razones, entre ellas la falta de una coordinación más eficaz entre las distintas entidades encargadas de la ciberseguridad en Perú, la insuficiencia de recursos técnicos y humanos para implementar medidas activas de defensa, así como la dependencia de herramientas internacionales sin contar con la infraestructura local adecuada para una respuesta más contundente. Asimismo, el que otros países previamente afectados por Guacamaya tampoco hayan tomado acción para degradar su presencia en el ciberespacio pone de manifiesto otras razones como la falta de una estrategia regional unificada en ciberdefensa, lo que dificulta la implementación de acciones coordinadas frente a amenazas cibernéticas transnacionales. Además, podría reflejar la limitada capacidad de estos países para enfrentar ataques de esta magnitud debido a la falta de recursos o de infraestructura adecuada, lo que limita su capacidad para contrarrestar de manera efectiva a grupos como Guacamaya. Este patrón de inacción también podría estar relacionado con la falta de voluntad política para enfrentar de manera decidida a los actores responsables.

En este sentido, se puede afirmar que en el caso del Perú, las instituciones con mayor presencia durante la respuesta al ataque de Guacamaya fueron la OEA y el Convenio de Budapest, que proporcionaron herramientas específicas como la MISP y la Red 24/7. Estas plataformas facilitaron el intercambio de información vital sobre amenazas, permitiendo una respuesta más coordinada y efectiva frente a la naturaleza del ciberataque. No obstante, es importante destacar que el enfoque adoptado por estas instituciones se centró principalmente en la defensa reactiva, es decir, en contener los efectos inmediatos del ataque, más que en la implementación de medidas ofensivas o proactivas para desarticular la amenaza en su origen.

Este enfoque evidenció una limitación en la estrategia general de ciberseguridad del Perú. Aunque las herramientas y plataformas proporcionadas fueron valiosas para mitigar el daño causado por Guacamaya, no se adoptaron medidas destinadas a neutralizar al grupo atacante o a evitar que continuara operando con impunidad. Esto expone una vulnerabilidad crítica en la respuesta peruana, ya que no se contemplaron estrategias para disminuir las capacidades operativas de los actores maliciosos, lo que permitió que continuaran sus actividades en el ciberespacio.

Además, la falta de una respuesta más contundente resalta una deficiencia en los recursos internos del país, tanto a nivel técnico como humano, para enfrentar amenazas de esta magnitud de manera más agresiva y efectiva.

Otro aspecto relevante es la ausencia de una política regional coordinada que permita enfrentar de manera integral y proactiva los riesgos derivados de ataques cibernéticos transnacionales como el de Guacamaya. Si bien se han logrado avances en la cooperación regional, especialmente en el intercambio de información y buenas prácticas, no existe una estrategia unificada que fomente la implementación de acciones conjuntas para neutralizar a grupos cibercriminales. En este sentido, la falta de voluntad política, sumada a la limitada capacidad técnica de los países involucrados, ha permitido que actores como Guacamaya sigan operando sin restricciones, lo que incrementa la vulnerabilidad de los países de la región ante futuros ataques.

Conclusiones

El presente trabajo ha examinado la participación del Perú en instituciones internacionales de ciberdefensa y ciberseguridad, así como los mecanismos de cooperación promovidos por estas, utilizando como eje de estudio el ciberataque del grupo Guacamaya en 2022. Este incidente no solo evidenció las vulnerabilidades del país ante amenazas cibernéticas, sino que también destacó la necesidad de evaluar su involucramiento y respuesta en un contexto internacional en constante evolución. A lo largo de la investigación, se han identificado tanto logros como áreas que requieren mayor atención y mejora.

Con base en los hallazgos obtenidos, se ha determinado que la hipótesis de este estudio se corrobora parcialmente. Si bien la participación del Perú en estas instituciones facilitó el acceso a recursos, información y apoyo técnico, la respuesta al ataque del grupo Guacamaya fue parcial e incompleta. Esto indica que, aunque estos mecanismos de cooperación contribuyeron en cierta medida, no fueron suficientes para estructurar una reacción plenamente organizada y efectiva. Sin embargo, es necesario cualificar esta cuestión debido a que parte de las deficiencias en cuanto a respuesta se debieron a una concepción interna de cuál debía ser una respuesta adecuada, lo que no incluía la persecución de los responsables como forma de desarticulación de la amenaza y disuasión de futuros ataques. Por ello, es fundamental seguir reforzando la integración del país en estas instituciones internacionales y la cooperación bilateral. Asimismo, es necesario revisar cómo se define internamente una respuesta adecuada a estos ataques y mejorar la coordinación y las estrategias nacionales, ya que la efectividad frente a las amenazas cibernéticas depende de factores tanto internos como internacionales.

Una de las principales reflexiones que se derivan de este estudio es el desafío que estos grupos plantean al momento de determinar su naturaleza, ya que operan en un área gris entre el activismo digital y el cibercrimen. En este sentido, sus acciones pueden ser vistas tanto como un acto de protesta legítima, motivado por causas políticas, sociales o en defensa de una minoría, como una forma de cibercrimen que pone en riesgo la seguridad de personas e instituciones. Esto se debe a que a menudo implican la vulneración de sistemas informáticos y la exposición de información sensible, la cual puede ser aprovechada de manera malintencionada por otros actores.

El caso del grupo Guacamaya ilustra esta problemática. Por un lado, sus objetivos declarados, centrados en la defensa de los derechos de las minorías y la protección del medio ambiente, reflejan un esfuerzo por exponer actividades que consideran injustas o corruptas. Sin embargo, los métodos empleados, como la penetración no autorizada de sistemas informáticos y la difusión de información, generan un dilema ético y legal. En tal sentido, la percepción de sus acciones varía: mientras algunos los interpretan como un esfuerzo por la transparencia, otros los perciben como una forma de cibercrimen que vulnera la privacidad y la seguridad de las personas e instituciones afectadas.

En el caso del Ministerio de Defensa, la evaluación de la amenaza planteada por Guacamaya se centra principalmente en las acciones concretas realizadas, más que en las intenciones manifestadas. La utilización de exploits como el Proxy Shell y el despliegue de malware para acceder a información confidencial no autorizada demuestra un enfoque técnico similar al de un hacker o cracker, lo que refuerza su categorización como una amenaza cibernética desde el punto de vista de la defensa nacional. Sin embargo, desde la perspectiva de otros actores, Guacamaya podría ser visto también como un agente de cambio que desafía estructuras de poder establecidas al divulgar información que denuncia abusos de poder o actividades sospechosas de seguimiento no consentido. En este sentido, la narrativa adoptada por ciertos medios, como La Encerrona, se ha enfocado más en el contenido de las filtraciones que en el hecho de que el Ministerio de Defensa fue víctima de un ciberataque, lo que refleja una interpretación alternativa de los hechos.

Este dilema entre la protección de la seguridad nacional y el derecho del público a conocer la verdad sobre las acciones de sus líderes resalta las complejidades que plantea el entendimiento del concepto de seguridad en un entorno digital. Por lo tanto, la percepción de un grupo hacktivista como Guacamaya depende, en última instancia, de la valoración de sus motivaciones y del contexto en el que se analicen sus acciones.

Luego de examinar la naturaleza del hacktivismo, una segunda conclusión aborda el rol de las instituciones internacionales en la protección del entorno digital de un país. En este sentido, el papel de las instituciones internacionales se basa en promover, mejorar y consolidar mecanismos de cooperación entre países, algo que resulta necesario en un entorno digital caracterizado por la ausencia de fronteras físicas y en constante evolución. Esta naturaleza ambigua lo convierte en un escenario

propenso a la aparición de actores no estatales, como hacktivistas, así como de amenazas cibernéticas que requieren enfoques integrales y colaborativos para su gestión. Es importante destacar que la colaboración y pertenencia a estas instituciones no garantizan una solución automática a los problemas de ciberseguridad; más bien, contribuyen a fortalecer las defensas del país. Para abordar estos desafíos, se hace importante que se complemente con medidas internas, como la asignación de presupuestos adecuados y el desarrollo de capacidades técnicas.

En el caso de estudio, se identificó tres tipos de relaciones que el Perú puede tener con estas instituciones: la primera es una participación formal, es decir, ser miembro y haberse adherido a instituciones importantes en materia de ciberseguridad y defensa como el Convenio de Budapest o las agencias de la OEA. La segunda es colaborar de manera bilateral o externa sin necesariamente ser miembro, como lo hace con la OTAN; y la tercera es no colaborar o no ser miembro de estas. Cabe resaltar que la falta de relación con otras instituciones no necesariamente representa una limitación, sino una oportunidad de cooperación que podría explorarse en el futuro.

Asimismo, se halló que estas instituciones internacionales tienden a desempeñar un rol predominantemente defensivo más que ofensivo, lo cual puede interpretarse de dos maneras. Por un lado, se enfoca en la preparación y la protección ante posibles amenazas; por otro lado, puede revelar una falta de estrategias más proactivas para enfrentar ciberataques o campañas de desinformación. Esta realidad subraya la necesidad de prestar mayor atención a la efectividad de las respuestas nacionales e internacionales, sugiriendo que la respuesta del Perú al ataque del grupo Guacamaya, aunque existió, fue parcial e incompleta.

La tercera conclusión se enfoca en la interrelación de la soberanía de los Estados con los marcos de cooperación en ciberseguridad. De esta forma, estos marcos permiten a los países establecer directrices que coordinan esfuerzos en la prevención y respuesta a ciberataques, así como en el intercambio de información y buenas prácticas Sin embargo, su efectividad depende en gran medida de la decisión soberana de cada Estado para implementar y respetar estas normativas, lo que puede generar cierto debate sobre hasta qué punto un país estaría dispuesto a sacrificar su autonomía en favor de una mayor cooperación en un ámbito tan importante como la seguridad que involucra el manejo de datos, la privacidad y la vigilancia. Entonces, cada Estado, como el Perú, evalúa de manera independiente cuáles de estas

recomendaciones aplica y en qué actividades, capacitaciones o talleres participará, de acuerdo con sus intereses y prioridades nacionales.

Mirando hacia adelante, y como cuarta conclusión, la participación de Perú en instituciones internacionales y la cooperación en ciberseguridad presentan tanto oportunidades como desafíos. En un contexto donde las ciberamenazas evolucionan rápidamente y no reconocen fronteras, resulta necesario que Perú continúe profundizando su integración en marcos internacionales de ciberseguridad. Esta participación no solo le permitirá acceder a nuevas herramientas, conocimientos y estándares internacionales, sino también fortalecer su habilidad para prevenir y responder incidentes de ciberseguridad.

No obstante, para maximizar los beneficios de esta cooperación, Perú debe consolidar su compromiso interno, fortaleciendo políticas y estructuras de ciberseguridad a nivel nacional. En definitiva, el futuro de la ciberseguridad en Perú dependerá de su habilidad para equilibrar la cooperación internacional con una estrategia nacional sólida y adaptada a su contexto, enfrentando los desafíos del ciberespacio con un enfoque integral y coordinado.

Este trabajo se ha centrado principalmente en la participación de Perú en instituciones internacionales de ciberseguridad y ciberdefensa, adoptando una perspectiva internacional. Sin embargo, a lo largo de la investigación han surgido diversas cuestiones que ameritan un análisis más detallado y propician nuevas líneas de investigación. En primer lugar, sería valioso realizar estudios que profundicen en el contexto nacional, especialmente en la capacidad interna de Perú para implementar las recomendaciones internacionales de manera efectiva y coherente con sus políticas nacionales. Esto implica explorar el nivel de adaptación y resistencia de las instituciones locales frente a estas directrices, así como su capacidad de integración con los actores internacionales.

En segundo lugar, se podría investigar también el papel del sector privado en el fortalecimiento de la ciberseguridad nacional y su vinculación con las iniciativas internacionales. Analizar la colaboración entre actores públicos y privados, así como los desafíos regulatorios y de coordinación, podría ofrecer una perspectiva más completa sobre la protección del ciberespacio peruano. Además, sería pertinente estudiar el impacto del contexto geopolítico en la toma de decisiones de Perú en materia de ciberseguridad. Evaluar cómo las tensiones globales o los alineamientos

regionales afectan la política peruana en términos de cooperación y compromisos en ciberdefensa, permitiría identificar tendencias y posibles estrategias.

Para finalizar, es importante destacar que el ámbito digital no es un tema que Perú, ni ningún país, debería desatender en el futuro cercano. La rápida evolución de las tecnologías y las nuevas formas de ciberamenazas exigen un enfoque estratégico y constante en ciberseguridad. Este trabajo representa solo un pequeño aporte dentro de un campo mucho más amplio que sigue en pleno desarrollo. La ciberseguridad no solo involucra a las instituciones, sino también a las políticas, la sociedad y el sector privado, lo que abre un sinnúmero de caminos para futuras investigaciones y mejoras. La relevancia del tema seguirá creciendo, y es esencial que Perú continúe avanzando y fortaleciendo su participación en este espacio para asegurar su resiliencia digital y mantener la seguridad colectiva en un mundo cada vez más interconectado.

Referencias bibliográficas

Abbasi, A. (2016). Outline of program Prism and its effects on cyber security of Pakistan. International Journal of Research in IT, Management and Engineering, 6(4), 1-12. https://www.indusedu.org/pdfs/IJRIME/IJRIME_762_73825.pdf

Abi-Habib, M. (2022, 6 de octubre). El hackeo del ejército mexicano expone secretos de la institución más poderosa del país. The New York Times. Nueva York, NY, Estados Unidos. https://www.nytimes.com/es/2022/10/06/espanol/mexico-sedena-guacamaya-hackeo.html

Agencia de Implementación de la Comunidad del Caribe para la Criminalidad y la Seguridad (CARICOM IMPACS). (s.f.). Projects. Recuperado de https://www.caricomimpacs.org/projects

Agencia de la Unión Europea para la Ciberseguridad (ENISA). (s.f.). Acerca de la ENISA - Agencia de la Unión Europea para la Ciberseguridad. Recuperado el 8 de junio de 2024, de https://www.enisa.europa.eu/about-enisa/about/es

Agencia de Seguridad Nacional y Servicio de Seguridad Central (NSA/CSS). (s.f.). About NSA/CSS. Recuperado de https://www.nsa.gov/

Agnew, J. (1994). The territorial trap: The geographical assumptions of international relations theory. Review of International Political Economy, 1(1), 53-80. https://doi.org/10.1080/09692299408434268

Aguilar, J. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estudios Internacionales, 53(198), 169-197. https://www.scielo.cl/pdf/rei/v53n198/0719-3769-rei-53-198-00169.pdf

Aid, M. (2014). The National Security Agency's shift to cyber espionage. CSCAP. https://www.jstor.org/stable/pdf/resrep22259.8.pdf

Álvarez, C. (2020). Las capacidades operacionales de la Fuerza Aérea del Perú en la seguridad multidimensional (2011-2019). Revista Fuerzas Armadas, 252, 52-63. Recuperado de https://esdegrevistas.edu.co/index.php/refa/article/view/525/765

Andrei, I. (2016). Hacktivism – Means and Motivations (Hacktivism – Mijloace Şi Motivaţii). En Proceedings of Scientific Conference "New Challenges Related to EU's Internal Security" (5th Ed.), Doctoral Schools from Alexandru Ioan Cuza Police Academy, Bucharest, Romania. Recuperado de https://ssrn.com/abstract=2790066

Asia Pacific Computer Emergency Response Team (APCERT). (s.f.). APCERT member and partner categories policy. https://www.apcert.org/documents/pdf/APCERT_Member_and_Partner_Categories_Policy.pdf

Asia Pacific Computer Emergency Response Team (APCERT). (2003). APCERT annual report 2003. https://www.apcert.org/documents/pdf/annualreport2003.pdf

Bacchi, N. L. (2023). Cooperación internacional en materia de ciberseguridad: Un análisis entre la República Argentina y la Organización de los Estados Americanos en el período 2012-2022 (Tesis de licenciatura, Universidad Nacional del Centro de la Provincia de Buenos Aires, Facultad de Ciencias Humanas). https://ridaa.unicen.edu.ar:8443/server/api/core/bitstreams/c8ce0b86-b796-47d2-9303-34fadacb2421/content

Baldi, S., Gelbstein, E., & Kurbalija, J. (2003). The activities of the uncivil society in cyberspace. Malta: DiploFoundation. Recuperado de https://baldi.diplomacy.edu/italy/isl/Hacktivism.pdf

Bansi, M. (2015). Between control and hacker activism: The political actions of Anonymous Brasil. História, Ciências, Saúde – Manguinhos, 22(3), 795-814. https://doi.org/10.1590/S0104-59702015000300009

Barbachán, I. (2009). Visión geográfica del ciberespacio. Revista Electrónica de Recursos en Internet sobre Geografía y Ciencias Sociales, 13(117). Recuperado de https://www.ub.edu/geocrit/aracne/aracne-117.htm

Baron, R., & Kenny, D. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. Journal of Personality and Social Psychology, 51(6), 1173-1182. https://www.researchgate.net/publication/281274059_The_moderator-mediator_variable_distinction_in_social_psychological_research_Conceptual_strategic_and_statistical_considerations

Bendiek, A. (2012). European cyber security policy (SWP Research Paper No. 2012/RP 02). Stiftung Wissenschaft und Politik. https://www.researchgate.net/publication/270761442_European_Cyber_Security_Policy

Boemcken, M., & Schetter, C. (2016). What is it? What does it do? (Think Piece No. 9, pp. 1-5). Bonn, Alemania: Friedrich-Ebert-Stiftung. https://library.fes.de/pdf-files/iez/12368.pdf

Bonifaz, R. (2017). La NSA según las revelaciones de Snowden (Tesis de licenciatura). Universidad de Buenos Aires. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0938_BonifazR.pdf

Borbúa, R., Herrera, L. R., & Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. Revista Latinoamericana de Estudios de Seguridad, 20, 31–45. https://doi.org/10.17141/urvio.20.2017.2571

Burton, J. (2015). NATO's cyber defence: Strategic challenges and institutional adaptation. Defence Studies, 15(4), 297–319. https://doi.org/10.1080/14702436.2015.1108108

Calduch, R. (1991). Relaciones internacionales. Ediciones de las Ciencias Sociales. Madrid, España. https://www.academia.edu/594426/Relaciones_internacionales

Calles, J. (2022). “Guacamaya Roja”, el grupo de hackers que filtra millones de documentos de una minera. Prensa Comunitaria. https://prensacomunitaria.org/2022/03/guacamaya-roja-el-grupo-de-hackers-que-filtra-millones-de-documentos-de-una-minera/

Candau, J. (2021). Ciberseguridad: Evolución y tendencias. Revista del IEEE, 49, 460-494. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=8175398

Cardinale, M. E. (2016). Debates en seguridad internacional: hacia una redefinición de la perspectiva predominante. Tensões Mundiais, 12(22), 49–78. https://doi.org/10.33956/tensoesmundiais.v12i22.389

Cardona, D. (2004). Hasta dónde llega la seguridad: una lectura crítica de Krause y Williams. Desafíos, 11(semestre II), 10-42.

Caro, M. J. (2011). Nuevo concepto de ciberdefensa de la OTAN. Documento informativo del IEEE (Nº 09/2011). Instituto Español de Estudios Estratégicos. https://dialnet.unirioja.es/descarga/articulo/7271583.pdf

Castillo, E. (2021). Análisis sobre la política sectorial de ciberdefensa: Una necesidad impostergable. Centro de Estudios Estratégicos del Ejército del Perú. https://ceeep.mil.pe/wp-content/uploads/2021/11/CEEEP-2021-Politica-Sectorial-de-Ciberdefensa-1.pdf

Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile (CEEAG). (2018). La ciberguerra: sus impactos y desafíos (Primera edición). https://www.ceeag.cl/wp-content/uploads/2020/06/LA-CIBERGUERRA-SUS-IMPACTOS-Y-DESAFIOS.pdf

Centro de Estudios Internacionales Gilberto Bosques. (2022). XIII Reunión de la Comisión de Seguridad Ciudadana y Administración de Justicia y VI Reunión de la Comisión Interparlamentaria de Asuntos Financieros y Presupuestario del Foro de Presidentes y Presidentas de Poderes Legislativos de Centroamérica y la Cuenca del Caribe (FOPREL), San José, Costa Rica, 7 y 8 de noviembre de 2022 (Serie: América, N° 56). Recuperado de https://centrogilbertobosques.senado.gob.mx/docs/LXV-1-serieeamerica_56.pdf

Centro Nacional de Seguridad Digital (CNSD). (2022). Alerta integrada de seguridad digital (N.º 272-2022-CNSD). Lima, Perú. https://cdn.www.gob.pe/uploads/document/file/3738549/Alerta%20integrada%20de%20seguridad%20digital%20N%C2%B0%20272-2022-CNSD.pdf.pdf

Chacha, M. (2019). Análisis de las metodologías ENISA y APCERT para la creación del Centro de Respuesta a Incidentes Informáticos (CSIRT). Caso práctico: Prototipo de un CSIRT en la Universidad Nacional de Chimborazo [Trabajo de titulación de grado, Universidad Nacional de Chimborazo]. Repositorio Digital UNACH. http://dspace.unach.edu.ec/bitstream/51000/6284/1/AN%C3%81LISIS%20DE%20LA

S%20METODOLOG%C3%8DAS%20ENISA%20Y%20APCERT%20PARA%20LA%20CREACI%C3%93N%20DEL%20CENTRO%20DE%20RESPUESTA.pdf

Choucri, N., Madnick, S., & Koepke, P. (2017). Institutions for cyber security: International responses and data sharing initiatives. Department of Political Science, Massachusetts Institute of Technology. https://dspace.mit.edu/bitstream/handle/1721.1/144062/Choucri%2c%20Madnick%2c%20Koepke%20%282017%29%20Institutions%20for%20cyber%20security.pdf?sequence=1&isAllowed=y

Ciberilatam. (2024). Ecosistema Latinoamericano de Ciberseguridad 2024. Ciberilatam, 1(001), 24-25. https://www.segurilatam.com/revistas/ciberilatam/001/

Ciper Chile. (2022, 22 de septiembre). Hackeo masivo al Estado Mayor Conjunto expuso miles de documentos de áreas sensibles de la defensa. Santiago, Chile. https://www.ciperchile.cl/2022/09/22/hackeo-masivo-al-estado-mayor-conjunto-expuso-miles-de-documentos-de-areas-sensibles-de-la-defensa/

CISObeat. (2019). Adhesión del Perú al Convenio de Budapest [Archivo de video]. YouTube. https://www.youtube.com/watch?v=LjFnduHrjnY

Coleman, G. (2013). Anonymous in context: The politics and power behind the mask. Centre for International Governance Innovation (CIGI), 3(8), 1-22. https://www.cigionline.org/sites/default/files/no3_8.pdf

Coleman, G. (2014). Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous. Verso.

Comando Conjunto de las Fuerzas Armadas. (2020). Comando Conjunto participa en entrega de Secretaría Pro Tempore del Foro Iberoamericano de Ciberdefensa [Nota de prensa]. Recuperado de https://www.gob.pe/institucion/ccffaa/noticias/501957-comando-conjunto-participa-en-entrega-de-secretaria-pro-tempore-del-foro-iberoamericano-de-ciberdefensa

Comando Conjunto de las Fuerzas Armadas. (2021). Comando Conjunto de las Fuerzas Armadas obtuvo tercer lugar en ejercicio del Foro Iberoamericano de Ciberdefensa [Nota de prensa]. Recuperado de https://www.gob.pe/institucion/ccffaa/noticias/549870-comando-conjunto-de-las-fuerzas-armadas-obtuvo-tercer-lugar-en-ejercicio-del-foro-iberoamericano-de-ciberdefensa

Comas, O. (2010). El caso WikiLeaks como piedra de toque de la democracia deliberativa de Jürgen Habermas. Dilemata, 8, 123–151. https://www.dilemata.net/revista/index.php/dilemata/article/view/121

Comisión para la Verdad y Acceso a la Justicia en el Caso Ayotzinapa. (s.f.). Página oficial de la Comisión para la Verdad y Acceso a la Justicia en el Caso Ayotzinapa. Ciudad de México, México. https://comisionayotzinapa.segob.gob.mx/

Congreso de la República del Perú. (2002). Resolución Legislativa N° 26362. Diario Oficial El Peruano. https://docs.peru.justia.com/federales/resoluciones-legislativas/26362-sep-28-1994.pdf

Congreso de la República. (2011). Ley de Protección de Datos Personales. Diario El Peruano. https://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf

Congreso de la República. (2013). Ley de Delitos Informáticos. Diario El Peruano. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

Consejo de Europa. (2001). Convenio sobre ciberdelincuencia. Estrasburgo, Francia: Consejo de Europa. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Consejo de Europa. (2003). Protocolo adicional al Convenio sobre Ciberdelincuencia, relativo a la criminalización de actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos. Estrasburgo, Francia: Consejo de Europa. https://rm.coe.int/168008160f

Consejo de Europa. (2022). Informe explicativo del Segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia sobre cooperación mejorada y divulgación de pruebas electrónicas. Estrasburgo, Francia: Consejo de Europa. https://rm.coe.int/1680a49c9d

Council of Europe. (2022). Taller 4 – Red 24/7 del Convenio de Budapest: Cooperación en situaciones de emergencia: el papel de los puntos de contacto 24/7. Recuperado de https://www.coe.int/es/web/americas-regional-forum-cybercrime/cooperation-in-emergency-situations-the-role-of-24/7-points-of-contact

Croasdell, D., & Palustre, A. (2019). Transnational cooperation in cybersecurity. En Proceedings of the Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2019.674

Cubeiro, E. (2023). Ciberespacio espacial: el talón de Aquiles de la seguridad y defensa. Cuadernos de Pensamiento Naval, 35, 53–68. Recuperado de https://armada.defensa.gob.es/archivo/mardigitalrevistas/boletinpensamiento/2023/2023cpn35.pdf

Defensoría del Pueblo. (2022). La ciberdelincuencia en el Perú: Estrategias y retos de Estado (Informe n.º 001-2023). Lima, Perú: Defensoría del Pueblo. https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Diario El Peruano. (2000). Ley que incorpora los delitos informáticos al Código Penal. Congreso de la República. https://cdn.www.gob.pe/uploads/document/file/356824/NORMA_1887_Ley_27309.pdf?v=1567090257

Diario El Peruano. (2018). Aprueban la definición de Seguridad Digital en el Ámbito Nacional. Decreto Supremo N° 050-2018-PCM. Fecha de publicación: 15/05/2018. https://busquedas.elperuano.pe/dispositivo/NL/1647865-1

Dobusch, L., & Schoeneborn, D. (2015). Fluidity, identity, and organizationality: The communicative constitution of Anonymous. Journal of Management Studies, 52(8), 1005-1035. https://doi.org/10.1111/joms.12139

Dogrul, M., Aslan, A., & Celik, E. (2011). Developing an international cooperation on cyber defense and deterrence against cyber terrorism. In 2011 3rd International Conference on Cyber Conflict (pp. 1-15). Tallinn, Estonia. https://ieeexplore.ieee.org/abstract/document/5954698

El Peruano. (2018). Aprueban la definición de Seguridad Digital en el Ámbito Nacional [Decreto Supremo N° 050-2018-PCM]. https://busquedas.elperuano.pe/dispositivo/NL/1647865-1

El Peruano. (2019). Reglamento de la Ley N° 30999, Ley de Ciberdefensa. Título Preliminar: Disposiciones Generales. El Peruano. Fecha de publicación: 11/12/2019. https://busquedas.elperuano.pe/dispositivo/NL/1748338-2

El Peruano. (2020). Decreto de urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento. El Peruano. Fecha de publicación: 12/03/2020. https://busquedas.elperuano.pe/dispositivo/NL/1844001-2

El Peruano. (2021). Normas legales. Recuperado de https://busquedas.elperuano.pe/api/media/http://172.20.0.101/file/4J8ymPl9KN_9KzdfaonmKg/*/2002580-1.pdf/PDF

Enlace Hacktivista. (s.f.). Poema Guacamaya. https://enlacehacktivista.org/poema_guacamaya.txt

Enlace Hacktivista. (s.f.). Fuerzas represivas. https://enlacehacktivista.org/comunicado_guacamaya4.txt

Establecimiento de Seguridad de las Comunicaciones (CSE). (s.f.). Cyber Security. Recuperado de https://www.cse-cst.gc.ca/en/mission/cyber-security

European Union. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, 15-69. Recuperado de https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC

Fojón, E., & Colom, G. (2014). La NSA en la era del ciberespionaje masivo. Política Exterior, 28(157), 34-39. https://www.jstor.org/stable/43594908

Foro Africano de Equipos de Respuesta a Incidentes Informáticos (AfricaCERT). (s.f.). About us. Recuperado de https://www.africacert.org/about-us/

Foro Africano de Equipos de Respuesta a Incidentes Informáticos (AfricaCERT). (2023). Five years review. Recuperado de https://www.africacert.org/wp-content/uploads/2023/02/1-fiveyearsreview.pdf

Ganuza, N. (2011). Situación de la ciberseguridad en el ámbito internacional y en la OTAN. Cuadernos de estrategia (pp. 167-214). Madrid: Ministerio de Defensa, Subdirección General de Publicaciones. https://dialnet.unirioja.es/descarga/articulo/3837337.pdf

García, V. (2019). ¿Cómo está avanzando la ciberseguridad en el Perú? Breve aproximación al marco normativo. AC Jurídica, 52(1), 176-179. https://www.uria.com/documentos/publicaciones/6687/documento/foro-latam14.pdf?id=8972&forceDownload=true

García-Estévez, N. (2018). Origen, evolución y estado actual del activismo digital y su compromiso social. Ciberactivismo, hacktivismo y slacktivismo. En II Congreso Internacional Move.net sobre Movimientos Sociales y TIC (pp. 139-156). Sevilla, España: Grupo Interdisciplinario de Estudios en Comunicación, Política y Cambio Social de la Universidad de Sevilla (COMPOLÍTICAS). Recuperado de https://idus.us.es/bitstream/handle/11441/70636/Pages%20from%20actas_ii-congreso-internacional-movenet_candon-mena-11.pdf?sequence=1&isAllowed=y

Gestión. (2023, 24 de agosto). Perú se suma a red internacional para prevenir ciberataques gubernamentales. Recuperado de https://gestion.pe/economia/oea-peru-se-suma-a-red-internacional-para-prevenir-ciberataques-gubernamentales-noticia/

Global Forum on Cyber Expertise (GFCE). (s.f.). Nuestro impacto. Recuperado de https://thegfce.org/about/our-impact/

Gómez, J. P. (2022). Modelo de ciberseguridad aplicable en el comercio marítimo en Colombia para contener amenazas del ciberespacio. Revista Ciberespacio, Tecnología e Innovación, 1(2), 1-15. Bogotá, D.C, Colombia. https://esdegrevistas.edu.co/index.php/rcit

GuacamayaLeaks. (2022). Twitter. https://twitter.com/GuacamayanLeaks

Guerrero, C., & Borgioli, M. (2018). De Budapest al Perú. En M. Díaz (Coord.), Grupo de trabajo sobre Ciberseguridad en América Latina. Derechos Digitales. Recuperado de https://www.derechosdigitales.org/wp-content/uploads/minuta_hiperderecho.pdf

Guiora, A. N. (2019). Ciberseguridad: un modelo de cooperación. En F. González (Ed.), ¿Hacia una nueva Ilustración? Una década trascendente (pp. 331-407). Fundación BBVA.

Iglesias, M. (2011). La evolución del concepto de seguridad (Documento n.º 5). Instituto Español de Estudios Estratégicos, Ministerio de Defensa de España.

Infobae. (2023, 7 de octubre). Guacamaya Leaks: ¿Qué hay en los correos filtrados que exponen al Ejército del Perú y Comando Conjunto? Buenos Aires, Argentina. https://www.infobae.com/america/peru/2022/10/07/guacamaya-leaks-peru-se-filtran-283-mil-correos-entre-ejercito-peruano-comando-conjunto/

Jiménez, C. (2022). El acercamiento del Perú a la Organización del Tratado del Atlántico Norte como socio global (Tesis de maestría). Academia Diplomática del Perú. http://repositorio.adp.edu.pe/bitstream/handle/ADP/210/2022%20Tesis%20Jimenez%20Romero%20Mazariegos%2c%20Carlos.pdf?sequence=3&isAllowed=y

Junta Interamericana de Defensa (JID). (s.f.). Historia. https://jid.org/historia/

Junta Interamericana de Defensa (JID). (2020). Guía de ciberdefensa: Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar. https://jid.org/wp-content/uploads/2022/01/Ciberdefensa10.pdf

Kahhat, F. (2019). Seguridad internacional: Una introducción crítica. Lima, Perú: Fondo Editorial PUCP.

Kaspersky. (2022). Las vulnerabilidades aprovechadas por el grupo Guacamaya continúan dejando víctimas en América Latina. https://latam.kaspersky.com/about/press-releases/las-vulnerabilidades-aprovechadas-por-el-grupo-guacamaya-continuan-dejando-victimas-en-america-latina-alerta-kaspersky?srsltid=AfmBOooCcPeD51XAFu_lWclKxZSQk-N020ebvKas0K1ax_YCYzJpTGf

Keohane, R. O. (1984). After hegemony: Cooperation and discord in the world political economy. Princeton, NJ: Princeton University Press.

Keohane, R. O. (1988). International institutions: Two approaches. International Studies Quarterly, 32(4), 379–396. https://doi.org/10.2307/2600589

Keohane, R., y Martin, L. L. (1995). The promise of institutional theory. International Security, 20(1), 39-51. https://doi.org/10.2307/2539214

Lallande, J. P. (2021). El liberalismo institucional. En Teorías de relaciones internacionales en el siglo XXI: Interpretaciones críticas desde México y América Latina. Recuperado de https://www.coursehero.com/es/file/plj7u2/Existen-organismos-internacionales-globales-Organizaci%C3%B3n-de-las-Nacio-nes/

La-Lista. (10 de octubre de 2022). Entrevista exclusiva: La vulnerabilidad de Sedena fue explotada en masa por muchos hackers: grupo de hacktivistas Guacamaya. La-Lista. https://la-lista.com/mexico/2022/10/10/hackers-guacamaya-entrevista-exclusiva-con-el-grupo-hacktivista

La República. (2022). Ministro de Defensa descartó que se haya filtrado “información sensible” sobre caso de ataque de hackers. https://larepublica.pe/politica/gobierno/2022/10/10/daniel-barragan-ministro-de-

defensa-descarto-que-se-haya-filtrado-informacion-sensible-sobre-caso-de-ataque-de-hackers-guacamaya-leaks

Lima Costa, A. D. (4 de abril de 2024). "Los conflictos que ocurren a miles de kilómetros pueden afectar a la ciberseguridad de Latinoamérica" [Entrevista]. Segurilatam. https://www.segurilatam.com/ciberilatam/foro-iberoamericano-de-ciberdefensa-los-conflictos-que-ocurren-a-miles-de-kilometros-pueden-afectar-a-la-ciberseguridad-de-latinoamerica_20240404.html#:~:text=El%20Foro%20Iberoamericano%20de%20Ciberdefensa,dos%20de%20sus%20elementos%20estrat%C3%A9gicos.

Magen, S. (2017). Cybersecurity and economic espionage: The case of Chinese investments in the Middle East. Cyber, Intelligence, and Security, 1(3), 3-124. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/INSS-Cyber,%20Intelligence,%20and%20Security,%20Volume%201,%20No.%203.pdf

Martínez, C. (2015). El uso de ciberataques como herramienta de relaciones internacionales por parte de actores estatales: Los casos de Estados Unidos y Rusia (Tesis de licenciatura). Universidad Pontificia Comillas, Madrid. https://repositorio.comillas.edu/rest/bitstreams/2873/retrieve

McGuinness, D. (5 de mayo de 2017). Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país. BBC Mundo. Recuperado de https://www.bbc.com/mundo/noticias-39800133

Menn, J. (2019). Cult of the dead cow: How the original hacking supergroup might just save us. New York, NY: PublicAffairs.

Microsoft. (2021). Descripción de la actualización de seguridad para Microsoft Exchange Server 2019, 2016 y 2013: 2 de marzo de 2021 (KB5000871). https://support.microsoft.com/es-es/topic/descripci%C3%B3n-de-la-actualizaci%C3%B3n-de-seguridad-para-microsoft-exchange-server-2019-2016-y-2013-2-de-marzo-de-2021-kb5000871-9800a6bb-0a21-4ee7-b9da-fa85b3e1d23b

Ministerio de Defensa (Mindef). (2006). Libro Blanco de la Defensa Nacional. Recuperado de https://cdn.www.gob.pe/uploads/document/file/397073/Libro_blanco.pdf

Ministerio de Defensa (Mindef). (2019). Resolución 0573-2019. Recuperado de https://cdn.www.gob.pe/uploads/document/file/313020/0573-2019.pdf?v=1557510159

Ministerio de Defensa (Mindef). (2021). Resolución Ministerial N.° 0600-2021-DE, 19 de octubre de 2021. Recuperado de https://www.gob.pe/institucion/mindef/normas-legales/2222970-0600-2021-de

Ministerio de Defensa (Mindef). (2022). Política nacional multisectorial de seguridad y defensa nacional al 2030: Resumen ejecutivo. Recuperado de

https://cdn.www.gob.pe/uploads/document/file/3350044/RESUMEN%20EJECUTIVO%20PNMSDN%20AL%202030.pdf.pdf?v=1656963441

Ministerio de Justicia y Derechos Humanos. (1991). Decreto Legislativo Nº 681: Dictan normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional cuanto la producida por procedimientos informáticos en computadoras. Sistema Peruano de Información Jurídica. https://cdn.www.gob.pe/uploads/document/file/1511737/D-Leg-681.pdf.pdf?v=1609609566

Ministerio Público. (2020). Guía de análisis forense. https://portal.mpfn.gob.pe/descargas/normas/d66588.pdf

Ministerio Público Fiscalía de la Nación. (2020). "Convenio sobre la Ciberdelincuencia" permite a jueces y fiscales realizar requerimientos de cooperación internacional [Nota Informativa]. https://www.gob.pe/institucion/mpfn/noticias/302628-convenio-sobre-la-ciberdelincuencia-permite-a-jueces-y-fiscales-realizar-requerimientos-de-cooperacion-internacional

MISP Project. (s.f.). MISP Project: The open source threat intelligence platform. https://www.misp-project.org/

Mogollón, F. (2017). Desafíos de la ciberseguridad y respuestas estatales: El caso del Estado ecuatoriano en el período 2008-2015 (Tesis de Licenciatura). Pontificia Universidad Católica del Ecuador, Quito. http://repositorio.puce.edu.ec/bitstream/handle/22000/14104/DESAF%C3%8DOS%20DE%20LA%20CIBERSEGURIDAD%20Y%20RESPUESTAS%20ESTATALES%20EL%20CASO%20DEL%20ESTADO%20ECUATORIANO%20EN%20EL%20PER%C3%8DODO.pdf?sequence=1&isAllowed=y

Moreno, D. (s.f.). Cybersecurity Program. Comité Interamericano contra el Terrorismo, Secretaría de Seguridad Multidimensional, Organización de los Estados Americanos. Recuperado de https://rm.coe.int/oea-cicte-programa-de-ciberseguridad-david-moreno-es/1680aab4e3

Naciones Unidas. (2013). Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional: Informe del Secretario General (A/68/156) [Informe]. https://documents.un.org/doc/undoc/gen/n13/397/38/pdf/n1339738.pdf

Naciones Unidas. (2021). La ciberseguridad en las organizaciones del sistema de las Naciones Unidas (JIU/REP/2021/3). [Informe]. Unidad de Inspección Conjunta.https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_spanish.pdf

Nebreda, I. (2013). El origen de Internet: El camino hacia la red de redes (Tesis de grado, IMAGEN & SONIDO, Universidad Politécnica de Madrid). DIATEL. Recuperado de https://oa.upm.es/22577/1/PFC_IVAN_NEBREDA_RODRIGO.pdf

Niño, C., & Ortega, A. (2018). Seguridad en las Relaciones Internacionales Contemporáneas: Una mirada para estudiantes de la disciplina (pp. 149-170). En Sánchez, F. & Liendo, N. Estudios y tendencias de la política y las relaciones internacionales. Bogotá: Universidad Sergio Arboleda. https://repository.usergioarboleda.edu.co/bitstream/handle/11232/1452/Seguridad%20%20Relaciones%20Internacionales%20Contempora%CC%81neas.pdf?sequence=1&isAllowed=y

Nye, J. (2012, abril 10). Cyber war and peace. Project Syndicate. https://www.project-syndicate.org/commentary/cyber-war-and-peace-2012-04?barrier=accesspaylog

Ochoa, A. (2021). Desafíos globales del cibercrimen: Caso Ecuador período 2014 – 2019 (Tesis de maestría). Universidad Andina Simón Bolívar, Sede Ecuador, Área de Estudios Sociales y Globales, Maestría en Relaciones Internacionales, Quito. https://repositorio.uasb.edu.ec/bitstream/10644/7919/1/T3432-MRI-Ochoa-Desafios.pdf

Oficina de la Lucha contra el Terrorismo (OLCT). (s/f). Ciberseguridad. Naciones Unidas. https://www.un.org/counterterrorism/es/cybersecurity

Organización de los Estados Americanos (OEA). (2002). Declaración de Bridgetown: Enfoque multidimensional de la seguridad hemisférica. https://www.oas.org/xxxiiga/espanol/documentos/docs_esp/agcgdoc15_02.htm

Organización de los Estados Americanos (OEA). (2003). Declaración sobre Seguridad en las Américas. https://www.oas.org/36ag/espanol/doc_referencia/DeclaracionMexico_Seguridad.pdf

Organización de los Estados Americanos (OEA). (2015). Mesa de Discusión para el Desarrollo de una Estrategia Nacional de Seguridad Cibernética. Boletín de Actividades y Noticias (pp. 1-7). Recuperado de https://www.oas.org/FPDB/NATOFF/DOCS/BOLETIN%20PERU%20abril%202015.pdf

Organización de los Estados Americanos (OEA). (2019). Conferencia de Ciberseguridad del Hemisferio Occidental. Washington, D.C., EE. UU. https://scm.oas.org/pdfs/2020/CP42175SINFORMEANUALJIDCORR1.pdf

Organización de los Estados Americanos (OEA) & Banco Interamericano de Desarrollo. (2016). Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? (Informe). Observatorio de la Ciberseguridad en América Latina y el Caribe, 1-193. https://publications.iadb.org/es/publications/spanish/viewer/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

Organización Internacional de Policía Criminal (Interpol). (s.f.-a). Centro de Innovación de INTERPOL. Recuperado de https://www.interpol.int/es/Como-trabajamos/Innovacion/Centro-de-Innovacion-de-INTERPOL

Organización Internacional de Policía Criminal (Interpol). (s.f.-b). INTERPOL Global Complex for Innovation opens its doors. Recuperado de https://www.interpol.int/

Organización Internacional de Policía Criminal (Interpol). (s.f.-c). Perú. Recuperado de https://www.interpol.int/es/Quienes-somos/Paises-miembros/Las-Americas/PERU

Organización del Tratado del Atlántico Norte (OTAN). (s.f.). Bienvenido a la OTAN. https://www.nato.int/nato-welcome/index_es.html

Organización del Tratado del Atlántico Norte (OTAN). (2023). Boletín de Integridad N°16. Recuperado de https://www.nato.int/nato_static_fl2014/assets/pdf/2023/2/pdf/230207-BI_newsletter_16_es.pdf

Ormachea, J. F. (2020). Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional. Revista de Ciencia e Investigación en Defensa-CAEN, 1(4), 36-48. https://www.recide.caen.edu.pe/index.php/recide/article/download/36/32/29

Orozco, G. (2005). El concepto de la seguridad en la teoría de las relaciones internacionales. Revista CIDOB d'Afers Internacionals, 72, 161-180. http://www.jstor.org/stable/40586218

Orozco, G. (2006). Problemas y desafíos de la seguridad en la globalización. Centro Argentino de Estudios Internacionales. https://www.academia.edu/13445371/Problemas_y_Desaf%C3%ADos_de_la_Seguridad_en_la_Globalizaci%C3%B3n

Oxfam. (2016). Nuevas dinámicas de comunicación, organización y acción social en América Latina: Reconfiguraciones tecno-políticas (Informe). Oxford, Reino Unido: Oxfam Publishing. https://www-cdn.oxfam.org/s3fs-public/file_attachments/nuevas_dinamicas_de_comunicacion_organizacion_y_accion_social_en_americalatina._reconfiguraciones_tecnopoliticas.pdf

Parlamento Europeo y Consejo de la Unión Europea. (2019). *Reglamento (UE) 2019/881 relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 (Reglamento sobre la Ciberseguridad)*. Diario Oficial de la Unión Europea, L 151/15–L 151/69. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32019R0881

Parmar, I. (Ed.). (2014). Obama, WikiLeaks, and American power. New directions in US foreign policy (pp. 243-257). https://openaccess.city.ac.uk/id/eprint/16934/1/PARMAR%20-%20Obama,%20Wikileaks%20and%20American%20Power.pdf

Patiño, G. A. (2019). El sistema internacional cibernético: elementos de análisis. Oasis, 30, 163–186. https://doi.org/10.18601/16577558.n30.10

Poder Ejecutivo. (2018). Decreto Legislativo que aprueba la Ley de Gobierno Digital. El Peruano. https://cdn.www.gob.pe/uploads/document/file/353216/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1.pdf?v=1566312763

Poder Ejecutivo. (2024). Decreto Supremo que aprueba el Reglamento de la Ley Nº 30999, Ley de Ciberdefensa. El Peruano. https://www.congreso.gob.pe/Docs/DGP/DIDP/files/ds_017-2024-pcm.pdf

Prado, J. (2017). El liberalismo institucional de las relaciones internacionales. Araucaria. Revista Iberoamericana de Filosofía, Política, Humanidades y Relaciones Internacionales, 19(37), 367-386. https://www.academia.edu/32156737/El_Liberalismo_Institucional_de_las_Relaciones_Internacionales

Prado, J. (2021). Liberalismo institucional. En J. Schiavon, A. Ortega, M. López, & R. Velázquez (Eds.), Teorías de las Relaciones Internacionales del siglo XXI: Interpretaciones críticas desde México y América Latina (pp. 409-428). CIDE. Recuperado de https://www.academia.edu/45613778/El_Liberalismo_Institucional

Presidencia del Consejo de Ministros. (2023). Perú presenta propuestas en Naciones Unidas para convención internacional contra la ciberdelincuencia. Perú. https://www.gob.pe/institucion/pcm/noticias/646916-peru-presenta-propuestas-en-naciones-unidas-para-convencion-internacional-contra-la-ciberdelincuencia

Prieto, V. M., & Pan, R. A. (2014). Virus informáticos (Trabajo de máster, Universidad de Coruña, España). Recuperado de http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/08%20-%20Virus%20Informaticos.pdf

Quevedo, C. (2023). Ciberdefensa y ciberseguridad en el Perú: Realidad y retos en torno a la capacidad de las FF.AA. para neutralizar ciberataques que atenten contra la seguridad nacional. Revista de Ciencias e Investigación en Defensa-CAEN, 1, 55-76. https://www.recide.caen.edu.pe/index.php/recide/article/download/99/121

Quian, A., & Elías, C. (2018). Strategies and reasons for the impact of WikiLeaks on world public opinion. Revista Española de Investigaciones Sociológicas, 162, 91-110. https://doi.org/10.5477/cis/reis.162.91

Reardon, R., & Choucri, N. (2012, abril). The role of cyberspace in international relations: A view of the literature. Ponencia presentada en la ISA Annual Convention, San Diego, CA, Estados Unidos. https://nchoucri.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%202012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf

Ripoll, A. (2007). La cooperación internacional: Alternativa interestatal en el siglo XXI. Revista de Relaciones Internacionales, Estrategia y Seguridad, 2(1), 67-83. Bogotá, Colombia: Universidad Militar Nueva Granada. Recuperado de https://www.redalyc.org/pdf/927/92720104.pdf

Rossi, G. (2021). La seguridad y defensa en la era de la cuarta revolución industrial: Elementos para una propuesta de estrategia de política exterior para el fortalecimiento de las capacidades del Perú en materia de ciberdefensa y amenazas híbridas (Tesis de licenciatura, Academia Diplomática del Perú). Repositorio Institucional de la Academia Diplomática del Perú.

http://repositorio.adp.edu.pe/bitstream/handle/ADP/170/2021%20Tesis%20Rossi%20Levano,%20Giancarlo.pdf?sequence=1

RPP. (2022, 10 de octubre). 'Guacamaya Leaks': "Se ha filtrado un ratio bajo de información peruana, pero es una amenaza contra toda América Latina", afirma especialista. Lima, Perú. https://rpp.pe/politica/gobierno/guacamaya-leaks-especialista-senala-que-se-ha-filtrado-un-ratio-bajo-de-informacion-peruana-pero-es-una-amenaza-contra-toda-america-latina-noticia-1438405?ref=rpp

Ruiz, C. B., & Cortés Borrero, R. (2023). Los ciberdelitos y la ciberseguridad: Una cuestión de género. Informática y Derecho: Revista Iberoamericana de Derecho Informático (Segunda Época), 13, 73-84. Recuperado de https://revistas.fcu.edu.uy/index.php/informaticayderecho/article/view/3999

Secretaría de Relaciones Exteriores de México. (s. f.). Comisión de Seguridad Hemisférica, del Consejo Permanente. Secretaría de Relaciones Exteriores de México. https://mision.sre.gob.mx/oea/index.php/actividades/18-menu/271-seguridad#:~:text=la%20Declaraci%C3%B3n%20sobre%20Seguridad%20en%20las%20Am%C3%A9ricas%20fue%20resultado%20de,partida%20de%20una%20nueva%20etapa

Sohr, R. (2011). América Latina según Washington, vía WikiLeaks. Mensaje, 60(596), 11-13. Residencia San Roberto Bellarmino. https://repositorio.uahurtado.cl/static/pages/docs/2011/n596_11.pdf

Stratcom Centre of Excellence (2007). Cyber Attacks in Estonia. https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf.

Tenable. (2021). ProxyShell attackers actively scanning for vulnerable Microsoft Exchange servers (CVE-2021-34473). https://www.tenable.com/blog/proxyshell-attackers-actively-scanning-for-vulnerable-microsoft-exchange-servers-cve-2021-34473

Trautman, L. J. (2015). Cybersecurity: What about U.S. policy? Journal of Law, Technology and Policy, 2015(1), 341-410. https://doi.org/10.2139/ssrn.2548561

Unión Internacional de Telecomunicaciones (UIT). (1932). Constitución de la Unión Internacional de Telecomunicaciones. https://www.itu.int/en/council/Documents/basic-texts/Constitution-S.pdf

Unión Internacional de Telecomunicaciones (UIT). (2020). Índice global de ciberseguridad 2020. Sector de Desarrollo de la UIT. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/global-cybersecurity-index-2020.pdf

Unión Internacional de Telecomunicaciones (UIT), Banco Mundial, Secretaría de la Commonwealth (Comsec), Organización de Telecomunicaciones de la Commonwealth (CTO), & Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE OTAN). (2018). Guía para la elaboración de una estrategia nacional de ciberseguridad – Participación estratégica en la ciberseguridad. Creative Commons

Attribution 3.0 IGO (CC BY 3.0 IGO). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-S.pdf

United Nations Office at Geneva. (s.f.). International Telecommunication Union (ITU). https://www.ungeneva.org/es/about/organizations/itu

Val, K., & Akyesilmen, N. (2021). Competition for high politics in cyberspace: Technological conflicts between China and the USA. Polish Political Science Yearbook, 50(1), 43-69. https://czasopisma.marszalek.com.pl/images/pliki/ppsy/50/ppsy202116.pdf

Valencia, D. (2015). El Estado en la era de la globalización y las nuevas tecnologías. Bogotá D.C., Colombia: Grupo Editorial Ibáñez.

Valeriano, B., Jensen, B., & Maness, R. C. (2018). Cyber strategy: The evolving character of power and coercion. New York, NY: Oxford University Press.

Vallés, J. M. (2007). Ciencia política: una introducción. Barcelona, España: Ariel. Recuperado de https://ovejasconpieldelobo.wordpress.com/wp-content/uploads/2016/01/josep-m-valles-ciencia-politica-una-introduccion.pdf

Vicente, L. (2004). ¿Movimientos sociales en la Red? Los hacktivistas. El Cotidiano, 20(126), 85-92. Recuperado de http://www.redalyc.org/pdf/325/32512615.pdf

Vilca, A., & Gabi, L. (2018). Los hackers: Delitos informáticos frente al código penal peruano (Tesis de título profesional). Universidad Nacional Santiago Antúnez de Mayolo (UNASAM), Perú. https://repositorio.unasam.edu.pe/handle/UNASAM/2496

Vicens, A. (19 de septiembre de 2022). Hacking group focused on Central America dumps 10 terabytes of military emails, files. CyberScoop. https://www.cyberscoop.com/central-american-hacking-group-releases-emails/

Wilkinson, I. (octubre de 2023). ¿Qué es el Tratado de la Organización de las Naciones Unidas sobre el Cibercrimen y por qué es importante? FES Briefing, Red de Seguridad Incluyente, No. 3. Fundación Friedrich Ebert, Oficina Bogotá. https://library.fes.de/pdf-files/bueros/la-seguridad/20667.pdf

Zurita, M. D. (2007). La Guerra Fría en el marco de las Relaciones Internacionales [Objeto de conferencia]. https://secyt.presi.unlp.edu.ar/cyt_htm/ebec07/pdf/zurita.pdf