RICI Revista Ibero-Americana de Ciência da Informação

ISSN 1983-5213

Política e Estratégias da Segurança Cibernética, um estudo de caso múltiplo: Argentina, Peru e Brasil

Arthur Christian Huamani Cuba
Universidade Federal de Minas Gerais, Programa de Pós-graduação em Ciência da Informação, Belo Horizonte, MG, Brasil
ORCID: https://orcid.org/0000-0002-3118-7889
arthur.huamani@opendeusto.es

Maria Aparecida Moura
Universidade Federal de Minas Gerais, Programa de Pós-graduação em Ciência da Informação, Belo Horizonte, MG, Brasil
ORCID: https://orcid.org/0000-0003-2670-923X
mamoura@ufmg.br

DOI: https://doi.org/10.26512/rici.v17.n1.2024.51481

Recebido/Recibido/Received: 2023-11-05
Aceitado/Aceptado/Accepted: 2024-03-11
Publicado/Publicado/Published: 2024-03-27

ARTIGOS

Resumo

O estudo de caso busca compreender aos elementos e agentes influenciados nas estratégias de segurança cibernética da Argentina, Peru e Brasil. Através do análise de conteúdo computacional foram analisados 108 documentos digitais, 06 entrevistas e 20 questionários individuais semiestruturados. Na perspectiva da ciência da informação, foram descritos 6 fatores, que orienta os códigos, as categorias temáticas e suas relações. Sendo agrupados e comparados a partir dos 7 aspectos: Ameaças e riscos, capacidades e resposta, poder e dominação, geopolítico e diplomático, sociocultural e organizacional, socioeconómico e comercial, e tecnológico e industrial. Fortalecendo a compreensão dos fenômenos não evidentes. Em conclusão, o Aspecto Sociocultural e Organizacional é relevante para os objetivos da segurança cibernética. Porém, o Aspecto Geopolítico e Diplomático é menos relevante para estes três países. Por fim, foram apresentadas as implicações teóricas e recomendações para a segurança cibernética destes países.

Palavras-chave: Segurança cibernética. Ciberdefesa. Política de Segurança Cibernética. Segurança da Informação. Ciber política.

Política y Estrategias de la Seguridad Cibernética, un estudio de caso múltiple: Argentina, Perú y Brasil

Resumen

El estudio de caso busca comprender a los elementos y agentes influenciados en las estrategias de la seguridad cibernética de Argentina, Perú y Brasil. Por medio del análisis de contenido computacional, fueron analizados 108 documentos digitales, 06 entrevistas y 20 cuestionarios individuales semiestructurados. Desde la perspectiva de la ciencia de la información, fueron descritos 6 fatores que direcciona a los códigos, categorías temáticas y de sus relaciones. Agrupados y comparadosdesde7 aspectos: Amenazas y riesgos, capacidades y respuesta, poder y dominación, geopolítico y diplomático, sociocultural y organizacional, socioeconómico y comercio, y tecnológico e industrial. Fortaleciendo la comprensión de los fenómenos no evidentes. En conclusión, el Aspecto Sociocultural y Organizacional es

relevante en los objetivos de la seguridad cibernética. No obstante, el Aspecto Geopolítico y Diplomático es menos relevante para estos tres países. Finalmente, fueron presentadas las implicaciones teóricas y recomendaciones a la seguridad cibernética de estos países.
PALABRAS CLAVE: Ciberseguridad. Ciberdefensa. Política de Ciberseguridad. Seguridad de la información. Ciberpolítica.

Policy and Strategies in Cyber Security, a multiple case study: Argentina, Peru and Brazil

Abstract

The case study seeks to understand the elements and agents influenced by the cybersecurity strategies of Argentina, Peru and Brazil. Through computational content analysis, 108 digital documents, 06 interviews and 20 individual semi-structured questionnaires were analyzed. From the perspective of information science, 6 factors were described that direct the codes, thematic categories and their relationships. Then, group them and compare them from 7 aspects: Threats and risks, capabilities and response, power and domination, geopolitical and diplomatic, sociocultural and organizational, socioeconomic and trade, and technological and industrial. Strengthening the understanding of non-evident phenomena. To summarize, the Sociocultural and Organizational Aspect has greater relevance for the cybersecurity objectives. However, the *Geopolitical and Diplomatic Aspect* is less relevant for these countries. Finally, the theoretical implications and recommendations for the cybersecurity of these countries were presentad.

Keywords: Cybersecurity. Cyber Defense. Cybersecurity Policy. Information Security. Cyberpolitics.

1. Introducción

En el debate político-estratégico de la seguridad y defensa cibernética, las capacidades cibernéticas de los países son estimuladas por el impacto cultural, geoeconómico y sociopolítico. Por primera vez, en 1998hemos observado propuestas para el control de armas cibernéticas a través de la Organización de la Naciones Unidas (ONU, 1998), existiendo discrepancias y desinterés en los países desarrollados de elaborar un contrato social global en el dominio cibernético. Siendo un desafío para los países en vías de desarrollo, en su anhelo de poseer una política de seguridad cibernética (SegCiber) con estrategias idóneas y relevantes a sus intereses y objetivos nacionales. En la agenda de la seguridad nacional de países desarrollados, la amenaza cibernética está en sus escenarios y prioridades. El *World Economic Forum*(WEF) publicó que la ciberdelincuencia y la inseguridad cibernética generalizada ocuparán la octava posición con relación a otros riesgos globales (WEF, 2023). El problema central que desafiará a gobiernos y sociedades será en la coordinación de los talentos individuales, colectivos y nacionales para producir seguridad, prosperidad y esperanza sustentable (Nasser, 2019, p.34). La Organización de los Estados Americanos (OEA) en la óptica de la seguridad multidimensional busca garantizar la seguridad de sus integrantes, con la cooperación de varios frentes de la seguridad, el desarrollo de políticas y estrategias motivando reformas en la Doctrina de Seguridad Nacional (DSN) a través de su Junta Interamericana de Defensa(JID).

> La JID busca impulsar un Programa de Ciberdefensa para facilitar la comunicación y colaboración en ciberdefensa entre las Fuerzas Armadas del

> Hemisferio Occidental. Los principales objetivos del Programa de Ciberdefensa de la JID son: Fortalecer las capacidades individuales y colectivas de defensa cibernética en el Hemisferio Occidental. Apoyar la implementación de un marco de Cooperación en Ciberdefensa en las Américas. Mejorar el diálogo, la comunicación y la colaboración entre países (Junta Interamericana de Defensa [JID], 2023).

En contraste, las amenazas de los países sudamericanos tratan de problemas sociales de orden transnacional, de modo que esta investigación transita sobre6 factores: *Primer factor*, trata del poco interés delos países sudamericanos en un conflicto cibernético entre Estados. Para Castells (2018, p.241) casi todos los países sudamericanos están envueltos en agitaciones y crisis causados por la conexión directa e indirecta entre el crimen organizado y la política. Siendo las tecnologías de la información y de la comunicación (TIC) un medio sutil que alcanza el ámbito cultural, como difusores de la cultura del crimen organizado. Para Castells (2018, p.200) son elementos que constituyen un trazo esencial de la nueva economía global y de la dinámica política-social de la era de la información. *Segundo factor*, es la inestabilidad política regional donde sus sistemas democráticos inmaduros y la desconfianza a sus gobernantes y autoridades son clasificados como nuevas amenazas. En ese sentido, son discutidos en cómo son alterados el orden global y su naturaleza de poder, por tendencias que convergen y dificultan en la cooperación y gobernanza de los Estados-Nación. Entre las tendencias que están transformando el paisaje global son:

> [..].La economía global está cambiando. El bajo crecimiento económico persistirá en el corto plazo. La tecnología está acelerando el progreso, pero causa rupturas. Ideas e identidades están generando una ola de exclusión. Será cada vez más difícil gobernar; 6. La naturaleza del conflicto está cambiando […](Nasser, 2019, pp.37-39).

El *tercer factor*, es la inversión en SegCiber donde es defendida la tasa de éxito que ejerce ese tipo de inversión con relación a las iniciativas políticas del Estado, principalmente, en el ámbito económico y financiero. Para los países sudamericanos la capacidad de sus recursos tecnológicos es limitado e insuficiente. En donde las prioridades gubernamentales son problemáticas relacionadas al desarrollo socioeconómico: corrupción, inseguridad interna, educación precaria, desempleo, pobreza, tráfico de drogas, insuficientes servicios de salud, entre otros. Por tanto, inferimos que las necesidades de inversión para mitigar las amenazas de la seguridad y defensa cibernética sudamericana divergen de países hegemónicos. *Cuarto factor*, los países en vías de desarrollo enfrentan amenazas complejas, indefinidas, desestructuradas, con problemas desgobernados, con dependencia político-tecnológica y ausencia de identidad. Entiéndase como hegemonía política-tecnológica a la supremacía de un Estado sobre otro, convirtiéndolo en un Estado soberano dado por su fuerza política y de producción tecnológica

en base al mecanismo invisible de su influencia en la sociedad y de la dominación consentida. Los países sudamericanos tienen dependencia económica y tecnológica frente a hegemonías como Estados Unidos y China (Preciado, Uc, 2015).*Quinto factor*, un país que durante el proceso de planificación multisectorial de sus capacidades cibernéticas no considere el contexto geopolítico y geoeconómico del ciberespacio en sus intereses nacionales, dispondrá de una política que podría dificultar en la comprensión de los retos y beneficios en el uso del ciberespacio y del Internet en la sociedad. En consecuencia, podría generar utopías con relación a la llamada *Onda Digital*, ahondando más, en los principales problemas socioeconómicos relacionados con los niveles de vida, pobreza, desempleo, informalidad, corrupción, violencia (CEPAL, 2020).*Sexto factor*, la conexión de la política de Estado y su capacidad cibernética acordes con los recursos y activos disponibles en el Estado-Nación. Por tanto, los desafíos de la cadena productiva estatal en el dominio del ciberespacio incluyen el incremento de la capacidad humana y de tecnologías para resolver problemas cibernéticos, equilibrar las libertades civiles y elaborar necesarios acuerdos internacionales (KRAMER, et al, 2009).

Sin embargo, para los países sudamericanos ¿son los mismos desafíos?, ¿qué elementos son influenciados en la política de SegCiber? y ¿cómo esos elementos son considerados en sus especificaciones geoeconómicas? En la perspectiva de la ciencia de la información, la dinámica informacional de los 6 fatores relatados direccionará el análisis crítico reflexivo de los elementos y agentes adherido sen las políticas y estrategias de la SegCiber de los países de Argentina, Brasil y Perú. Además, en lo teórico relacionaremos lo propuesto por Huntington (2010, p.24) en la reconfiguración de la política mundial a través de líneas culturales y civilizacionales. Para Huntington (2010) la seguridad mundial requiere de la aceptación multicultural global, siendo amenazada por la crisis global de la gobernabilidad. En el contexto contemporáneo estamos vivenciando una crisis global y cambios en el orden mundial, acelerados por la guerra de Ucrania y Rusia. Asimismo, en este siglo, han ido ascendiendo otras civilizaciones impulsando procesos globales de indigenización y resurgimiento de culturas no occidentales, causados por la modernización y las TIC. Según Huntington (2010) los conflictos futuros serán por criterios culturales y religiosos. Como limitación y de interés a nuestra investigación, vamos a interesarnos en el criterio cultural y no en lo religioso. A su vez, Huntington incita que los países latinoamericanos deben definir su identidad, pudiendo ser a la de una civilización occidental o como un Estado-Núcleo, por ello nuestros análisis fluctuaran en 3 países de Sudamérica como candidatos para constituir la base de un Estado-Núcleo sudamericano.

> Los Estados-Núcleos intentan congregar legiones civilizacionales, hacer alianzas con Estados de terceras civilizaciones, promover la división y las deserciones en civilizaciones opuestas, y emplear la combinación adecuada de acciones diplomáticas, políticas, económicas y clandestinas, así como

> instigaciones por propaganda y forma de coerción, para lograr sus objetivos (Huntington, 2020, p. 350).

La problemática será analizada en la perspectiva del modelo social y pragmático: como *modelo social*, en el anhelo de la sociedad de participar en la gobernanza, no sólo como administradora, también en apoyo a la administración de sus objetivos nacionales. Según Dunn e Egloff (2019, p.47-48), debido a la complejidad de la SegCiber la responsabilidad del Estado fue incrementada, pasando por 3 fases: (1) De ser un Estado propietario de la información y de las redes (En el año de 1980). (2) De ser un Estado propietario del problema, siendo responsable de resolver y mejorar la seguridad del sistema y del colectivo (En el año de 1990). (3) De ser un Estado originador del problema, en su corrida armamentista y de guerra cibernética (En el año 2000). En la perspectiva del modelo pragmático*,* se concretiza en la acción, investigando las propiedades y los comportamientos con la SegCiber, así como, de las fuerzas que rigen en el flujo informacional, medios y relaciones de poder e influencia. Así el análisis crítico se sustenta en la perspectiva del régimen de la información, permitiéndonos comprender las relaciones existentes en las políticas de las tecnologías de la información, cultura e información. Entiéndase como régimen de la información:

> Un modelo de producción informacional dominante en una formación social, conforme el cual serán definidos sujetos, instituciones, reglas y autoridades informacionales, los medios y los recursos preferenciales de información, los padrones de excelencia y los arreglos organizacionales de su procesamiento selectivo, sus dispositivos de preservación y distribución (González de Gómez 2002, p.34).

Para Foucault (2019) en la sociedad son diversas las relaciones de poder que construyen el cuerpo social, ellas no pueden disociarse, establecerse o funcionar sin: una producción, una acumulación, una circulación, un funcionamiento del discurso verdadero. Por tanto, el problema de la soberanía, principalmente occidentales, está ligada al discurso y la técnica del derecho en función de disolver el núcleo del poder, la dominación, reduciendo o enmascarando los derechos legítimos de la soberanía y la obligación legal de la obediencia. Conforme exploremos las relaciones de un modo sistemático, uno de los aspectos que necesitan de nuestra atención es la comprensión de la economía política, expresada en las políticas y líneas de acción del Estado-Nación. Según Foucault (2020) la economía política es un sistema de pensamientos que nos permiten entender todo, de cómo la economía política y las instituciones del mercado permiten determinar el valor de bienes y servicios. Si los gobiernos conocen los mecanismos económicos en su naturaleza íntima y compleja, ellos la respetarán. Ese respeto no quiere decir aprovisionarse de una estructura jurídica con relación a las libertades y derechos fundamentales. El respeto del mecanismo es dotar a la política de conocimientos rigurosos,

constantes, claros y diferenciados, limitado por la evidencia y no por la libertad de los individuos. Entonces la vigilancia informacional, en la mecánica de los intereses no es peligrosa, debiendo responder a las estrategias de la seguridad que en ciertas condiciones será lo inverso a la condición del liberalismo.

> El liberalismo no es aquello que acepta la libertad. El liberalismo es aquello que propone fabricarla a cada instante, suscitarla y producirla, ciertamente con [todo el conjunto](*) de limitaciones, de problemas de costos creados por esa fabricación. ¿Cuál va a ser entonces el principio de cálculo de ese costo de fabricación de la libertad? El principio de cálculo es, evidentemente, aquello que se llama seguridad (Foucault, 2020, p. 95).

Por tanto, es importante analizar la dependencia tecnológica en una era de cambios tecnológicos y aceleración mundial. Cuando Castells (2018, p.238) aborda los asuntos de desarrollo y dependencia, afirma que la globalización e identidad interactúan en la economía criminal de Latinoamérica. Para Zuboff (2020) el Internet es esencial en la participación de la sociedad, sin embargo, es subordinada al capitalismo de vigilancia, que es asimétrico con relación al conocimiento y al poder que de él emergen, desconsiderando normas sociales, anulando derechos de autonomía individual, amenazando la esencia de una sociedad democrática.

> El capitalismo de vigilancia no es tecnología; es una lógica que impregna la tecnología y la direcciona en una acción. El capitalismo de vigilancia es una forma de mercado que es inimaginable fuera del medio digital, pero no es la misma cosa que digital (Zuboff, 2020, p. 26).

Las reflexiones de Castells (2018) y Zuboff (2020) de la inevitabilidad tecnológica, definenaún más, los parámetros de este artículo; dejando en evidencia que la tecnología no es ni debe ser un fin en sí. Para Max Weber la tecnología posee una orientación económica, siendo una expresión de los objetos económicos que la dirigen para la acción. A partir del marco teórico descrito, juntamente con los documentos colectados dela SegCiber de Argentina, Brasil y Perú, servirán de catalizadores al análisis crítico reflexivo, a fin de disponer del panorama actual de las configuraciones y estrategias en SegCiber. Esta investigación busca abrir caminos sobre la comprensión de los elementos, agentes y las relaciones que son influenciados en las políticas y estrategias de la SegCiber de los países estudiados.

2. Organización del análisis y características de los corpus

Analizamos108 documentos digitales, 6 entrevistas y 20 cuestionarios semiestructuradas. La colecta documental se basa en el contexto y tópicos tratados en la seguridad y defensa cibernética. Las categorías temáticas fueron agrupadas en 7 aspectos: Aspecto de las amenazas y riesgos (AAR), Aspecto de las capacidades y respuesta (ACR), Aspecto

del poder y dominación (APD), Aspecto geopolítico y diplomático (AGD), Aspecto sociocultural y organizativo (ASO), Aspecto socioeconómico y comercio (ASC) y Aspecto tecnológico e industrial (ATI), componiendo nuestro estudio de caso múltiplo (Yin, 2001, p. 64). El estudio de caso es una estrategia de investigación que busca una lógica de planeamiento incorporando tópicos específicos a la colecta y análisis de los datos. Según Yin (2001) en el estudio de caso, la principal pregunta de investigación es el ¿cómo? o el ¿por qué?, no se tiene control de los eventos comportamentales y el foco del estudio trata de un fenómeno contemporáneo.

> En primer lugar, los estudios de casos, en general, no deben utilizarse para evaluar la incidencia de fenómenos. Según un estudio de caso, tendría que tratar tanto el fenómeno de interés como su contexto, produciendo muchas variables potencialmente relevantes.[…]. En tercer lugar, si la lógica del muestreo tuviera que aplicarse a todos los tipos de investigación, muchos temas podrían no investigarse empíricamente (Yin, 2001, p. 71-72).

El diferencial de un estudio de caso es el comprender los fenómenos sociales complejos. Un estudio de caso es un fenómeno presente o del pasado, confeccionada con diversas fuentes de pruebas, desde datos de observación directa, entrevistas sistemáticas, investigaciones en archivos públicas y privados (Voss, Tsisikriktsis e Frohlic, 2002). El análisis documental y teórico, hace uso del método de análisis de contenido computacional, por medio del *software MAXQDA* para la visualización y descripción sistematizada de las observaciones cuantitativas y cualitativas. "El principio del análisis de contenido consiste en desmontar la estructura y los elementos de este contenido para esclarecer sus diferentes características y extraer su significado"(LAVILLE, DIONNE, 1999, p. 214).Escogimos *MAXQDA* porque sus funcionalidades permiten atribuir códigos en partes seleccionadas del contenido de un documento digitalizado, pudiendo ser párrafos de textos, palabras, porciones de imagen, video o audios. Las funciones relevantes utilizadas son las siguientes:

Codificación: Asignar códigos a partes de un documento (pasaje de texto, parte de una imagen, clip de vídeo). Forma categorías inductivamente a partir del texto […] (Rädiker, Kuckartz, 2020). Proceso donde los datos brutos son transformados sistemáticamente y agregados en unidades, permitiendo una descripción exacta de las características del contenido (Bardin, 2016). La codificación utilizada sigue el enfoque inductivo.

Código o subcódigo: Se asigna a un segmento de texto, imagen, audio o vídeo. Por tanto, los códigos y subcódigos son descripciones condensadas de fenómenos descubiertos en los datos de los documentos. El sistema de códigos sigue una jerarquía, donde un conjunto de subcódigos constituye un código. Un conjunto de subcódigos y códigos conforman una categoría. Notas analíticas preliminares: Contienen las notas del investigador, como descripciones e instrucciones en el uso de las categorías. Pueden utilizarse en la formulación, registro, enlace de

supuestos e hipótesis sobre relaciones o hallazgos importantes en los documentos explorados (Rädiker, Kuckartz, 2020).

Categorías: Son rubricas que reúnen un grupo de elementos (unidades de registro) sobre un título genérico. Ese agrupamiento es debido a características comunes de los elementos (Bardin, 2016).

> Las categorías se utilizan para estructurar el contenido, para generar tipos y para la valoración (evaluación) de los enunciados (Kuckartz, 2014b). En los proyectos de investigación que siguen un enfoque de teoría fundamentada, las categorías asumen un papel importante en el desarrollo de las teorías (Charmaz, 2014; Corbin & Strauss, 2015) […] (Rädiker, Kuckartz, 2020)

Categorías temáticas: Basadas en el contenido, sirven para estructurar el contenido. Es como una señal de tránsito, que señala un área temática o tema en el texto (Rädiker, Kuckartz, 2020).La agrupación de categorías temáticas, por similitud y correspondencia de la teoría o de explicaciones provisorias, constituyen un aspecto que puede ser cualitativo producto de la inferencia.

Esta investigación no visa responder a causas y efectos, de los eventos sociales relacionados con la consolidación de las políticas en SegCiber en los países estudiados. La elección del estudio de casos múltiplos, obedece a lo siguiente: (1) Optamos en trabajar con la política, programas y doctrina militar en seguridad y defensa cibernética de Argentina, Brasil y Perú. Por el motivo de existir pocas publicaciones oficiales, en formato digital. Además, son escasas las investigaciones que aborden una comparación documental de las políticas y estrategias de la SegCiber entre países sudamericanos.(2)La proximidad, con los documentos investigados, incluyendo del idioma, siendo razón factible para el análisis documental e instrumentalización.(3) Son países miembros de la OEA y la ONU, participando de los planes, programas y proyectos en el ámbito de la SegCiber regional.(4) Por las semejanzas en los riesgos y amenazas, según el WEF (2023) los ataques cibernéticos no ocupan las diez primeras posiciones de los riesgos mapeados en la región Sudamericana.(5) Poseen brechas tecnológicas en común y dependencia de sus telecomunicaciones con relación a los países occidentales (Romero, 2020).(6) Influencia de la Guerra Fría, principalmente, en la creación de sus DSN y que sirvió de instrumento para instaurar dictaduras militares en sus países (Guimarães, 2014).(7) La geolocalización central e influencia geopolítica de Brasil por el Atlántico y de Perú por el Pacífico. Conformando ambos un *Hub* fronterizo con los demás países Sudamericanos.(8) En el índice de

desempeño industrial competitivo de 2020 (*Competitive Industrial Performance Index*[1]) los países estudiados no alcanzan el *Top Quintile* del *ranking* mundial.

La colecta documental se limita al nivel político-estratégico de la SegCiber, otra limitante es el acceso, por la existencia de documentos reservados o confidenciales. La colecta investiga sites gubernamentales de los dominios: .gob.ar; .gov.br y .gob.pe. Seleccionando documentos que citan a Internet, seguridad de la información (SI), ciber, ciberseguridad y ciberespacio. Además, estudiar todos los niveles, en forma cuantitativa y cualitativa, corremos el riesgo de generalizar los resultados, brindando una falsa noción de unidad, impidiendo el tratamiento de un problema específico. En el proceso de organización documental, cada país constituye un único *corpus*. El etiquetado del corpus corresponde a grupos temáticos: Leyes y regulaciones nacionales (LRN), política y líneas de acción estratégica (PLA) y publicaciones del departamento de defensa (PDD). Para luego, ser sometidos a *MAXQDA*[2]para su procesamiento y análisis.

Tabla 1. Organización y características de los corpus

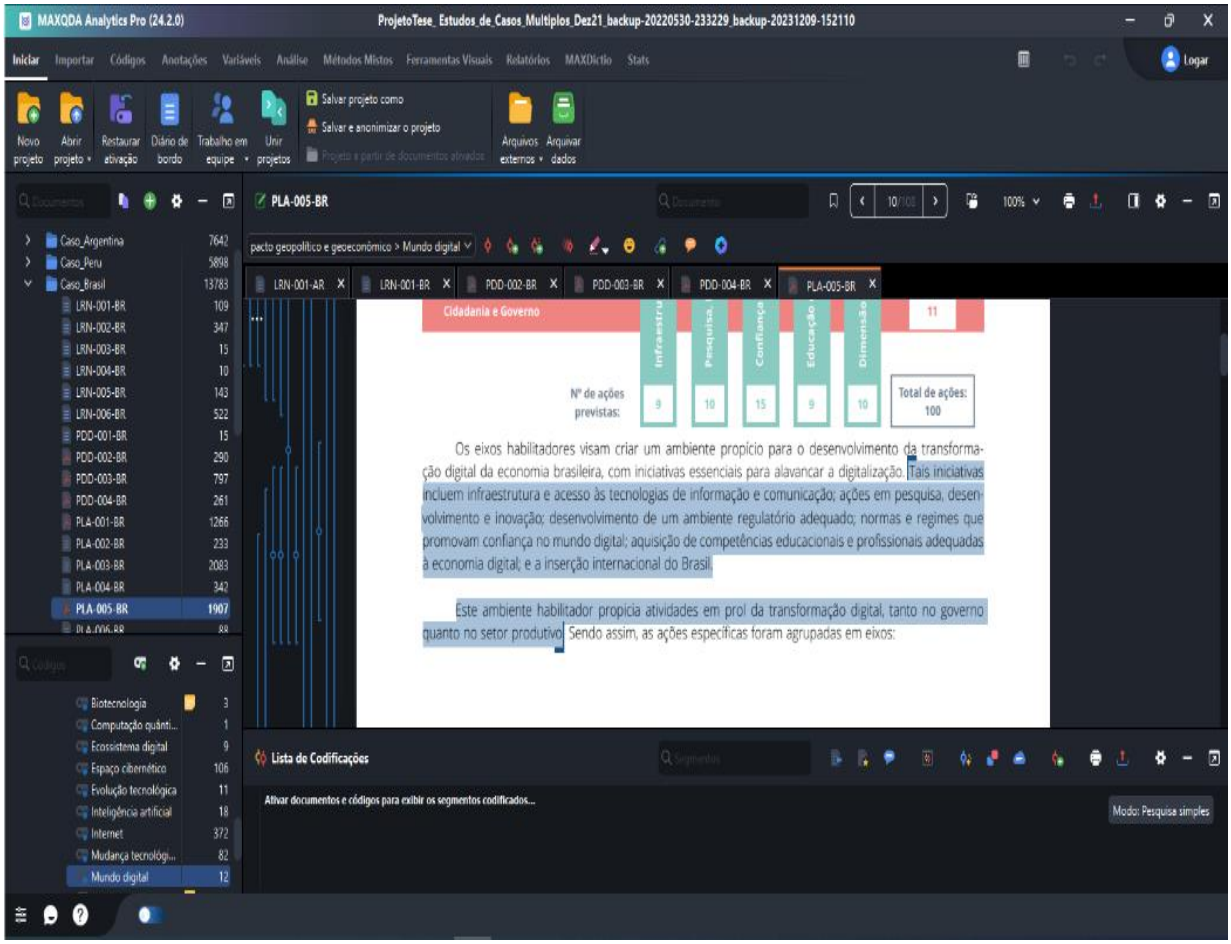
Estudio de Caso	Grupos temáticos			Características del Corpus (fuente pública y gubernamental)
	LRN	PLA	PDD	
Argentina	5	27	7	Anexo I: documentos en formato website (html) y ".txt".
Perú	13	18	5	Anexo II: documentos en formato PDF (*Portable Document Format*)
Brasil	6	23	4	Anexo III: documentos en formato PDF (*Portable Document Format*) y ".txt"

Fuente: Elaboración propia.

[1] Disponible en <https://stat.unido.org/cip/?_ga=2.143995447.367874604.1663818771-1179266831.1663818771# > . Acceso 20 julio de 2022.

[2] MAXQDA es un programa de software para el análisis cualitativo y de métodos mixtos asistido por computador. Disponible en <https://www.maxqda.com/>. Acceso 20 de Julio de 2022.

Figura1. Organización del *corpus* en el *software MAXQDA*



Fuente: Elaboración propia.

Para Dunn e Egloff (2019) en el año 2000, se inicia la corrida ciber armamentista y de la ciberguerra. Según el Centro de Excelencia en Defensa Cibernética Cooperativa de la OTAN, son 81 países que poseen una política nacional en SegCiber. A partir del 2011,se observa un incremento en la elaboración de políticas (CCDCOE, 2022).Por ello, la colecta documental[3] fue de enero del 2000 a setiembre del 2020[4].Así, conformamos 3 corpus del tipo selectivo y computarizado. Además, para el corpus ser válido y confiable, nuestra selección sigue los requisitos de autenticidad, representatividad, muestra, diversidad y tamaño (Aluísio, Barcellos, 2006, p.158).El análisis del contenido con *MAXQDA* facilitó la exploración de los documentos. Según Bardin (2016, p. 126) para el investigador la elaboración del preanálisis documental radica en la organización. Después, con la operación de la codificación serán explorados los documentos de forma individual y monótona, alcanzando la saturación teórica.

> Se considera saturada la colecta de datos cuando ningún nuevo elemento es encontrado y el incremento de nuevas informaciones deja de ser necesario,

[3] Con excepción de 1 documento del Corpus de Brasil, que es de 1997.
[4] Fecha límite elegida por los investigadores, para dar inicio al análisis y tratamiento documental.

> pues no altera la comprensión del fenómeno estudiado (NASCIMENTO et al., 2018, p. 244).

Al alcanzar la saturación teórica, activamos la codificación automática de *MAXQDA,* logrando estructurarlas categorías temáticas. Como método complementario, realizamos cuestionarios y entrevistas[5]cualitativas con características semiestructuradas e individuales.Abordando7 aspectos identificados, permitiéndonos explorar en profundidad nuestras categorías, en relación con la experiencia del experto. Analizando sus decisiones, motivaciones, comportamientos, creencias y actitudes de los expertos. La evaluación de los resultados obtenidos suministró informaciones valiosas no contempladas.

> La entrevista cualitativa, pues, proporciona los datos básicos para el desarrollo y la comprensión de las relaciones entre los actores sociales y su situación. El objetivo es una comprensión detallada de las creencias, actitudes, valores y motivaciones, en relación con los comportamientos de las personas en contextos sociales específicos (Bauer, Gaskell, 2019, p. 65)

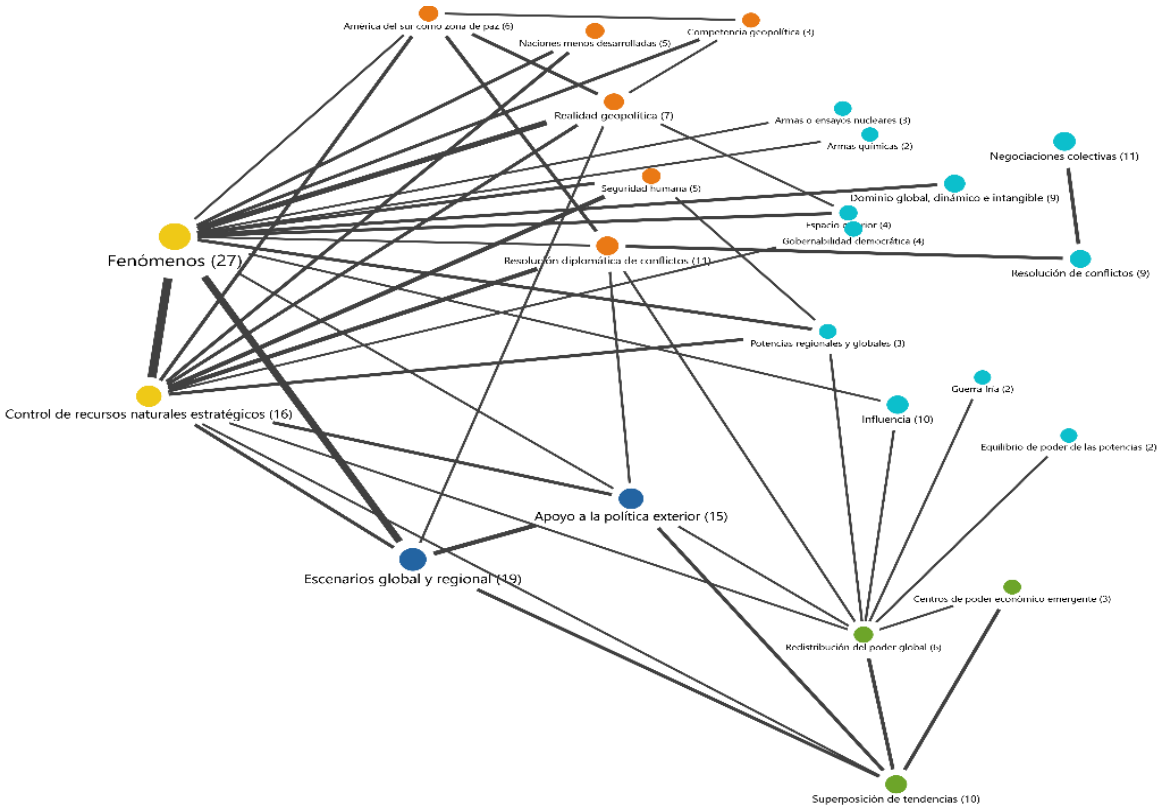
En la planificación, realizamos un pretest con2 expertos, a fin de identificar imprecisiones discursivas, errores gramaticales o técnicos, complejidades, preguntas desnecesarias, vergüenza y agotamiento del participante. El análisis cualitativo es un procedimiento intuitivo, según Bardin (2016, p.145) “es más maleable y adaptable a los índices imprevistos, o a la evolución de hipótesis”. El agrupamiento de los códigos caracteriza a la creación de categorías, las cuales proveen de temas con significados, fundamentando nuestro análisis al inferir en las “relaciones entre un índice del mensaje y una o varias variables del locutor (o de la situación comunicativa)” (Bardin, 2016, p. 145).Un principio es evitar que los conceptos teóricos existentes se sobrepongan al análisis, para identificar y desenvolver nuevos conceptos y teorías. Los corpus siguen la codificación inductiva, lo que significa que el sistema de las categorías no fue suministrado. La codificación inductiva “permite la elaboración de deducciones específicas sobre un acontecimiento o una variable de inferencia precisa y no en inferencias generalizadas” (Bardin, 2016, p. 145). En el recorrido de datos brutos a estructurados, se busca identificar índices invisibles. Sirviendo de soporte a los objetivos del estudio y abriendo la posibilidad de tratar nuevos conocimientos. La exploración realizada a través de la codificación y triangulación de los resultados constituyeron las unidades de registros de nuestra categorización.

[5] Los datos personales colectados en los cuestionarios (del tipo cualitativo y preguntas abiertas) y entrevistas (por medo de un balotario de preguntas abiertas, del tipo cualitativa e individual) fueron realizados vía online, teniendo la autorización de los entrevistados y respondientes para su tratamiento. Las providencias para la protección de los datos personales, siguen los requisitos de la Ley 13.709/2018 LGPD, en el Brasil. El guion de las entrevistas y cuestionarios están disponibilizadas en el anexo IV.

3. Análisis y tratamiento cuantitativo de los *corpus*

Son diversos los análisis realizados, por medio de la observación, la frecuencia y las relaciones existentes de los elementos de mensaje. Apoyados en la exploración y del método estadístico computacional, para la obtención de datos descriptivos, un primer paso, fue analizar la frecuencia de palabras de los corpus comparándolas entre sí, observando características similares. Seguidamente, analizamos las combinaciones de palabras. En este tipo de análisis, encontramos ciertos indicios, visualizando los temas y palabras claves que son discutidos en los documentos. Otro análisis, es el mapa de códigos, donde identificamos las relaciones directas e indirectas entre los códigos, sea individual y conjunta. Las relaciones entre códigos son determinadas por su proximidad en un mismo documento, donde las líneas de color gris y la longitud de la línea representa la frecuencia.

Figura2. Mapa de códigos (Frecuencia mínima=5, Clúster=5, distancia máxima= 3 párrafos)



Fuente: Elaboración propia.
Nota: Códigos del Aspectos Geopolítico y Diplomático (Corpus: Argentina y Perú)

Al finalizar la categorización observamos similitudes en los corpus de Argentina y Perú. Sin embargo, existen ligeros rasgos cuantitativos diferenciales. Por ejemplo, el Aspecto Socioeconómico y Comercio (ASC) es más relevante para el caso peruano con relación al

argentino, existiendo más segmentos codificados. En la Tabla 2, se observan los 7 aspectos y sus categorías temáticas. La síntesis de los reflejos observados, son obtenidas a través de la visualización, descripción sistematizada e inferencias aplicadas a los corpus. Permitiendo una comprensión comparativa y cualitativa que denominaremos de panorama actual. Estos resultados superan la incerteza y enriquecen de temáticas, que no eran fácilmente perceptibles en los corpus:

Tabla 2. Aspectos y categorías temáticas de los países estudiados

Aspectos	Estudio de caso: Brasil	Estudio de caso: Argentina y Perú
	Categorías temáticas	Categorías temáticas
AAR	Monitoramiento y prevención en seguridad	Vigilancia y control de los individuos
	Preocupación nacional e impacto en la sociedad	Factores de preocupación e impacto nacional en la sociedad
	Amenazas, riesgos y problemas de interés nacional	Amenazas, riesgos y problemas del interés nacional
	Actividades de inteligencia como instrumento de control	Las actividades de inteligencia como instrumento de control
ACR	Superposición de actividades de SI y la comunicación y ciberseguridad	Actividades sobrepuestas de la SI y la ciberseguridad
	Ejercicio de Seguridad Nacional y Defensa	Ejercicio en el rol de la defensa nacional
	Capacidades, coordinación y competencias nacionales	Desarrollo de capacidades y competencias institucionales
APD	Naturaleza y atributo del poder estatal	Naturalidad y atributo del poder estatal
	Agentes nacionales de seguridad interna	Actores de la seguridad interna nacional
	Organizaciones y asuntos internacionales de influencia	Organizaciones y asuntos internacionales de influencia
	Actuación en los ámbitos regulatorio, judicial y sancionador	Actuación en el ámbito regulador, judicial y de sanción
AGD	Acuerdos diplomáticos y de relaciones exteriores	Acuerdos de diplomacia y relaciones exteriores
	Factores de preocupación e impacto geopolítico y geoeconómico	Factores de preocupación e impacto geopolítico y geoeconómico
ASO	Factores y elementos que intervienen en la globalización	Firma digital en la identificación de personas
	Formación profesional y recursos	Modelo de gestión y supervisión de la red pública
	Gobierno y gestión de la información gubernamental	Protección de la privacidad y libre expresión
	Red pública	Formación y tecnificación del recurso humano de la red pública
	Identificación de personas en digital	Gobierno y gestión de la información gubernamental

	Impulso del gobierno electrónico en la gestión pública	Participación de los actores públicos, privados y sociedad
	Impulso del desarrollo, el progreso y el bienestar	Impulsar el motor de desarrollo, progreso y bienestar nacional
	Instrumentalización de las políticas públicas en la articulación nacional	Transformación y reforma de la estructura pública
	Participación de actores públicos, privados y de la sociedad	Impulso del gobierno electrónico en la gestión pública
	Protección de la privacidad y la libertad de expresión	Factores y elementos involucrados en la globalización
	Transformación y modernización de la estructura pública	Instrumentar las políticas públicas para su articulación estatal
ASC	Comercio	Integración del aparato económico, financiero y productivo
	Economía y finanzas	
	Mercado	
ATI	Elementos estructurales en la creación del ciberespacio	La concepción de la tecnología en el contexto internacional
	Innovación tecnológica	
	Desarrollo e innovación	
	Propiedad intelectual	
	Industria cibernética	Elementos estructurales en la creación del ciberespacio
	Cooperación internacional	
	Escenario internacional	
	Universo conectado y seguro	

Fuente: Elaboración propia.

Con el apoyo computacional realizamos un abordaje cuantitativo, en la frecuencia de los elementos del mensaje y de sus relaciones. En donde los segmentos codificados agrupados por aspectos resulto lo siguiente: ASO (41,6%), ACR (23,5%), APD (12,9%), ATI (8,7%), AAR (8,6%), ASC (2,8%) y AGD (1,9%). Este análisis puede ser ahondado a nivel de la coexistencia de los códigos en un segmento. Sin embargo, todos los análisis realizados no están descritos en el artículo. Todos esos análisis permitieron comprender e indagar en temáticas tratadas en la SegCiber de los países estudiados, complementando al análisis cualitativo y teórico.

Tabla 3. Síntesis cuantitativa de los reflejos observados entre los corpus

Asuntos	Argentina	Perú	Brasil
Códigos con mayor frecuencia	- Personas y organizaciones. - Seguridad de la información. - Sector público. - Prevención, detección, respuesta y recuperación. - Atribuir responsabilidad. - Ministerio de	- Personas y organizaciones. - Capacidades. - Normas jurídicas, marcos regulatorios, estándares y protocolos. - Atribuir responsabilidad. - Gobierno digital y electrónico. - Redes, sistemas de información y telecomunicaciones.	- Seguridad cibernética. - Internet. - SI y comunicaciones. - Inteligencia. - Economía e financiero. - Riesgos.

	modernización.		
Relaciones y conexiones de los códigos	El código “personas y organizaciones” ocupan una posición central y de conexión con los otros grupos de códigos. Sin embargo, tiene mayor aproximación con las temáticas desarrolladas en la SI, ciberseguridad, amenazas, incidentes, regulaciones y los riesgos. Otra característica fue que las “capacidades” están relacionadas en mayor ponderación al ámbito de la defensa y de las fuerzas armadas.	Las relaciones de los códigos “Capacidades” y “Atribuir responsabilidad” constituyen un mismo grupo, poseen menor ponderación en el ámbito de la defensa y de las fuerzas armadas. Sin embargo, esas capacidades son concentradas en el ámbito de las personas y de otras entidades públicas.	Las relaciones y conexiones del código SegCiber con el grupo que trata de las preocupaciones de los riesgos, de la SI y de la comunicación e IC nacionales son próximas. Sin embargo, la SegCiber tiene relaciones y conexiones menos intensas con el grupo que concentra los tópicos económico y financiero.
Análisis de las intersecciones de los códigos	El ASO, por medio de los códigos: - Internet y banda ancha. - Personas y organizaciones. - Sociedad. - Tecnologías de la información y las comunicaciones (TIC). Posee el mayor número de intersecciones con otros aspectos. En forma similar, es con el ATI, por medio del único código: Redes, sistemas de información y telecomunicaciones.	36 de los códigos del ASO posee el mayor número das intersecciones con respecto a los demás aspectos. Existen códigos de otras categorías que poseen más de dos intersecciones, siendo el caso del AGD por medio de sus códigos: “Fenómenos” y “Control de recursos naturales y estratégicos”.	El ACR, por medio del código actividades sobrepuestas de Seguridad de la Información y la Comunicación (SIC) y SegCiber, poseen el mayor número de las intersecciones respecto a las otras categorías. Existen códigos, de otros aspectos que poseen intersecciones significativas: - Participación de los actores públicos, privados y sociedad. - Amenazas, riesgos y problema de interés nacional. - Gobierno y gestión de la información gubernamental. - Factores de preocupación e impacto geopolítico y geoeconómico. - Instrumentalizar las políticas públicas en la articulación nacional.
Inferencias del análisis de frecuencias	Los códigos “Personas y organizaciones” y “Seguridad de la información” poseen 224 y 185 segmentos codificados respectivamente. Inferimos que el caso busca atender criterios o necesidades	Los códigos “Personas y organizaciones” y “Capacidades” poseen la mayor frecuencia en los segmentos codificados (485 y 217, respectivamente). Tópicos como: gobierno digital y electrónico, normas jurídicas, marcos regulatorios, estándares y	Los códigos de mayor frecuencia son: SegCiber e Internet, ambos poseen 372 segmentos codificados. Sin embargo, códigos como: SI y comunicaciones, inteligencia, economía y financiero siguen en la lista. Podemos inferir que el ACR es motivado por las actividades sobrepuestas

	relacionadas a las personas y organizaciones para los fines de la política de la SI. Para el Estado argentino, son de mayor relevancia, en sus pretensiones las acciones relacionadas a las capacidades y respuestas nacionales en SegCiber.	protocolos, también, poseen una mayor frecuencia en el corpus analizado. Inferimos en el caso, que las capacidades buscan atender a los criterios y necesidades relacionadas a las personas y organizaciones a través de los objetivos de las políticas y estrategias del gobierno digital y electrónico, teniendo como principal actor a la Secretaria de Gobierno y Transformación Digital da Presidencia de Consejo de Ministros (SegDi).	entre la SIC y la SegCiber, teniendo en el Gabinete de Seguridad Institucional de la Presidencia de la República (GSI) como su principal actor. Además, el ASO, tiene su mayor esfuerzo en la búsqueda de la participación de los actores públicos, privados y sociedad. Sin embargo, sus esfuerzos están en instrumentalizar las políticas públicas en la articulación nacional y las preocupaciones del gobierno y gestión de la información gubernamental.
Análisis a los cuestionarios semi-estructurados	El ASO posee el mayor porcentaje, en las respuestas de los expertos. Los códigos más discutidos son los siguientes: (1) Gobierno y gestión de la información gubernamental. (2) Instrumentar las políticas públicas para su articulación estatal. (3) Formación y tecnificación del recurso humano de la red pública.	El ASO posee el mayor porcentaje, en las respuestas de los expertos. Los códigos más discutidos son los siguientes: (1) Gobierno y gestión de la información gubernamental. (2) Impulsar el gobierno electrónico en la gestión pública. (3) Instrumentar las políticas públicas para su articulación estatal.	El ASO posee el mayor porcentaje en las respuestas de los expertos. Los códigos más discutidos son los siguientes: (1) Instrumentar las políticas públicas para su articulación estatal. (2) Participación de los actores públicos, privados y sociedad. (3) Gobierno y gestión de la información gubernamental.
Ranking de las categorías en los cuestionarios semi-estructurados	ASO(45,2%)	ASO(47,7%)	ASO(39,5%)
	ACR(15,4%)	ACR(16,7%)	ACR(18,1%)
	APD(12%)	AAR(11,8%)	APD(14,1%)
	AAR(12%)	APD(10,8%)	AAR(11,6%)
	ATI(8,2%)	ATI(7,4%)	ATI(9,8%)
	AGD(3,8%)	AGD(3,1%)	ASC(3,5%)
	ASC(3,4%)	ASC(2,5%)	AGD(3,3%)

Fuente: Elaboración propia.

4. Análisis y tratamiento cualitativo de los corpus

Seguidamente, describiremos los resultados e interpretaciones del análisis de contenidos e instrumentos de investigación. Sustentados en el análisis categorial y de las relaciones, las explicaciones provisorias, son resultado del análisis reflexivo. No buscamos proponer un modelo porque deben ser consideradas las idiosincrasias y el contexto inherente de cada estudio de caso. No obstante, apoya al Estado del Arte, de donde inferimos que el panorama de las configuraciones de las políticas y estrategias de la seguridad y defensa cibernética de los países estudiados tratan de7 aspectos.

Tabla 4. Explicaciones provisorias del Estado del Arte

Aspectos	Explicaciones provisorias	Notas analíticas preliminares
AAR	La estrategia cibernética exige coordinación e integración con el sistema de inteligencia. Debiendo disponer de un soporte legislativo y judicial.	En situaciones de cibercrisis nacional, el sistema de inteligencia coordina, monitorea y comunica el escenario situacional cibernético.
	Las ciberestrategias nacionales buscan proteger de las amenazas y del espionaje global en todos sus niveles.	Protección de amenazas y espionaje global (inteligencia de amenazas).
	La estrategia cibernética está dirigida principalmente a proteger las IC nacionales.	Priorización en la protección en los sistemas de los sectores más críticos del país.
ACR	La estrategia cibernética orienta la creación de capacidades cibernéticas en los diferentes sectores del sistema nacional.	Creación de cibercapacidades en el sistema nacional.
	Internet y el ciberespacio están en el control e interés de los mecanismos de defensa y seguridad nacional.	Ejercicio en el control de la Internet y del ciberespacio, a través del mecanismo de defensa y seguridad nacional.
	Las ciberestrategias nacionales justifican la carrera de cibermilitarización y ciberarmas para la defensa del ciberespacio e Internet.	Carrera de militarización y armas en el ciberespacio.
	La protección del ciberespacio aumenta la seguridad, reduce las amenazas y los riesgos en la sociedad de la información.	Protección del ciberespacio.
	Las estrategias en el ciberespacio tienen su mayor capacidad en las fuerzas armadas. Actuando en la ofensiva orientada a los intereses y objetivos estratégicos nacionales, como entidad segregada, independiente y autónoma.	Las operaciones en la ofensiva cibernética tienen en las fuerzas armadas su mayor capacidad e independencia en otros sectores, que también, están actuando en seguridad y defensa cibernética.
APD	El ciberespacio y el Internet son instrumentos de interconexión global y globalizadora.	Interconexión e instrumentos globalizadores.
	La estrategia de ciberseguridad apoyará la influencia de la expansión y dominación nacional.	Influencia de la expansión y dominación.
	La política de ciberseguridad y sus estrategias tienen como prioridad a la seguridad nacional. Deben estar alineados y subordinados al sistema de defensa y seguridad nacional.	Protección de la Seguridad Nacional.
	La estrategia nacional cibernética busca regular o sancionar las acciones cibernéticas que puedan atentar contra los intereses nacionales.	Sanciona las acciones cibernéticas que ponen en peligro los intereses nacionales.
AGD	Para el fortalecimiento de la estrategia nacional cibernética se necesita de los otros sistemas nacionales, de aliados y socios estratégicos.	Integración a otros sistemas nacionales, aliados y socios estratégicos.
	El ciberpoder nacional se estructura sobre la base del incremento y gestión centralizada del ciberespacio y los principios de la gobernanza del Internet.	Gobernanza centralizada del ciberespacio a través de los principios del Internet: libre acceso, interoperabilidad, confiabilidad y seguridad.
ASO	La estructura burocrática en los sectores es elevada y compleja, la política y los programas en ciberseguridad deben estar adecuadamente definidos para cada uno de los sectores y sus necesidades. El nivel de madurez del control interno se convierte en un facilitador para que la política sea implementada.	Las política y programas de ciberseguridad deben contar con mecanismos de control interno y facilitadores para su adecuada implementación, superando la burocracia y el accionar tecnicista de las agencias y sectores.
	La política de ciberseguridad complementa a la ley de transparencia y de reforma del sistema nacional en TIC. Podría decirse que tiene características que lo convierten en un indexador gubernamental y facilitador de cambios sectoriales.	La política de ciberseguridad promueve e incentiva otras leyes como la creación de reformas en otros sectores del sistema nacional.
	La estrategia en defensa y SegCiber orienta a tener en los componentes nacionales una estructura de gobierno de la información y procesos de mando y control.	Gobernanza de las informaciones para la toma de decisiones.
	La política cibernética nacional es un instrumento que promueve la integración de los componentes del sistema nacional, coordinando y priorizando responsabilidades	Ejercicio en el control del ciberespacio a través del mecanismo de defensa y seguridad nacional.

	entre el mecanismo de gobierno y el sector privado. Siendo el sector de la seguridad interna el principal responsable de estas integraciones, aunque el sector de defensa ejercerá el liderazgo y la conducción con los demás componentes en situaciones de crisis o emergencias nacionales.	
	El ciberespacio, al igual que Internet, es de interés geopolítico y de seguridad internacional, configurando nuevas relaciones de poder y priorización económica en los actores.	Valoración geopolítica y económica.
	Las estrategias nacionales en el ecosistema cibernético promueven la creación de un ambiente de prosperidad y desarrollo en la sociedad y los sujetos informacionales.	Prosperidad y desarrollo en la sociedad.
ASC	La política de ciberseguridad fomenta el consumo nacional de las TIC, buscando la concienciación de su dependencia tecnológica.	Consumo de tecnología nacional y conciencia de dependencia tecnológica.
	El ciberespacio es altamente complejo con grandes inversiones en seguridad. Desde la perspectiva de costo y efectividad, los programas en seguridad y defensa cibernética orientan centralmente, en la ejecución de esfuerzos conjuntos, en busca de una optimización de costos y beneficios.	Elevadas inversiones y muy complejo para poder ser securizado.
	La política de ciberseguridad promueve la economía y el mercado digital, convirtiéndose en un pilar del ecosistema digital nacional.	Ecosistema digital, mercado y economía digital.
ATI	El impulso de las ciber industrias, en conjunto con la investigación, el desarrollo e innovación (I+D+i) son factor prioritario en las estrategias nacionales de seguridad y defensa cibernética.	Promoción e impulso de la innovación, los estándares y las industrias TIC.
	La estrategia de ciberseguridad hace de las empresas nacionales, sean públicas o privadas, un instrumento de ciber poder con la finalidad de poseer una hegemonía político-tecnológica.	Sirve como instrumento de poder y de hegemonía política-tecnológica.
	La política y estrategias de ciberseguridad promoverán la innovación tecnológica con un enfoque estratégico en incrementar el acceso a Internet y banda ancha nacional.	Las naciones industrializadas modernas promueven el acceso a Internet y la conectividad.

Fuente: Elaboración propia.

Como proceso de validarlas inferencias y conceptos teóricos, observamos características relevantes en los códigos y categorías temáticas, desvelándolas intenciones de los documentos.

Tabla 5. Relevancia e influencia de las categorías temática y códigos estudiados

Corpus	Aspecto	Categorías temáticas y códigos	
		De mayor influencia	De menor influencia
Argentina	AAR	Amenazas, riesgos y problemas del interés nacional	Vigilancia y control de los individuos
Brasil			Monitoramiento y prevención en seguridad
Perú			Vigilancia y control de los individuos
Argentina	ACR	Actividades sobrepuestas de la SI y la ciberseguridad	Desarrollar capacidades y competencias institucionales
Brasil			Capacidades, articulación y competencias nacionales
Perú			Desarrollar capacidades y competencias institucionales
Argentina	APD	Actuación en el ámbito regulador, judicial y de sanción	Actores de la seguridad interna nacional.

Brasil		Naturaleza y atributo del poder estatal	
Perú		Actuación en el ámbito regulador, judicial y de sanción	
Argentina	AGD	Factores de preocupación e impacto geopolítico y geoeconómico	Acuerdos de la diplomacia y relaciones exteriores
Brasil			
Perú			
Argentina	ASO	Participación de los actores públicos, privados y sociedad	Modelo de gestión y supervisión de la red pública
Brasil			Identificación de personas en lo digital.
Perú		Impulsar el gobierno electrónico en la gestión pública	Modelo de gestión y supervisión de la red pública
Argentina	ASC	Integración del aparato económico, financiero y productivo	Economía digital
Brasil		Economía y financiero	Comercio
Perú		Integración del aparato económico, financiero y productivo	Economía digital
Argentina	ATI	Elementos estructurales en la creación del ciberespacio	La concepción de la tecnología en el contexto internacional
Brasil			Universo conectado y seguro
Perú			La concepción de la tecnología en el contexto internacional

Fuente: Elaboración propia.

A pesar de los resultados cuantitativos son reveladores, con estas dos fuentes de evidencias: entrevistas y cuestionarios, buscamos otorgar mayor robustez y confiabilidad al estudio. Seguidamente, presentamos la síntesis de los reflejos observados:

Tabla 6. Reflejos observados del análisis cualitativo en las entrevistas y cuestionarios

Aspectos	Finalidad de la pregunta	Reflejos observados
AAR	Identificar los actores involucrados en las estrategias en seguridad y defensa cibernética.	(1) En las prioridades de la seguridad y defensa cibernética están las IC nacionales. (2) Los actores en la gobernanza de Los riesgos cibernéticos, poco maduros con esfuerzos individualistas por la falta de una coordinación y visión holística. (3) Entre las amenazas que podrían originar una ciber crisis nacional están las que afectarían directamente a las IC nacionales. Sin embargo, se destacan también las operaciones de desinformación e influencia con fines políticos e ideológicos.
ACR	Identificar los actores involucrados en las estrategias en seguridad y defensa cibernética.	(1) En las estrategias y acciones del nivel político-estratégico se busca tener capacidades cibernéticas para el desarrollo industrial nacional, en contraste al consumo y dependencia tecnológica. (2) Como desafíos y capacidades cibernéticas, está en disponer del presupuesto y cualificación del recurso humano, siendo difícil la sustentación de la capacidad operacional del recurso humano en el sector estatal. (3) En tecnologías como Internet y del ciberespacio está en garantizar el acceso al servicio de Internet.
APD	Analizar los elementos que	(1) En la expansión y dominación por medio de las TIC, es aceptado e inevitable siendo establecida una dependencia tecnológica.

	constituyen una política de SegCiber.	(2) Sanciones justificadas en la seguridad y defensa cibernética nacional, no se han reportado casos de este tipo.
AGD	Analizar la geopolítica en el ámbito cibernético y sus repercusiones en la consolidación de las políticas y estrategias en SegCiber.	(1) Tímida injerencia de la ciber diplomacia nacional, a pesar de existir casos de espionaje a secretos nacionales por parte de otros países. (2) Poca clareza de la entidad responsable, en el ámbito ciberespacial, de la coordinación de la geoestrategia nacional.
ASO	Comprender que actores y elementos constituyen una política de SegCiber, en el ámbito sociocultural e institucional.	(1) La política nacional en SegCiber ha generado cambios y reformas institucionales. (2) Es difícil apreciar los beneficios de la SegCiber para la prosperidad, desarrollo e inclusión de la sociedad.
ASC	Comprender que agentes y elementos constituyen una política de SegCiber, en el ámbito socioeconómico y de mercado	(1) En el consumo nacional de TIC existen esfuerzos pocos maduros y superficiales. (2) En el ámbito de los programas en SegCiber de crear esfuerzos multisectoriales, no existen indicadores de efectividad o de monitoramiento de las inversiones de implementación de esos programas. (3) En el impulso de la economía y mercado digital nacional existen limitaciones en poseer estrategias integrales que no se vean influenciadas a las ideologías políticas.
ATI	Comprender que actores y elementos constituyen una política de SegCiber, en el ámbito tecnológico e industrial.	(1) Necesidad de capacitar a la entidad pública para la regulación y definición de estándares en TIC, bien como de los mecanismos para evaluar su cumplimiento. (2) No se dispone de una normatividad o entidad responsable que trate discusiones de empresas multinacionales en el marco de la SegCiber nacional. (3) En el incentivo de la competición de Proveedores de Servicios de Internet (ISP), el acceso al Internet es una preocupación en la agenda del Estado.

Fuente: Elaboración propia.

5. Informe de casos cruzados

En las dos últimas décadas, Sudamérica es una región sin incidencias de conflictos internacionales, sin embargo, son afectados por la inestabilidad política, el crimen organizado, los conflictos sociales y de violencia interna; complicando la consolidación de sus sistemas democráticos. La sociedad y la economía en los países estudiados son asediadas por la corrupción, la influencia del crimen global y de los grupos de poder empresarial. Como diagnóstico, inferimos que los métodos utilizados en el análisis de las capacidades de la SegCiber, han incentivado medidas y acciones estratégicas que no son transversales y multisectoriales a las problemáticas y amenazas vigentes de estos países. Poseen acciones desposeídas del tratamiento social y cualitativa, desde la perspectiva socioeconómica, geopolítica y cultural. En el análisis cuantitativo, observamos que los objetivos de la SegCiber están orientados en atender

a las personas (sujetos informacionales)y organizaciones estatales (dispositivos informacionales), motivados en el gobierno electrónico y digital, destacando el *Aspecto sociocultural y organizativo*. En la perspectiva de la ciencia de la información, se percibe que la información activada en el interior del dispositivo delineará un tipo de conocimiento, poder y de sujetos sometidos a los contextos sociales, políticos y económicos. En el caso argentino, evidenciamos que las capacidades cibernéticas son ponderadas desde sus fuerzas armadas y la defensa. En el caso peruano son intensificadas en los individuos y agentes públicos. En el caso brasilero difiere de los otros casos, porque está orientado en atender a las entidades de la Administración Pública Federal, a través de la SIC, sobresaliendo el *Aspecto de las Capacidades y Respuestas*. Por consiguiente, los resultados al compararlos con los análisis realizados en los cuestionarios y entrevistas, el *Aspecto Sociocultural y Organizacional*es relevante en las discusiones y preocupaciones de los expertos, con tópicos como el gobierno y la gestión de la información gubernamental y la articulación de las políticas públicas en el Estado. También, se observa que el *Aspecto Geopolítico y Diplomático*es de menor interés. Por esa razón, la generalización de las amenazas y el ligero tratamiento de los riesgos en el método, donde no son consideradas, variables como: el contexto geopolítico, cultural, social y económico; pueden inducir a errores o falsa sensación de capacidades cibernéticas nacionales. Estas capacidades deben garantizar el equilibrio de la dependencia político-tecnológica, la sustentación de la capacidad operacional y la calidad de las instituciones. Finalmente, lo descrito corresponde al análisis del contenido, complementada con las entrevistas y cuestionarios individuales. Resaltamos que pueden existir elementos de influencia, isomorfismo institucional o político, adopción de acuerdos o tratados internacionales, entre otros. Por ello, este estudio no busca responder a las causas y efectos de los eventos sociales relacionados a la SegCiber en los 3 países estudiados.

6. Desarrollo de las implicaciones teóricas

La metodología utilizada al correlacionarla con la dinámica informacional de los 6 fatores posibilita la comprensión de los elementos, agentes y relaciones de influencia concebidas en las políticas y estrategias de la SegCiber. Subvencionando al estudio nuestras implicaciones teóricas y de contribución en las estrategias de laSegCiber, siendo las siguientes:

Factores 4 y 6: El nexo de la información y la cibernética a través de la esfera política se establece mediante su inclusión en la intervención estatal, como parte de sus capacidades de ciberseguridad y de SI. Más allá de una dimensión administrativa, debe ser considerado como un factor estratégico de desarrollo científico-tecnológico. Lo expresado constituye un nuevo modelo de soberanía donde el Estado actúa como agente en el ciclo de vida de la información,

generando una doble representación de su intervención en los dominios territorial, social y simbólico. En donde el meta capital de un Estado moderno está compuesto por el capital de fuerza física, el capital económico y el capital de la información y del conocimiento. Así, el Estado podrá asegurar su influencia y poder sobre otros campos de la actividad y de la formación del capital social, industrial y financiero, entre otros.

Factor 5: La política nacional de SegCiber debe ser diseñada y dirigida desde una perspectiva holística y multisectorial, a través del sistema de planificación estratégica nacional. Este dispositivo debe ser responsable de la coordinación entre los ministerios y los niveles de gobierno. Por tanto, las estrategias en el campo de la seguridad y defensa cibernética deben estar alineadas con los intereses nacionales para asegurar el progreso sostenible y el logro del bienestar nacional. En resumen, la SegCiber no debe estar sujeta al principio de representación de la sociedad, ha de ejercerse desde la perspectiva del proyecto social, respetando los parámetros del orden social, pero aspirando a transformaciones fundamentales del orden económico, prescindiendo de intereses y deseos de la sociedad civil.

Factores 3 y 4: Tomar conciencia de la evolución histórica, causalidad social y estructural subyacente a la compleja interrelación existente en: economía, tecnología, sociedad y política. En otras palabras, los procesos de desarrollo económico y transformación estructural deben estar integrados en instituciones, culturalmente orientadas y consensuadas socialmente. A través de las políticas y estrategias comerciales, tecnológicas e de incentivos a la exportación nacional.

Factores 4 y 6: Debido a la pluralidad de saberes especializados y jerarquizados, en el ámbito de la SegCiber y de la información, se inserta el saber y la ciencia como principio de acreditación y cualificación, en relación con los nuevos medios de civilización y producción. Los 3 países estudiados, nunca alcanzarían su plena realización, si están sujetos a una modernización subalterna y conservadora. Habiendo innumerables escenarios, como el patrimonialismo y la privatización clientelar de lo público, convergencia tecnológica y económica, la ausencia de lo común y de la propia voluntad, la ausencia de reglas y estándares sociales reconocidos y aceptados por los sujetos en el proceso de la comunicación en red, entre otros. Constituyendo una omisión o desintegración de normas sociales y de segregación socioeconómica, siendo a la vez síntoma del régimen informacional presente en el Estado y en la sociedad, así como de las condiciones políticas de gobernanza de la información.

Factores 1, 4 y 6: Para disponer de las capacidades cibernéticas que garanticen el equilibrio de la dependencia tecnológica, deben ser articulados 3 ministerios claves: El sector de economía y finanzas, para incentivar las inversiones y créditos en exportaciones e importaciones, apoyando así el desarrollo científico y tecnológico de las empresas nacionales.

El sector de infraestructura y telecomunicaciones, para otorgar las condiciones materiales de producción y organización selectiva en la difusión de las TIC en el sector público e industrial local. El sector educativo, para preservar la identidad cultural y organizacional del sistema de estratificación y movilidad social. Ejerciendo un estricto control de la meritocracia en la contratación de altos cargos, en las instituciones del Estado. Así como, en el mantenimiento de la operatividad del talento humano y su adecuada distribución en los sectores de sus competencias profesionales.

Factores 2, 3, 5 y 6: Reconstruir las relaciones de Estado, sociedad y economía. Buscando condiciones de adaptabilidad y flexibilidad en las políticas y en las empresas, con relación a la demanda del mercado internacional. En estas relaciones, el Estado es el centro de la experiencia de la economía digital, brindando los incentivos necesarios para atraer capital extranjero, creando infraestructura industrial y de comunicaciones, que apoyen a las exportaciones de la industria tecnológica, favoreciendo a la ciencia y la tecnología, para el mejoramiento e innovación de los productos y servicios del Estado, en consecuencia, de la industria nacional. Con un Ministerio de Educación empoderado y articulador, para que la información y la investigación de las universidades e institutos técnicos puedan dialogar y ser aplicables a las demandas del mercado.

Factores 3 y 5: Promover la combinación flexible de redes centralizadas de Pequeñas y Medianas Empresas (PYME) que actúan como subcontratistas en empresas fabricantes de TIC. El Estado debe desarrollar una estructura industrial que permita la interconexión de las PYME con empresas especializadas en canalizar la exportación e importación de productos y servicios. Como resultado, se debe disponer de un sistema de bibliotecas digitales y de información, donde se brinden programas de capacitación, servicios de consultoría y tecnología, colaboración y producción técnico-científica, así como una red de seguridad para reducir el riesgo empresarial.

Factor 4: Fomentar estrategias de seguridad y defensa cibernética, frente a la dependencia de las multinacionales extranjeras que operan en el ámbito de las TIC. Sin desalentar los procesos de la globalización y estando a la expectativa de los fenómenos provocados por las asimetrías de la información existente; entre los objetivos de la ciberseguridad y las TI, que se han entrelazado completamente con la investigación, el desarrollo y la innovación. La relevancia de los centros de investigación, las empresas y los mercados prometen la integración de un país a las redes tecnológicas dominantes, así como una mejor evaluación de las necesidades estratégicas y el conocimiento de la información.

Factores 1, 2 y 5: La Política Nacional de SegCiber no debe ser ajena a las iniciativas multilaterales en materia de relaciones exteriores y diplomacia. A tales efectos, la institución habilitada debe incentivar los grupos de expertos militares, civiles y de la comunidad científico-

académica especializada, para la elaboración de estudios desde una perspectiva geopolítica y geoeconómica en el ámbito del ciberespacio.

Factores 1, 2, 4 y 5: Una forma de neutralizar los efectos y mitigar las intervenciones de los países hegemónicos que pretenden desestabilizar el bloque Sudamericano, sea en el ámbito sociopolítico como geoeconómico. Los tres países estudiados deben conformar un Estado-Núcleo (Huntington, 2010) y a través de los mecanismos del Consejo de Defensa Suramericano (CDS) deben ser acordadas políticas y estrategias en materia de seguridad y defensa, priorizándose los siguientes temas: (1) La hegemonía de influencia político-tecnológica occidental y asiática en el bloque Sudamericano. (2) Industrialización y producción de tecnologías emergentes en la región. (3) La ciberdiplomacia y la cibercoerción en los intereses nacionales y tecnológicos de los países Sudamericanos.

Factores 1, 2 y 6: Para una efectiva gobernanza de la SegCiber, se debe designar a la institución responsable de la coordinación nacional. Este articulador debe tener autonomía, recursos y un rol normativo en el espacio cibernético del país, trabajando estrechamente con el sistema de inteligencia nacional. Es de considerar que las operaciones de las empresas en un mercado autorregulado, sin lineamientos claros y sin control, pueden ser destructivas. En principio, cuando se permite que las empresas operen libres de leyes y regulación, sin la capacidad de equilibrar las asimetrías existentes, se pueden generar vicios y problemas en el ámbito social, económico y político.

Factores 2 y 6: La capacidad de los países desarrollados para adaptarse al paradigma de la información y cambios en la economía global a través de la modernización tecnológica, la expansión del mercado y la diversificación económica. Se fomenta, en principio, en el proceso de toma de decisiones de los distintos niveles de gobierno de un Estado. Se debe crear conciencia de la existencia de vicios y problemas de un Estado que afectan en el alcance de los intereses y objetivos de la ciberseguridad. La búsqueda de la desburocratización en la gestión económica, a través de estímulos a la productividad y resultados por parte de las instituciones de planificación estratégica, con la inserción de controles que permitan el seguimiento y rendición de cuentas de los resultados en las instituciones a través de las TI y la automatización, siempre que sean cumplidos los principios de transparencia, eficiencia y eficacia.

7. Conclusiones

La metodología, los instrumentos de investigación y el recurso computacional, facilitaron la organización, el tratamiento y la visualización del análisis y comprensión de los datos. El análisis de contenido computacional facilitó la comprensión de los *corpus* y de sus características inherentes en el proceso de la codificación inductiva. Brindando insumos en las

explicaciones provisorias y de sus categorías no obvias a principio. Fue primordial la exploración y dominio del marco teórico en los múltiples análisis, para organizar las categorías temáticas y luego agruparlas en 7 aspectos. El presente estudio permite visualizar las relaciones existentes de los códigos y las categorías temáticas, apoyándonos en comprender fenómenos ocultos y pocos conocidos para el investigador. Por ejemplo, visualizamos las relaciones indirectas de los códigos y sus elementos satélites que se influencian en otros códigos y categorías. Amplificando la concepción de las categorías, reforzando la re-teorización en la investigación. De donde concluimos que elASO es relevante para los fines de la política y estrategias de la SegCiberen Argentina, Perú y Brasil. Por tanto, se recomienda que los 7aspectosestudiadosestén adheridos en la elaboración de las capacidades cibernéticas nacionales, buscando su implementación en las estrategias multisectoriales de la SegCiber de los países sudamericanos. El presente estudio buscó fortalecer nuestras inferencias, enriqueciendo e innovando la investigación como un todo. De cara a futuros trabajos, será interesante realizar un estudio de casos múltiplos donde sean estudiados todos los países sudamericanos a partir de los 7 aspectos, para luego compararlos entre ellos.

Referencias:

Aluísio, Sandra M.; Barcellos, Gladis M. O que é e como se constrói um corpus? Lições aprendidas na compilação de vários corpora para pesquisa linguística. **Calidoscópio,** v. 4,n. 3, p. 156-178, 2006. Disponible en: http://revistas.unisinos.br/index.php/calidoscopio/article/view/6002Acceso en: 18 abr. 2022.

Bauer, Martin W.; Gaskell, George. **Pesquisa qualitativa com texto, imagem e som**: um manual prático. Petrópolis: Vozes, 2019.

Bardin, Laurence. **Análise de Conteúdo**. São Paulo: Edições 70, 2016.

Castells, Manuel (2018).**La era de la información, fin de milenio**.Madrid:Alianza Editorial, 2018. v.3.

CEPAL **Estudio económico de América Latina y el Caribe**. Principales condicionantes de las políticas fiscal y monetaria em la era pospandemia de COVID-19". Santiago, 2020. Disponible en: https://repositorio.cepal.org/bitstream/handle/11362/46070/89/S2000371_es.pdfAcceso en: 20 mar. 2022.

CCDCOE. **Strategy-and-governance**. 2022. Disponible en:<https://ccdcoe.org/library/strategy-and-governance/>. Acceso en: 01 de abr. de 2022.

Dunn, Myriam; Egloff, Floriam. The Politics of Cybersecurity: Balancing Different Roles of the State. **St Antony's International Review,** v**.** 15, n. 1, p.37-57, 2019. Disponível em:<https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-

studies/pdfs/Dunn_Cavelty_Egloff_2019%20STAIR%20Issue%2015.1.pdf>. Acesso em 26 jun. 2020.

Foucault, Michel. **Nascimento da Biopolítica**. São Paulo: Edições 70,2020.

González de Gómez, Maria Nélida. Regime de Informação:Construção de um Conceito. **Informação& Sociedade: Estudos**, João Pessoa, v.22, n.3, p. 43-60, set./dez. 2012. Disponível em:< https://www.brapci.inf.br/_repositorio/2015/12/pdf_3c42553162_0000011948.pdf>. Acesso em: 22 de ago. 2021.

Huntington, Samuel P. **O choque de civilizações e a recomposição da ordem mundial**. Rio de Janeiro: Objetiva, 2010.

Junta Interamericana de Defensa. **Ciberdefensa**. 26 de marzo de 2023. Disponível em:<https://www.jid.org/ciberdefensa-2/>. Acesso em: 26 abr. 2023.

Kramer, Franklin D.; Starr, Stuart H.; Wentz, Larry K. **Cyberpower and National Security**. Center Technology and National security Policy. Washington, April 2009.

Maia Guimarães Gesteira, L. A. A Guerra Fria e as ditaduras militares na América do Sul. **Scientia Plena**, v. 10, n. 12, 2014 Disponível em:<https://scientiaplena.emnuvens.com.br/sp/article/view/2062>. Acesso em: 26 abr. 2023.

Nascimento, L. C. N.; Souza,Tania Vignuda de; Oliveira, Isabel Cristina dos Santos; Moraes, Juliana Rezende Montenegro Medeiros de; Aguiar, Rosane Cordeiro Burla de; Silva, Liliane Faria da. Theoretical saturation in qualitative research: an experience report in interview with schoolchildren. **Revista Brasileira de Enfermagem**, v. 71, n. 1, p. 228-33, 2018 Disponible en: <http://dx.doi.org/10.1590/0034-7167-2016-0616>. Acceso en: 26 abr. 2023.

Nasser, Salem. **Relatório da CIA**: a nova era. São Paulo: Geração Editorial, 2019.

ONU. **Developments in the field of information and telecommunications in the context of international security**. [1998?]. Disponible en <https://www.un.org/disarmament/ict-security/>. Acceso en: 26 mar. 2023.

Preciado, Jaime A.; UC, Pablo. **América Latina frente a China y Estados Unidos**: triangulación geopolítica del sistema-mundo. El pensamiento latinoamericano: Diálogos en ALAS. 2015. ISBN-13: 9789877230567. Disponible en <https://www.teseopress.com/dialogosenalas/chapter/america-latina-frente-a-china-y-estados-unidos-triangulacion-geopolitica-del-sistema-mundo-2/>. Acceso en: 01 oct. 2023.

Laville, Christian; Dionne, Jean. **A construção do saber.Manual de Metodologia da Pesquisa em Ciências Humanas.** Porto Alegre: Artes Médicas/Belo Horizonte: Editora UFMG, 1999.

Rädiker, Stefan; Kuckartz, Udo. **Análisis de datos cualitativos con MAXQDA**: 2020.Texto, Audio, Video.

MAXQDA Press, Berlin, 1st edition. Disponible en:<https://www.maxqda-press.com/catalog/books/analisis-de-datos-cualitativos-con-maxqda>. Acceso en: 20 mar. 2022.

Romero, Oscar Jorge Jr. Telecomunicaciones y dependencia en América Latina: retos para la integración autónoma. **Controversias y Concurrencias Latinoamericanas**, v. 11, n. 19, p. 137-155, 2019. Disponible en: <https://www.redalyc.org/journal/5886/588661549008/html/>. Acceso en: 16 abr. 2022.

Voss, C.; N. Tsikriktsis e M. Frohlich. Case research in operations management. **International Journal of Operations & Production Management**, v. 22, n. 2, p. 195-219, 2022.

World Economic Forum. **The Global Risks Report 2023 18th Edition**. Geneva. Disponible en: https://www.weforum.org/reports/global-risks-report-2023.2023.Acceso en: 16 abr. 2022.

Yin, Robert K. **Estudo de caso: planejamento e métodos.** 2. ed. Porto Alegre: Bookman, 2001.

Zuboff, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020.