ISSN: 2237-826X
ARTÍCULO | PAPER

Estudio de caso de la Seguridad Cibernética Peruana: un panorama de sus configuraciones políticas y estratégicas

Case study of Peruvian Cyber Security: an overview of its political and strategic configurations

Arthur Christian Huamani Cuba [1], Maria Aparecida Moura [2]

[1] *Universidade Federal de Minas Gerais (UFMG), Belo Horizonte, Minas Gerais, Brasil. ORCID: https://orcid.org/0000-0002-3118-7889*

[2] *Universidade Federal de Minas Gerais (UFMG), Belo Horizonte, Minas Gerais, Brasil. ORCID: https://orcid.org/0000-0003-2670-923X*

Correo a/*Mail to:* Arthur Christian Huamani Cuba, arthur.huamani@opendeusto.es

Recibido/*Submitted*: 23 de junho de 2024; **Aceptado/*Approved*:** 8 de agosto de 2024

Resumen

Introducción: Este estudio, en el ámbito político-estratégico, busca comprender los aspectos que se consolidan en el panorama de las configuraciones políticas y estratégicas de la seguridad cibernética peruana, asimismo, los elementos y agentes influenciados. **Método:** Desde las directrices de la investigación cualitativa, la metodología de investigación aplicada fue el estudio de caso y el análisis de contenido, habiendo analizado por medio del software MAXQDA: 36 documentos oficiales digitalizados, 02 entrevistas y 07 cuestionarios semiestructurados - individuales a expertos peruanos del sector público, privado y académico. **Resultados:** Desde el enfoque de las ciencias sociales, analizamos las relaciones de los elementos y agentes concebidos en las iniciativas de la seguridad cibernética peruana. Se examinaron las repercusiones existentes a través del análisis temático y de las particularidades geopolíticas, geoeconómicas y sociocultural. Por tanto, el estudio fortalece la comprensión de fenómenos complejos, que no eran evidentes en el corpus estudiado, como parte del proceso metodológico ampliamos nuestra concepción de 07 aspectos, observando que el "Aspecto Sociocultural y Organizacional" es la más relevante para los fines de la política y las estrategias de la seguridad cibernética peruana. **Conclusión:** El estudio permitió construir diversos tipos de análisis que facilitaron la visualización de los códigos y categorías temáticas, que, sumado a la base conceptual y de las teorías del tema; ofrecieron implicaciones teóricas, amplificando para el caso peruano, la concepción de sus políticas y estrategias en seguridad cibernética.

Palabras clave: Ciberseguridad; Ciberdefensa; Política de Seguridad Cibernética; Capacidad Cibernética.

Abstract

Introduction: *This study, in the political-strategic field, seeks to understand the aspects that are consolidated in the panorama of political and strategic configurations, of Peruvian cyber security, as well as the elements and agents influenced.* ***Method:*** *From the guidelines of qualitative research, the applied research methodology was the case study and content analysis, having analyzed through the MAXQDA software: 36 digitalized official documents, 02 interviews and 07 semi-structured questionnaires - individual to Peruvian experts from the public, private and academic sectors.* ***Results:*** *From the social sciences approach, we analyze the relationships of the elements and agents conceived in the Peruvian cyber security initiatives. Examining the existing repercussions through thematic analysis and geopolitical, geoeconomic and sociocultural particularities. Therefore, the study strengthens the understanding of complex phenomena, which were not evident in the corpus studied. As part of the methodological process, we expanded our conception of 07 aspects. Noting that the "Sociocultural and Organizational Aspect" is the most relevant for the purposes of Peruvian cybersecurity policy and strategies.* ***Conclusions:*** *The study allowed the construction of various types of analysis that facilitated the visualization of the codes and thematic categories, which added to the conceptual base and the theories of the subject; The theoretical implications were offered, amplifying for the Peruvian case, the conception of its policies and strategies in cyber security.*

Keywords: *Cybersecurity; Cyber defense; Cybersecurity Policy; Cyber Capacity.*

INTRODUCCIÓN

Estudios indican que las confrontaciones geoeconómicas estarán en la categoría de riesgos graves para los próximos diez años. No obstante, la desigualdad digital y fallas de seguridad cibernética (SegCiber) estarán dentro de los riesgos de corto y medio plazo (World Economic Forum (WEF), 2022). La adopción del ciberespacio en los procesos de producción y cadenas de suministro ha impactado en las actividades socioeconómicas, de seguridad, de creación de oportunidades en innovación y bienestar social (Mbanaso & Dandaura, 2015). Sin embargo, existen discrepancias y desinterés, principalmente en países hegemónicos, para unificar esfuerzos y disponer de un contrato social global, en la dimensión ciberespacial. Siendo testigos de la intensificada competencia en nuevas tecnologías y geografías, evidenciando una militarización y desarrollo de armas ciberespaciales. "La competencia geopolítica alimenta la militarización del espacio, lo que aumenta los incentivos estatales para diseñar estrategias de espionaje cibernético, interferencia y ataque contra las operaciones espaciales de los rivales" (Fidler, 2018).

En las últimas dos décadas, hemos observado en los países suramericanos que sus amenazas a la seguridad nacional tratan de problemas sociales de orden transnacional, como la corrupción, desigualdad social, narcotráfico, inestabilidad política, etc. Según Castells (2018, p. 241) una gran parte de los países de América Latina están envolvidos en agitaciones y crisis causadas por la conexión entre el crimen organizado y la política. Por tanto,

un hipotético conflicto cibernético entre los países suramericanos es menos prioritarias, empero, la dependencia digital, la desinformación, los *Fake News*, entre otros problemas; vienen impactando en la fragilidad de sus sistemas democráticos y en la desconfianza de autoridades e instituciones.

Otra perspectiva son los limitados recursos y la producción tecnológica, teniendo como hipótesis que las amenazas y necesidades de la seguridad y defensa cibernética Suramericana divergen de los países que disponen de una hegemonía político-tecnológica como son Estados Unidos, Rusia y China.

Estudios y lecturas previas

Por ser un estudio poco explorado, existen un número limitado de publicaciones referentes al grupo social de la SegCiber peruana. No obstante, existen estudios realizados por la International Telecommunication Union (ITU), que buscan identificar el estado de la ciberseguridad, en base al índice de ciberseguridad global (International Telecommunication Union (ITU), 2021). Otros estudios referentes al contexto peruano, son del Banco Interamericano de Desarrollo (BID) y del Centro de Capacidad de Seguridad Cibernética Global (GCSCC) de la universidad de Oxford, que viene aplicando sus estudios en los países miembros de la Organización de Estados Americanos (Banco Interamericano de Desarrollo (BID) & Organización de los Estados Americanos (OEA), 2020).

METODOLOGÍA

Enfoque de la investigación

Buscando contribuir en el análisis crítico de los elementos y agentes inmersos en las políticas y estrategias de la SegCiber[1] peruana. La colecta documental (Corpus) y teórica ha tenido el objetivo de comprender aspectos relacionados con el fenómeno social complejo de la SegCiber peruana. La estrategia de investigación sigue los métodos del estudio de caso y del análisis de contenido, conjuntamente, con instrumentos, como entrevistas y cuestionarios individuales del tipo semiestructurados.

> La investigación de estudio de caso sería el método preferencial en comparación a los otros en situaciones en las cuales las principales preguntas de investigación son ¿cómo? o ¿Por qué?; un investigador tiene poco o ningún control sobre eventos comportamentales; y el foco de estudio es un fenómeno contemporáneo (en vez de un fenómeno completamente histórico) (Yin, 2001, p. 2).

> ¿Qué es el análisis de contenido actualmente? Un conjunto de instrumentos metodológicos cada vez más sutiles en constante perfeccionamiento, que se aplica a los discursos (contenido y continentes) extremamente diversificados. El factor común de esas técnicas múltiples y multiplicadas -desde el cálculo de frecuencias que suministra datos cifrados, hasta la traducción de estructuras traducidas en modelos- es una hermenéutica controlada, con base en la deducción: la inferencia. En cuanto esfuerzo de interpretación, el análisis de contenido oscila entre dos polos del rigor de la objetividad y de la fecundidad de la subjetividad. Bardin (2016, p. 15).

Debido a las diversas fuentes de pruebas utilizadas en este estudio, sea desde datos de observación directa, entrevistas, cuestionarios, investigaciones en documentos públicos y privados (Voss, Tsikriktsis, & Frohlich, 2002), fuimos motivados a realizar el estudio de caso peruano.

> 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. Esto terminaría requiriendo, sucesivamente, un número inconcebiblemente grande de casos, demasiado grande para permitir cualquier evaluación estadística de las variables 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).

Para subsidiar nuestro objetivo de investigación utilizamos el *software* MAXQDA en el análisis de los datos cualitativos, a través de la visualización y descripción sistematizada. Apoyados en la investigación cualitativa social, analizamos varias fuentes de información lo que permitió la triangulación de los datos: (1) 36 documentos digitales públicos de Perú (dominios.gob.pe). (2) 08 cuestionarios y 02 entrevistas, individuales a los expertos del sector público, privado y académico en el Perú. El balotario de preguntas abiertas fue elaborado con base a los aspectos e hipótesis del Estado del Arte (Tabla 2).

Los expertos fueron elegidos en base a sus conocimientos, experiencia y actuación directa con el tema de la ciberseguridad peruana. En su mayoría, los expertos peruanos han ejercido un rol fundamental, sea en el ejercicio del cargo público, bien como, el haber participado en el planeamiento de los proyectos de la ciberseguridad peruana.

[1]Esta investigación trata los términos de seguridad cibernética (SegCiber), ciberseguridad y seguridad digital, dentro de una misma definición.

Como parte de la planificación realizamos un pretest a un entrevistado y respondiente respectivamente, para identificar imprecisiones discursivas, errores gramaticales, errores técnicos, complejidad, preguntas desnecesarias, oprobio y agotamiento del participante. Todas las respuestas de los participantes fueron en español.

Identificador	Institución	Cargo	Modalidad
Entrevistado_Peru_1	Ministério de Transporte y Comunicaciones (MTC)	Regulación y Asuntos Internacionales de Comunicaciones	Videoconferencia
Entrevistado_Peru_2	Ministério de Transporte y Comunicaciones (MTC)	Regulación y Asuntos Internacionales de Comunicaciones	Videoconferencia
Respondiente_Peru_1	Ministério del Interior (MININTER)	Dirección General de Inteligencia	Formulario online
Respondiente_Peru_2	Smart Regulation Perú	Consultor Asociado	Formulario online
Respondiente_Peru_3	Organismo Supervisor de la Inversión en Energía y Minería (OSINERGMIN)	Gerencia de Sistemas y Tecnologías de la Información	Formulario online
Respondiente_Peru_4	Superintendencia Nacional de Migraciones	Jefatura de Plataforma y Seguridad Tecnológica	Formulario online
Respondiente_Peru_5	Secretaria de Gobierno y Transformación Digital (SEGDI)	Consultor	Formulario online
Respondiente_Peru_6	Presidencia del Consejo de Ministros (PCM)	Especialista en Análisis Político	Formulario online
Respondiente_Peru_7	Grupo Falabella	Gerencia corporativa de Proyectos de Ciberseguridad	Formulario online
Respondiente_Peru_8	Ministerio de Desarrollo e Inclusión Social	Consultor senior TIC	Formulario online

Tabla 1. Expertos del sector público, privado y académico en el Perú que participarón de la investigación

Un delimitador es no ahondar en fenómenos que respondan a causas y efectos sociales, presentes en las iniciativas de la SegCiber peruana. Además, la colecta documental se limitó al estudio de la SegCiber en el nivel político-estratégico, debido a que las informaciones de este sector son secretas o de clasificación reservada, entendiéndose que buscar estudiar todos los niveles conjuntamente, podríamos correr el riesgo de generalizar los resultados, cayendo en una falsa noción de unidad, y del tratamiento del problema. Sin embargo, para disponer de una perspectiva del panorama peruano, buscaremos comprender los elementos, agentes y relaciones que se influencian en la política y estrategias de la SegCiber peruana.

Organización del análisis y característica del corpus de estudio

Durante el proceso de organización documental, los 36 documentos (en *Portable Document Format* -PDF) que constituyen el corpus documental, fueron etiquetados en grupos temáticos: (1) Leyes y Regulaciones Nacionales (LRN), con 13 documentos. (2) Política y Líneas de Acción Estratégica (PLA), con 18 documentos. (3) Publicaciones del Departamento de Defensa (PDD), con 5 documentos.

Los documentos colectados fueron publicados entre enero del año 2000 y setiembre del 2020. Después de la colecta, seguimos con la técnica del análisis del contenido a través del *software* MAXQDA, pre analizando los documentos, realizando una exploración sistemática de los documentos (Bardin, 2016, p. 126). Consiguiendo observar indicios temáticos y de contexto, como resultado de la selección de las unidades de análisis, conocidas también de unidades de significado. Elegimos el software MAXQDA porque facilita el análisis de los datos recopilados para una investigación social empírica. La característica central del software es trabajar con subcódigos, códigos y categorías. Los códigos son atribuidos en partes seleccionadas del contenido del documento digitalizado, desde palabras, párrafos de texto, en imágenes, videos y audios. Según Bardin (2016), "La codificación es el proceso por el cual los datos en bruto se transforman sistemáticamente y se agregan en unidades, lo que permite una descripción precisa de las características pertinentes del contenido". Para esta investigación, las operaciones de codificación inductiva fueron exploradas hasta llegar a la saturación teórica. 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 la codificación inductiva, el sistema de códigos y categorías no son suministrados, siendo un recorrido de datos brutos a datos estructurados u organizados, siendo identificados índices invisibles a partir de los datos brutos. El esfuerzo inductivo de la codificación evita que conceptos teóricos existentes puedan sobreponerse al análisis, posibilitando desarrollar nuevos conceptos y

teorías. "Este análisis permite la elaboración de deducciones específicas sobre un acontecimiento o una variable de inferencia precisa y no en inferencias generales" (Bardin, 2016, p. 145). Además, "se considera saturada la colecta de datos cuando ningún nuevo elemento es encontrado y el incremento de nuevas informaciones deja de ser necesario, pues no altera la comprensión del fenómeno estudiado" (Nascimento et al., 2018, p. 244).

Por otra parte, el agrupamiento de los subcódigos a códigos, para luego, esos grupos de códigos con base a sus similitudes y relaciones caracterizarán en la creación de las categorías. De forma que las categorías abarcan un número variable de temas con significados, que al ser analizadas permitirán tener una aproximación sistemática en el desarrollo teórico e identificación de las temáticas en el corpus estudiado. Para Bardin (2016), las categorías "son rubricas o clases, las cuales reúnen un grupo de elementos (unidades de registro, en el caso de análisis de contenido) sobre un título genérico, ese agrupamiento es debido a características comunes de los elementos". Por tanto, las categorías temáticas, sirven para estructurar el contenido, señalando una temática o tema de un texto (Rädiker & Kuckartz, 2020) y las notas analíticas preliminares contienen las notas de los investigadores, como la descripción o uso de las categorías, siendo esos hallazgos importantes en los documentos explorados (Rädiker & Kuckartz, 2020).

En síntesis, con la metodología propuesta realizamos un abordaje cuantitativo y cualitativo de los elementos del mensaje y de sus relaciones. Sin embargo, no todos los análisis realizados por los investigadores serán detallados. A través del análisis de contenido pudimos comprender e indagar los tópicos tratados en el corpus estudiado, que sumado a los reflejos observados complementaron al referencial teórico, atendiendo al fortalecimiento de las categorías y de la verificación de las hipótesis provisorias durante el análisis cualitativo.

Selección del estudio de caso peruano

En el Perú no encontramos una Política de Estado en Seguridad Cibernética. Existen leyes, reglamentaciones y normativas que buscan atender la problemática. En el ámbito de las Telecomunicaciones e Internet, las inversiones y los ingresos operativos en el sector de telecomunicaciones crecieron un 3,1% y 9,7% en el año 2021 y 2022, respectivamente (OSIPTEL, 2023b). Sin embargo, se tiene un 54% de reclamos debido a problemas con el servicio móvil, con 53,2% en el canal telefónico (OSIPTEL, 2023a). Estando el sector de las telecomunicaciones dominada por la inversión privada de empresas extranjeras.

> En 1994, el gobierno peruano privatizó la Compañía Peruana de Teléfonos (CPT) encargada de brindar los servicios de telefonía básica en Lima y la Empresa Nacional de Telecomunicaciones (ENTEL), proveedor de los servicios de larga distancia nacional e internacional y telefonía local, y que se extendió hasta noviembre de 1999 (Rozas Balbontín, 2003, p. 44).

Por tanto, es observada la dependencia privada e internacional en el Perú, como en la región suramericana, pudiendo ser un factor de amenaza desde la perspectiva de la SegCiber, en donde un hipotético atentado o conflicto internacional dejarían vulnerables en cuanto al secreto de los datos oficiales y militares, por ello (Zibechi, 2012).

> La ausencia de conexiones directas entre la mayoría de los países latinoamericanos genera "un recorrido exótico e irracional. Un mail enviado entre dos ciudades limítrofes de Brasil y Perú, por ejemplo, entre Rio Branco, capital de Acre, y Puerto Maldonado, va hasta Brasilia, sale por Fortaleza en cable submarino, ingresa a Estados Unidos por Miami, llega a California para descender por el Pacífico hasta Lima y seguir viaje hasta Puerto Maldonado (Romero, 2019, p. 143).

En el año 2000, surgen las primeras iniciativas en ciberseguridad a través de la Ley N° 27291 al modificar el código civil, permitiendo el uso de medios electrónicos en la manifestación de voluntad y de la firma electrónica. En el 2003, se crea el Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) siendo parte de sus líneas de acción y de atención a la mejora de la calidad de los servicios públicos, a la seguridad de la información (SI). Luego después es creada la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) y el PeCERT en los años de 2005 y 2009 respectivamente. Posteriormente, son desarrolladas múltiples estrategias, planes y agendas principalmente en el ámbito del gobierno electrónico. Es en 2012, con la creación de la Secretaria de Defensa Nacional (SEDENA) en la Presidencia de Consejo de Ministros (PCM) que la ciberseguridad tomó un nuevo interés nacional, en donde son tratados las primeras definiciones de la ciberseguridad en el nivel político-estratégico, articulando 3 objetivos: defensa nacional, orden interno y acciones de desarrollo. En 2016, se dieron cambios institucionales, donde la SEDENA y el Centro de Altos Estudios Nacionales (CAEN) son adheridas al Ministerio de Defensa (MINDEF). Durante los siguientes años la ciberseguridad en el Perú fue intensificada desde una perspectiva legal. Siendo confirmado, en el estudio de la ITU (2021, p.67) en donde el Perú tiene como fortalezas el aspecto legal y jurídico, sin embargo, es deficiente en el aspecto de desarrollo de otras capacidades.

En el ámbito internacional, en el 2018 se dio la salida del Perú de la Unión de Naciones Suramericanas (UNASUR) viéndose afectados los intentos de desarticulación de las asimetrías existentes en las infraestructuras de telecomunicaciones y de la promoción de políticas de desarrollo inclusivas (Romero, 2019).

> Es necesario acompañar las políticas de infraestructura con políticas que promuevan la competencia dentro de la industria de telecomunicaciones en cada Estado, que incentiven la creación de servicios y contenidos propios que puedan competir con los productos y servicios estadounidenses. El anillo de fibra óptica no es el único caso en el que un modelo de integración regional es utilizado para impulsar este tipo de desarrollo (Romero, 2019, p. 147).

Los investigadores optamos, como estrategia de investigación, tener un Estado del Arte. Asistiéndonos de base, los estudios y lecturas previas realizadas en documentos públicos de la seguridad y defensa cibernética norteamericana, por las siguientes razones: (1) Amplio volumen de publicaciones disponibles en los sites institucionales estadounidenses; (2) Posee hegemonía política, militar y tecnológica; (3) Posee los mayores ciber ejércitos con capacidades cibernéticas globales; (4) El departamento de defensa y la academia norteamericana contribuyeron al desarrollo del Internet y de otras tecnologías disruptivas y su (5) Influencia geopolítica y tecnológica ejercida en Suramérica. Asimismo, la exploración temática realizada en los documentos estadounidenses, permitió tener en consideración siete aspectos de análisis y de sus respectivas hipótesis provisorias. Con la intención de observar los diferentes fenómenos a partir de ángulos distintos y que serán probados en el abordaje de nuestro estudio de caso peruano.

Aspectos	Hipótesis provisorias	Código	Notas Analíticas preliminares
AAR	La estrategia cibernética requiere coordinación e integración con el sistema de inteligencia y debe contar con apoyo legislativo y judicial.	Comunidad de inteligencia	En situaciones de crisis cibernética, el sistema de inteligencia coordina, monitorea y comunica el escenario situacional cibernético nacional.
AAR	Las estrategias a nivel cibernético nacional buscan proteger de las amenazas y el espionaje global en todos los niveles de operación.	Amenazas y riesgos nacionales	Protección de amenazas y espionaje global (inteligencia de amenazas).
AAR	La estrategia cibernética como prioridad la protección de las infraestructuras críticas nacionales, desde el ámbito interno y externo.	Priorización de protecciones	Priorización de la protección en los sistemas de los sectores más críticos del país.
ACR	La estrategia cibernética guía en la creación de capacidades cibernéticas a los diversos sectores del sistema nacional.	Capacidades cibernéticas	Creación de capacidades cibernéticas en el sistema nacional.
ACR	Internet, como el ciberespacio, está en el control e interés del mecanismo de defensa y seguridad nacional.	Ciberdefensa	Ejercicio del control en el ciberespacio por el mecanismo de defensa y seguridad nacional.
ACR	Las estrategias cibernéticas nacionales justifican la carrera de ciber militarización y ciberarmas para la defensa del ciberespacio e Internet.	Armas cibernéticas	Carrera de militarización y armas en el ciberespacio.
ACR	La protección del ciberespacio aumenta la seguridad, reduce las amenazas y los riesgos en la sociedad de la información.	Ciberseguridad	Protección del ciberespacio.
ACR	Las estrategias militares en el ciberespacio dotan a las fuerzas armadas de su mayor capacidad, actuando en la ofensiva orientada a los intereses y objetivos estratégicos nacionales como entidad segregada, independiente y autónoma.	Capacidades ofensivas	Las operaciones en la ciber ofensiva, tiene en las fuerzas armadas su mayor capacidad e independencia de otros sectores, que también están actuando en ciberseguridad y defensa.
APD	El ciberespacio como Internet, son instrumentos de interconexión global y globalizadora.	Conectividad global	Instrumentos de interconexión y globalización.
APD	La estrategia de ciberseguridad apoyará la influencia de la expansión y dominación nacional.	Influencia de expansión y dominación	Influencia de expansión y de dominación.

Aspectos	Hipótesis provisorias	Código	Notas Analíticas preliminares
APD	La política de ciberseguridad y sus estrategias priorizan la seguridad nacional. Deben estar alineados y subordinados al sistema de defensa y seguridad nacional.	Protección nacional	Protección de la Seguridad Nacional.
APD	La estrategia cibernética nacional busca regular y castigar las acciones cibernéticas que pueden afectar a los intereses nacionales.	Regulaciones y sanciones	Castigar las acciones cibernéticas que pongan en peligro los intereses nacionales.
AGD	Para fortalecer la estrategia cibernética nacional, se necesitan otros sistemas nacionales, sus aliados y socios estratégicos.	Socios cibernéticos	Integración en otros sistemas nacionales, aliados y socios estratégicos.
AGD	El ciberpoder nacional se estructura sobre la base del aumento y la gestión centralizada del ciberespacio y los principios de la gobernanza de Internet.	Gobernanza de Internet	Gobernanza centralizada del ciberespacio a través de los principios de Internet: libre acceso, interoperabilidad, fiable y seguro.
ASO	La estructura de la burocracia en los sectores es alta y compleja, la política y los programas en ciberseguridad, deben definirse adecuadamente para cada uno de los sectores y sus necesidades. El nivel de madurez del control interno se convierte en un facilitador para la política a implementar.	La burocracia es vasta y complicada	Las políticas y programas de ciberseguridad deben contar con mecanismos de control interno y facilitadores para su correcta implementación, superando la burocracia y desencadenando la acción técnica de las agencias y sectores.
ASO	La política de ciberseguridad complementa a la Ley de transparencia y reforma del sistema nacional de TIC. Se puede decir que tiene características que lo convierten en un indexador gubernamental y facilitador de cambios sectoriales.	Transparencia y reformas gubernamentales	La política de ciberseguridad promueve y fomenta otras Leyes como la creación de reformas en los demás sectores del sistema nacional.
ASO	La estrategia en defensa y ciberseguridad guía a tener en los componentes nacionales una estructura de gobierno de la información y procesos de mando y control.	Gobierno de la información	Gobierno de la información para la toma de decisiones.
ASO	La política cibernética nacional es un instrumento que promueve la integración de los demás componentes del sistema nacional, coordinando y priorizando responsabilidades entre el mecanismo del gobierno y el sector privado. El sector de seguridad interna es el principal responsable de estas integraciones, aunque el sector de defensa es el que ejercerá liderazgo y conducta con los demás componentes en situaciones de crisis de emergencia nacional.	Componente integral de todos los sectores	Ejercer control en el ciberespacio, a través del mecanismo de defensa y seguridad nacional.
ASO	El ciberespacio, como Internet, es de interés geopolítico y de seguridad internacional, configurando nuevas relaciones de poder y priorización económica en los actores.	Interés y prioridades nacionales	Valor geopolítico y económico.

Aspectos	Hipótesis provisorias	Código	Notas Analíticas preliminares
ASO	Las estrategias nacionales en el ecosistema cibernético promueven la creación de un entorno de prosperidad y desarrollo en la sociedad y en temas informativos.	Prosperidad y desarrollo	Prosperidad e desarrollo en la Sociedad.
ASC	La política de ciberseguridad fomenta el consumo de las tecnologías nacionales de la información y la comunicación, buscando la conciencia de su dependencia tecnológica.	Compra centralizada	Consumo de tecnología nacional y conciencia de la dependencia tecnológica.
ASC	El ciberespacio es altamente complejo con grandes inversiones en seguridad, desde la perspectiva de costo y efectividad, los programas en ciberseguridad y defensa guían centralmente la efectividad de los esfuerzos conjuntos en busca de una optimización de costos y beneficios.	Rentabilidad	Altas inversiones y demasiado complejas para poder ser securizado.
ASC	La política de ciberseguridad promueve la economía y el mercado digital, convirtiéndose en un pilar del ecosistema digital nacional.	Economía y mercados digitales	Ecosistema digital, mercado y economía digital.
ATI	El impulso de las industrias cibernéticas, junto con la investigación, el desarrollo y la innovación, son un factor prioritario en las estrategias nacionales de ciberseguridad y defensa.	Industrias cibernéticas	Promover e impulsar la innovación, las normas y las industrias en las TIC.
ATI	La estrategia de ciberseguridad convierte a las empresas nacionales, ya sean públicas o privadas, en un instrumento de ciberpoder con el propósito de poseer una hegemonía político-tecnológica.	Hegemonía	Sirve como instrumento de poder y hegemonía político-tecnológica.
ATI	La política y las estrategias en ciberseguridad promoverán la innovación tecnológica con un enfoque estratégico en el aumento del acceso a Internet y la banda ancha nacional.	Enfoque estratégico en Internet	Las naciones industrializadas modernas promueven el acceso a Internet y la conectividad.

Tabla 2. Aspectos e hipótesis provisorias que constituyen el Estado del Arte

La estrategia descrita permitió dilucidar conceptos y desarrollar líneas relevantes a las interrogantes con relación al estudio de caso peruano. Permitiéndonos cubrir aspectos substantivos cuanto metodológicos, observando experimentalmente diversos abordajes e *insights* de asuntos teóricos. Buscando reflejar en el estudio, aspectos teóricos-políticos como asuntos relevantes con la seguridad cibernética contemporánea.

Estudio de caso peruano

Análisis y tratamiento cuantitativo

Con MAXQDA fueron posibilitados diversos tipos de análisis a través de la observación, la frecuencia y las relaciones existentes entre los elementos del mensaje (subcódigos y códigos) de forma individual y conjunta. Otro análisis relevante fue el mapa de códigos, donde analizamos las relaciones entre los códigos.

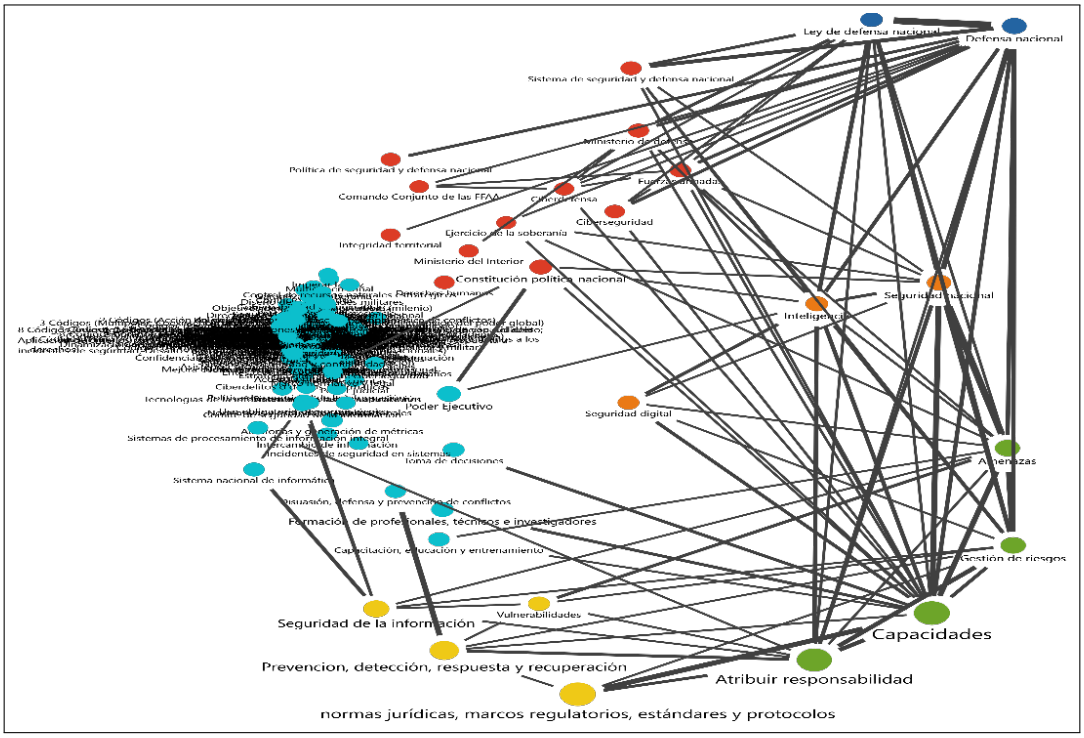

Figura 1. Mapa de códigos en el estudio de caso peruano (agrupados en 6 *clústers*)

En la Figura 1, observamos la intersección de los códigos en un segmento. Las relaciones son representadas con líneas grises, cuyo ancho representa la frecuencia, agrupados en seis *clusters* por el color de los nodos. Aplicando la exploración y el método estadístico al corpus peruano, analizamos la frecuencia y combinaciones de las palabras. Una de las combinaciones fue de 2 para 2 palabras, resultando la siguiente frecuencia: datos personales (20,83%), gobierno digital (7,47%), administración pública (6,79%) y gobierno electrónico (6,07%). Donde los datos personales poseen la mayor relevancia, siendo más evidente al analizar la frecuencia de los códigos, en donde el código: personas y organizaciones (con 485 segmentos codificados), tienen la mayor frecuencia; seguido del código: capacidades (con 217 segmentos codificados). Por tanto, podemos sugerir que la búsqueda de capacidades en el caso peruano es atender a criterios y necesidades de las personas y organizaciones, a través de los objetivos de las políticas y estrategias del gobierno digital y electrónico, con su principal actor en la Secretaria de Gobierno y Transformación Digital (SEGDI). Lo sugerido se corresponde con el análisis de nube de códigos, donde los códigos de mayor frecuencia poseen mayor tamaño, siendo la frecuencia mínima: 5 y de 168 códigos exhibidos (Figura 2).

Tabela de referência cruzada

	Questionario_Peru_1	Questionario_Peru_2	Questionario_Peru_3	Questionario_Peru_4	Questionario_Peru_5	Questionario_Peru_6	Questionario_Peru_7	Questionario_Peru_8	Total
Aspecto tecnológico e industrial	2.6%	17.6%			13.6%	5.9%	7.5%	9.1%	7.4%
Aspecto socioeconómico y comercio	7.9%				3.4%	2.0%	3.0%		2.5%
Aspecto sociocultural y organizacional	34.2%	29.4%	63.4%	72.7%	45.8%	39.2%	52.2%	63.6%	47.7%
Aspecto geopolítico y diplomático	7.9%	2.9%			1.7%	5.9%	3.0%		3.1%
Aspecto del poder y dominación	13.2%	5.9%	19.5%		11.9%	11.8%	9.0%	9.1%	10.8%
Aspecto de las capacidades y respuesta	23.7%	29.4%	12.2%	22.7%	13.6%	13.7%	11.9%	18.2%	16.7%
Aspecto de las amenazas y riesgos	10.5%	14.7%	4.9%	4.5%	10.2%	21.6%	13.4%		11.8%
SOMA	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
N = Documentos	1 (12.5%)	1 (12.5%)	1 (12.5%)	1 (12.5%)	1 (12.5%)	1 (12.5%)	1 (12.5%)	1 (12.5%)	(100.0%

Figura 2. Nube de códigos del estudio de caso peruano

Un análisis similar fue en los cuestionarios de respuestas de expertos. Comparamos las frecuencias de las categorías temáticas con la tabla de referencia cruzada (Figura 3) donde Aspecto sociocultural y organizacional (ASO) obtuvo el mayor porcentaje; los 3 códigos más relevantes de ese aspecto son los siguientes: (1) Gobierno y gestión de la información gubernamental (31 segmentos codificados). (2) Impulsar el gobierno electrónico en la gestión pública (22 segmentos codificados). (3) Instrumentar las políticas públicas para su articulación estatal (18 segmentos codificados). Por tanto, el ASO representa el 41,6% de los segmentos codificados en el estudio de caso peruano.

Figura 3. Frecuencias de los aspectos estudiados en la tabla de referencia cruzada

Análisis y tratamiento cualitativo

A continuación, describiremos de forma sistemática la aplicación del análisis de contenido y de la conducción de los instrumentos de investigación. Sin antes comentar, que todo dato personal colectado en los cuestionarios y entrevistas fueron tratados con el consentimiento de los participantes y con providencias para la protección de los datos personales, tipificadas en la Ley 13.709/2018 LGPD en el Brasil.

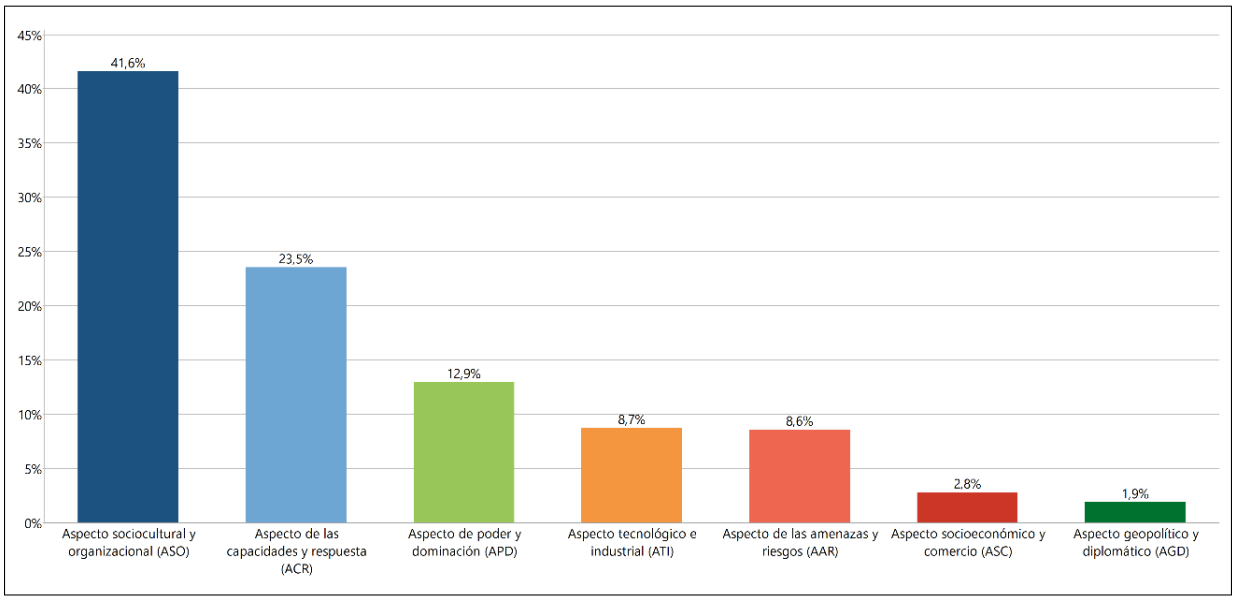

Figura 4. Aspectos del estudio de caso peruano (porcentaje de segmentos codificados)

Entiéndase al análisis cualitativo como un procedimiento intuitivo, para Bardin (2016, p. 145) "es más maleable y adaptable a los índices imprevistos, o a la evolución de hipótesis". En esta fase fueron construidas nuestras categorías que agrupan los códigos y subcódigos identificados. Con este análisis, buscamos fundamentar nuestras hipótesis 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 a considerar, es evitar que los conceptos teóricos existentes se sobrepongan al análisis, para tener la posibilidad de identificar y desenvolver nuevos conceptos y teorías. De la aplicación del análisis de contenido en el corpus peruano y apoyados del Estado del Arte (Tabla 2) evidenciamos sistemáticamente el panorama de las configuraciones políticas y estratégicas en el ámbito de la seguridad y defensa cibernética peruana (Tabla 3). Debido a la complejidad social de la SegCiber peruana, inferimos que los factores de amenazas influyen, determinan o intervienen en la problemática mínimamente en uno o más de los siete aspectos descritos. En consecuencia, un factor de amenaza son elementos, circunstancias e influencias que colaboran en la producción de un resultado. Las categorías temáticas no buscan ser un modelo porque debe tenerse en consideración las idiosincrasias y el contexto inherente por cada estudio de caso investigado.

Aspectos	Categorías temáticas	Notas Analíticas preliminares
AAR	Vigilancia y control de los individuos	Preocupación del Estado en disponer de las herramientas e instrumentos de vigilancia digital y de control informacional para prevención criminal, por medio del monitoramiento y observación de los individuos en las redes informáticas y de la comunicación.
AAR	Factores de preocupación nacional y de impacto en la sociedad	Debido al multiculturalismo, las discusiones y preocupaciones de la sociedad están centradas en las relaciones de trabajo, derechos humanos e en la sustentabilidad económica, más allá, de ser inclusivas. Busca la seguridad estratégica em la protección de los derechos esenciales del ciudadano y el intercambio de ideas y el dialogo democrático.
AAR	Amenazas, riesgos y problemas del interés nacional	Las mayores amenazas y riesgos están relacionados a la criminalidad organizada em el ambiente interno de su ciber sociedad, sin embargo, existen preocupaciones relacionadas a la complejidad, interdependencia económica y financiera, comprensión mínima de sus vulnerabilidades y dependencia en las tecnologías cibernéticas.
AAR	Actividades de inteligência como instrumento de control	En situaciones de crisis cibernéticas el sistema de inteligencia coordina, monitora y comunica el escenario situacional nacional en el ámbito cibernético, con mayor actuación en la inteligencia criminal. En otras situaciones, en la protección y clasificación del secreto militar y en el acceso de las personas autorizadas.
ACR	Actividades sobrepuestas de la seguridad de la información y la ciberseguridad	Las funciones de la seguridad de la información (SI) y ciberseguridad, son presentadas como acciones complementares, sobrepuestas en las acciones y responsabilidades por parte de los atores gubernamentales.
ACR	Ejercer el rol de la defensa nacional	El ejercicio de la defensa nacional en el uso de la fuerza y del poder militar conjunto, posee limitaciones doctrinarias, presupuestales, de recursos y de restructuración en su organización.
ACR	Desarrollar capacidades y competencias institucionales	La preocupación del Estado no sólo es poseer capacidades cibernéticas, pero también, en el desarrollo de capacidades humanas, logísticas y operacionales que le permitan articular competencias y recursos institucionales.
APD	Naturaleza y atributo del poder estatal	Poder y comportamiento del Estado: atributo del poder, naturaleza del poder, atribución de responsabilidad, paradigma.
APD	Actores de la seguridad interna nacional	Fuerzas policiales y agencias de seguridad nacional, en el ámbito de la seguridad interior.
APD	Organizaciones y asuntos internacionales de influencia	La influencia y dinámica de las organizaciones internacionales, de los acuerdos de gobernanza global y la integración de los organismos multilaterales, en los asuntos nacionales y de intereses gubernamentales.
APD	Actuación en el ámbito regulador, judicial y de sanción	Existen mecanismos que buscan regular, procesar y punir acciones y responsabilidades en las nuevas formas de crimines en el uso de las fuentes digitales abiertas y del campo tecnológico.
AGP	Acuerdos de diplomacia y relaciones exteriores	Los fenómenos que envuelven a la tecnología exigen en los países, negociaciones por medio de acuerdos de cooperación y acciones de resolución de conflictos.
AGP	Factores de preocupación e impacto geopolítico y geoeconómico	Las preocupaciones concebidas a debate por organismos internacionales o por las principales potencias mundiales tienen como características de estudio el aspecto geopolítico y geoeconómico.
ASO	Firma digital en la identificación de personas	Uso de la firma digital en ciudadanos para identificación de personas en el ámbito digital.

Aspectos	Categorías temáticas	Notas Analíticas preliminares
ASO	Modelo de gestión y supervisión de la red pública	La fiscalización de los servicios de la red pública, la celebración de contratos e integración, requieren de planeamiento y acuerdos que constituyan una estrategia y un modelo de gestión en red.
ASO	Protección de la privacidad y libre expresión	La preocupación del Estado de regular y salvaguardar la protección de la privacidad de los datos personales, como también, la libertad de expresión de sus ciudadanos.
ASO	Formación y tecnificación del recurso humano de la red pública	Una de las grandes preocupaciones del sector público, en el ámbito de las tecnologías de información y de la comunicación (TIC), es instruir, capacitar y tecnificar a sus recursos humanos en todos los niveles de gobierno. Dejando en evidencia que el foco principal de la instrucción y entrenamiento corresponde a la usabilidad y consumo de las TIC.
ASO	Gobierno y gestión de la información gubernamental	La necesidad de las entidades públicas busca establecer niveles de madurez en la gobernanza y gestión de sus informaciones.
ASO	Participación de los actores públicos, privados y sociedad	La búsqueda de unificar los esfuerzos en la seguridad y defensa nacional incentivando la integración, participación y consenso de los actores públicos, privados y sociedad.
ASO	Impulsar el motor de desarrollo, progreso y bienestar nacional	Promover el desarrollo, el progreso y el bienestar que generan impacto socioeconómico, cultural y tecnológico sobre los individuos y organizaciones nacionales.
ASO	Transformación y reforma de la estructura pública	Esfuerzos para la reforma y modernización en la gobernanza y de la gestión pública por medio de la utilización de las TIC.
ASO	Impulsar el gobierno electrónico en la gestión pública	Ejecución de las estrategias y planes en todos los niveles de gobierno, para la adopción del gobierno electrónico o digital en la prestación de servicios públicos digitales en favor de la sociedad.
ASO	Factores y elementos envolvidos en la globalización	Varios elementos están envolvidos en el fenómeno de la globalización: empresas multinacionales, ciberespacio, países en vías de desarrollo, países desarrollados. Sin embargo, existen factores comunes como la economía digital, el uso infinito de datos, pacificación y coordinación por el ciberespacio, entre otros.
ASO	Instrumentar las políticas públicas para su articulación estatal	Políticas y estrategias, en los niveles de gobierno, permite la articulación del aparato estatal en la coordinación de los esfuerzos para el acatamiento de los objetivos nacionales.
ASC	Integración del aparato económico, financiero y productivo	La preocupación del Estado en atender a las necesidades esenciales, subsidios y control, implica básicamente en la integración del sistema económico y social al del sector productivo e financeiro.
ATI	La concepción de la tecnología en el contexto internacional	Las necesidades de mudanza tecnológica en el país traen expectativas de un futuro próspero, inclusivo e de desarrollo sobre la provocación de disponer de mecanismos de cooperación internacional.
ATI	Elementos estructurales en la creación del ciberespacio	La materialización del ciberespacio se basa en la construcción de elementos como: infraestructura, datos, información, conocimiento, automación, inteligencia, conectividad global y control.

Tabla 3. Categorías temáticas del estudio de caso peruano

Seguidamente, observamos características que validan nuestras inferencias y conceptos teóricos. Por cada categoría temática existen códigos relevantes e intenciones de influencia en los documentos analizados. Evidenciando las siguientes características:

Aspectos	De mayor influencia	De menor influencia
AAR	Amenazas, riesgos y problemas del interés nacional	Vigilancia y control de los individuos
ACR	Actividades sobrepuestas de la SI y la ciberseguridad	Desarrollar capacidades y competencias institucionales
APD	Actuación en el ámbito regulador, judicial y de sanción	Actores de la seguridad interna nacional
AGD	Factores de preocupación e impacto geopolítico y geoeconómico	Acuerdos de la diplomacia y relaciones exteriores
ASO	Impulsar el gobierno electrónico en la gestión pública	Modelo de gestión y supervisión de la red pública
ASC	Integración del aparato económico, financiero y productivo	Economía digital
ATI	Elementos estructurales en la creación del ciberespacio	La concepción de la tecnología en el contexto internacional

Tabla 4. Relevancia e influencia de las categorías temáticas y los códigos

En el análisis de los cuestionarios y entrevistas, observamos ciertas semejanzas, estos reflejos observados guardan relación con los elementos y agentes influenciados en la SegCiber peruana. Los reflejos evidenciados por los expertos complementan nuestro referencial teórico y enriquecen al análisis cualitativo, fortaleciendo nuestras categorías y verificación de hipótesis provisorias.

Aspectos	Finalidad de la pregunta	Reflejos observados
AAR	Identificar los actores involucrados en las estrategias em seguridad y defensa cibernética.	(1) En las prioridades está en disponer de capacidades técnicas, así como, del fortalecimiento regulatorio y legal en el ámbito cibernético. (2) Necesidad de generar confianza digital en los ciudadanos, haciéndose necesario de una conducción estatal con autonomía para la implementación de estrategias en seguridad cibernética. Por la ausencia de un liderazgo, existen lagunas funcionales que han permitido que algunas instituciones se desentiendan de sus responsabilidades en el tema. (3) Se observa una duplicidad de funciones y competencias entre la SEGDI y el MINDEF, dándose casos, en que se dificultan las iniciativas y proyectos futuros. (4) Existe poca madurez en los esfuerzos relacionados a la gobernanza de los riesgos cibernéticos. Falta de una comprensión uniforme, entre las instituciones con relación a las amenazas que ocasionarían una crisis nacional.
ACR	Identificar los actores involucrados en las estrategias em seguridad y defensa cibernética.	(1) En las estrategias y acciones del nivel político-estratégico existe la necesidad de tener una política nacional en ciberseguridad, que fomente una objetividad en sus resultados. (2) En los desafíos y capacidades cibernéticas, está el 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 el ámbito de las capacidades humanas, para los entrevistados, el Ministerio de Educación (MINEDU) no sería una institución que pudiera liderar la gobernanza de la seguridad cibernética en el país. (4) Se deben garantizar el acceso al servicio de Internet a los lugares más remotos y el uso seguro del ciberespacio.

Aspectos	Finalidad de la pregunta	Reflejos observados
APD	Analizar los elementos que constituyen una política de SegCiber.	(1) Es aceptada la expansión y dominación de países desarrollados a través de las TIC, por ende, es inevitable la ventaja que ellos poseen, existiendo una dependencia tecnológica en el Perú. (2) Son citados, dos tipos de modelos de la vigilancia y control, una primera del modelo chino, con relación a la soberanía de los datos y la otra perspectiva, del modelo norteamericano, que es ejercido por medio de los instrumentos jurídicos y regulatorios por sus empresas multinacionales. (3) No existen precedentes de puniciones a terceros y empresas, justificadas desde el ámbito de la seguridad y defensa cibernética nacional, donde hayan sido afectados los intereses nacionales. Fue citado, por los entrevistados, del caso Ariza relacionado a la revelación de secretos nacionales y espionaje.
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) Intervencionismo por parte de entidades u organizaciones internacionales. Debido a ciertos acuerdos de libre comercio de mantener una neutralidad tecnológica, esto podría afectar a otras iniciativas y proyectos nacionales. (3) 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) Las iniciativas nacionales en seguridad cibernética han generado cambios y reformas institucionales. Se observan avances en seguridad digital, en el ámbito regulador y normativo, sin embargo, las instituciones aún poseen tecnología obsoleta y procesos pocos maduros, sin haber alcanzado niveles de automación. (2) Burocracia e ineficacia en las iniciativas de interés público, siendo aprobados decretos de urgencia, pero los esfuerzos de la aplicación de esas reformas son inconclusos, siendo dilatados, aún más, en cada cambio de gestión de gobierno. (3) Para la mayoría de los entrevistados, es difícil apreciar los beneficios de la seguridad cibernética, en favor, a la prosperidad, desarrollo e inclusión de la sociedad peruana. Comunidades remotas y rurales serían los que menos beneficiados de las iniciativas en el ámbito ciberespacial.
ASC	Comprender que agentes y elementos constituyen una política de SegCiber, en el ámbito socioeconómico y de mercado.	(1) En el consumo nacional de las Tecnologías de la Información y de la Comunicación (TIC) existen esfuerzos pocos maduros y superficiales. Las acciones e iniciativas promovidas por los gobiernos no buscan equilibrar la dependencia tecnológica externa. Los entrevistados asumen que en la Política Nacional de Ciberseguridad peruana debería incentivar el consumo tecnológico. (2) Los programas en seguridad cibernética deben crear esfuerzos multisectoriales, no existen indicadores de efectividad y de monitoramiento de las inversiones de implementación de esos programas. Las autoridades competentes, no toman seriamente las inversiones en seguridad cibernética, existiendo proyectos nacionales inconclusos como la Red Dorsal de Fibra Óptica. (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.

Aspectos	Finalidad de la pregunta	Reflejos observados
ATI	Comprender que actores y elementos constituyen una política de SegCiber, en el ámbito tecnológico e industrial.	(1) Los entrevistados coinciden en la necesidad de capacitar a la entidad pública reguladora para establecer los estándares en TIC, bien como, de los mecanismos para evaluar su cumplimiento. (2) No queda claro, cual es la entidad del Estado en ejercer la función de regular y definir los estándares en TIC. Entre las Entidades citadas están: la SEGDI, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) y Consejo Nacional de Ciencia, Tecnología e Innovación (CONCYTEC). (3) No existe la institución responsable de normar, articular y tratar discusiones relacionadas a las empresas multinacionales en el marco de la seguridad cibernética nacional. Un grupo de los entrevistados, asumen que sería el SEGDI y el MINDEF son adversos a esos temas. (4) 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 peruano. Queda en evidencia que no existe empresa pública que ofrezca esos servicios, estando todos ellos privatizados.

Tabla 5. Reflejos observados de las entrevistas y cuestionarios

Informe del estudio de caso peruano

En las últimas dos décadas, Suramérica es una de las regiones que no se han suscitado conflictos internacionales. Sin embargo, son afectados por la inestabilidad política, el crimen organizado, los conflictos sociales y violencia interna, siendo complicada la consolidación de sus sistemas democráticos. La sociedad peruana es asediada por la corrupción, la influencia del crimen global y de los grupos de poder empresarial transnacionales.

> [...]las redes ilegales más importantes que operan en el país (minería informal, tráfico ilícito de drogas, tala ilegal y trata de personas), las cuales se desarrollan en un contexto nacional en el que la corrupción es considerada uno de los principales obstáculos hacia el desarrollo. [...] por la irrupción de movimientos políticos sin bases sólidas y que apelan a liderazgos fuertemente personalistas. El tema se complica mucho más cuando, como se ha descrito, estas aventuras devienen organizaciones que terminan capturando el aparato público (Patriau, 2018, p. 344).

En el análisis del corpus documental y del contenido, observamos las relaciones directas e indirectas entre los códigos y las categorías, destacándose a nivel estratégico, que el objetivo peruano es de impulsar el gobierno electrónico y digital en la gestión pública, orientados en el acceso a la banda ancha y el Internet. No fue identificada una Política Nacional en Seguridad Cibernética, sin embargo, existe una Política de Estado denominada: Estado eficiente, transparente y descentralizado, que en su línea política N°35: Política de Sociedad de la Información y Sociedad del Conocimiento, son tratadas las preocupaciones relevantes a la seguridad de la información y ciberseguridad. Como primer diagnóstico al panorama de las configuraciones de la SegCiber peruana, inferimos que los instrumentos utilizados en el análisis de las capacidades de la seguridad y defensa cibernética son incentivados por acciones multisectoriales con estrategias no transversales a sus problemáticas y amenazas vigentes. Siendo acciones desposeídas, en su tratamiento social, principalmente en la perspectiva socioeconómica, geopolítica y cultural. También observamos, que los intereses de la SegCiber peruana se orienta en atender a los sujetos informacionales y a sus instituciones estatales (dispositivos informacionales) articulados a través del gobierno electrónico y digital, en donde el Aspecto Sociocultural y Organizacional (ASO) es predominante, con relación a los otros aspectos estudiados. En la perspectiva de la ciencia de la información, percibimos que la información activada en el interior del dispositivo delineará un tipo de conocimiento, poder y de sujetos sometidos a los contextos únicamente locales en lo social, político y económico. Por tanto, el ASO contrasta con las categorías de análisis cualitativa del informe del *International Institute for Strategic Studies*, donde el poder y la capacidad cibernética de los países desarrollados, están focalizados en aspectos del ecosistema cibernético, como de sus intersecciones con la seguridad internacional, competición económica y asuntos militares (International Institute for Strategic Studies (IISS), 2021). Estando las capacidades cibernéticas ponderadas al ámbito de la defensa y de las fuerzas armadas. Además, el ASO se muestra relevante en las discusiones y preocupaciones de los expertos peruanos, con tópicos relacionados al gobierno y gestión de la información gubernamental y la necesidad de una articulación de sus políticas públicas entre los sectores. Finalmente, observamos que el AGD es de menor relevancia en el estudio de caso peruano. Por esa razón, en el ámbito de la SegCiber, la generalización y el ligero tratamiento de los factores de amenazas, pueden inducir a errores o falsos modelos de capacidades cibernéticas nacionales. Como parte del método aplicado, las variables: contexto geopolítico, cultural, social y económico, deben ser traídas a discusión en sus estrategias, específicamente, en el caso peruano. Estas variables buscarán garantizar el equilibrio de la dependencia político-tecnológica, la sustentación de su capacidad operacional y la calidad de la informaciones en sus instituciones.

Desarrollo de las implicaciones teóricas

Disponiendo del panorama de las configuraciones de políticas y estratégicas de la SegCiber peruana, serán presentadas las implicaciones derivadas de las perspectivas teóricas que direccionaron nuestro estudio. Buscando sugerir mejoras o adecuaciones en el caso peruano estudiado, siendo las siguientes: (1) La política de la información y la cibernética son definidas por su inclusión en la intervención estatal, a través de las capacidades ciberespaciales. Debiendo ser considerado como un factor estratégico de desarrollo científico-tecnológico. Correlacionado a nuevos modelos de soberanía, en donde el Estado actúa como agente privilegiado en el ciclo de la información; dándose una "dupla representación de sus dominios territorial, social y simbólica" (González de Gómez, 2002, p. 27). Un Estado moderno está "dotado de un metacapital que permite ejercer un poder sobre todo capital" (Bourdieu, 2014, p. 273). Así el Estado peruano podrá asegurar su influencia y poder sobre otros campos de la actividad y de la formación del capital social, industrial y financiero, entre otros. (2) El no disponer de una Política en SegCiber no es un delimitador, porque puede estar influenciada en otras iniciativas públicas y gubernamentales. Sin embargo, el direccionamiento holístico y multisectorial por medio su sistema de planificación estratégica nacional deberá tener una participación en la coordinación de los sectores y niveles de gobierno. En el caso de la seguridad y defensa cibernética deberán estar alineadas a sus intereses nacionales y no por la libertad de sus individuos. Siendo sugerido que la SegCiber peruana no debe estar sujeta al principio de representación de la sociedad, sino en la perspectiva de un proyecto social, respetando los parámetros del orden social, aspirando a fundamentos del orden económico, absteniéndose de intereses políticos-partidarios y de la sociedad civil. Según Foucault (2020, p. XIV) la economía política y las instituciones del mercado permiten determinar el valor de los bienes y servicios, la estructura esencial del Estado y la sociedad. (3) "El Estado no puede y no debe curvarse fácilmente a los intereses de grupos que se aproximan buscando donaciones, rendas y privilegios desnecesarios, como cortes de impuestos" (Mazzucato, 2021, p. 29). Los procesos de desarrollo económico y de transformación estructural deben estar orientadas cultural y socialmente consensuadas en las instituciones gubernamentales. Buscando atender aspectos de historicidad, causalidad social y estructural subyacente a las interrelaciones de la economía, tecnología, sociedad y política. La SegCiber peruana deberá incentivar estrategias comerciales, tecnológicas y de incentivos a la exportación tecnológica nacional. (4) La pluralidad de saberes especializados y jerarquizados en la SegCiber, son concentrados en países desarrollados que poseen hegemonía política-tecnológica. La omisión y desintegración de las normas sociales y de exclusión socioeconómica, son síntomas de un régimen informacional (González de Gómez, 2012) que atraviesa al Estado y su sociedad, como a las condiciones políticas de gobernanza de la información. En el caso peruano, inferimos que no alcanzará una plena realización si está sujeta a la modernización subalterna y conservadora de sus saberes y de su ciencia. Deberá mitigar sus estereotipos sociales como: el patrimonialismo y la privatización clientelar de lo público, convergencia tecnológica y económica, la ausencia de reglas y estándares socio-tecnológicos, el inmediatismo en el contexto de cambios tecnológicos radicales, etc. (5) La dependencia tecnológica es equilibrada en base a las capacidades cibernéticas alcanzadas. En el caso peruano, deben ser fortalecidos los sectores de economía y finanzas, donde sean incentivadas inversiones y créditos a las exportaciones e importaciones de empresas nacionales que desarrollen ciencia y tecnología. En el sector de infraestructura de telecomunicaciones, ofreciendo condiciones materiales de producción y organización selectiva de las TIC en la industria local y pública. En el sector educativo, más allá del control meritocrático en los altos cargos de las instituciones, deberán ser aculturados en el ecosistema cibernético y de las tecnologías disruptivas; incentivando el mantenimiento de la operatividad del talento humano y de su distribución en los demás sectores. El MINEDU debe ser empoderado, articulando el conocimiento y la investigación científica en universidades e institutos técnicos, dialogando con las demandas del mercado y de la industria. (6) Reconstruir las relaciones entre Estado, sociedad y empresa; adaptando las estrategias cibernéticas en relación con la demanda del mercado internacional. El Estado peruano, como centro de gravedad en la experiencia de la economía digital, incentivando el capital extranjero y la creación de una infraestructura industrial de telecomunicaciones, incentivando las exportaciones de la industria tecnológica. In pro de la ciencia y desarrollo tecnológico de sus instituciones e industrias. Promoviendo la combinación de redes centralizadas de subcontratistas con las Pequeñas y Medianas Empresas (PYME) junto a empresas fabricantes de TIC. El Estado peruano debe facilitar una estructura industrial de interconexión de las PYME con empresas terceras especializadas para la exportación e importación de productos y servicios tecnológicos. Una estrategia, es la creación de un sistema de bibliotecas digitales seguras y confiables donde se desarrollen programas de capacitación, consultorías, colaboración tecnológica y producción técnico-científica, reduciendo el riesgo empresarial. Las estrategias de seguridad y defensa cibernética deben mitigar la dependencia de las multinacionales extranjeras que operan en las TIC, a través de la integración de centros de investigación, empresas y mercados. Sin desalentar los procesos de la globalización, siendo conscientes de los fenómenos provocados por la asimetría de la información. (7) La SegCiber peruana no debe estar desconectada de iniciativas multilaterales en materia de relaciones exteriores y diplomacia. La geoestrategia peruana deberá incentivar la colaboración de grupos de expertos militares, inteligencia, civiles y de la comunidad científico-académica especializada, elaborando estudios de perspectiva geopolítica y geoeconómica en el ámbito ciberespacial y de las tecnologías disruptivas. (8) Para neutralizar los efectos de las operaciones de influencia y ciberespaciales, como el mitigar las intervenciones de países desarrollados con hegemonía política-tecnológica se sugiere que la SegCiber peruana adopte un Estado-Núcleo a través de los mecanismos del Consejo de Defensa Suramericano (CDS).

Según Huntington (2010, p. 350) "los Estados-Núcleos, congregan legiones de civilizacionales [...] combinación adecuada de acciones diplomáticas, políticas, económicas y clandestinas, así como instigaciones de propaganda y forma de coerción, para lograr sus objetivos"; siendo priorizados tres tópicos en la región: (a) La hegemonía de influencia político-tecnológica occidental y asiática. (b) Industrialización de tecnologías disruptivas para la defensa. (c) La ciber diplomacia y la ciber coerción en los intereses de los países Suramericanos. (9) La SegCiber peruana debe designar a una institución como coordinador nacional. Este coordinador debe regular con autonomía y recursos en el ámbito ciberespacial, articulando con el sistema de inteligencia nacional. Se sugiere que en el artículo 54 de la Constitución Peruana, el dominio del ciberespacio sea adscrito a los parámetros del territorio del Estado peruano. Las operaciones de las empresas en un mercado autorregulado pueden ser destructivas. En principio, cuando empresas operan libres de leyes y regulación, no son equilibradas las asimetrías existentes, generando vicios y problemas en el ámbito social, económico y político. (10) Las capacidades de la SegCiber peruana debe adaptarse a los paradigmas informacionales y de cambios en la economía global a través de la modernización tecnológica, del mercado digital y la diversificación económica. Como en la identificación de vicios y problemas que afectan a los intereses de la SegCiber, principalmente, la desburocratización de la gestión económica por medio de la digitalización de activos, estimulando la productividad y resultados de sus instituciones. Implementando controles de monitoramiento y rendición de cuentas, a través de la automatización y auditorias internas, en atención, a los principios de transparencia, eficiencia y eficacia.

CONCLUSIONES

La metodología de investigación aplicada en el estudio de caso de la SegCiber peruana favoreció en la organización, visualización y análisis de los resultados. El método del análisis de contenido permitió la identificación de los códigos y agentes, así como de sus relaciones configuradas en las estrategias de la seguridad y defensa cibernética. Habiendo definido nuestras hipótesis provisorias y sus siete categorías, relacionadas con la seguridad cibernética peruana. Observase que la exploración y dominio de conceptos teóricos fueron primordial en el análisis y de potencial apoyo para el desarrollo de la investigación. Otro aspecto, la visualización de las relaciones entre los códigos fortaleció nuestra comprensión de indicios no obvios en el corpus documental, como de fenómenos que, en principio, no eran del conocimiento de los investigadores. Observando inclusive las relaciones indirectas de los códigos y sus elementos satélites que se influencian en otros códigos o categorías. Esta particularidad amplifica la concepción de las categorías, reforzando una re-teorización del estudio. Resaltando que el Aspecto Sociocultural y Organizacional (ASO) es relevante para los fines de las políticas y estrategias de la SegCiber peruana. Finalmente, el artículo propone siete aspectos para el diseño y construcción de las capacidades cibernéticas peruanas, con base en las implicaciones teóricas sugeridas por los autores. En este contexto, el presente estudio fortaleció nuestras inferencias, enriqueciendo e innovando la presente investigación como un todo. De cara a futuros trabajos, proponemos elaborar un estudio de casos múltiplos, donde sea aplicada la metodología en los países de Suramérica, partiendo de los 07 aspectos estudiados, para luego compararlas entre ellas.

REFERENCIAS

Banco Interamericano de Desarrollo (BID), & Organización de los Estados Americanos (OEA). (2020). *Ciberseguridad: riesgos, avances y el camino a seguir en américa latina y el caribe.* Banco Interamericano de Desarrollo. Descargado de https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Bardin, L. (2016). *Análise de conteúdo.* Edições 70. (Tradução de Luís Antero Reto e Augusto Pinheiro)

Bourdieu, P. (2014). Sobre el estado. cursos en el collège de france (1989-1992). *methaodos revista de ciencias sociales*, *3*(1). doi: 10.17502/m.rcs.v3i1.73

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

Fidler, D. P. (2018). *La ciberseguridad y la nueva era de las actividades espaciales.* Council on Foreign Relations. Descargado de https://www.cfr.org/report/cybersecurity-and-new-era-space-activities

Foucault, M. (2020). *Nascimento da biopolítica.* Lisboa: Edições 70.

González de Gómez, M. N. (2002). Novos cenários políticos para a informação. *Ciência da Informação*, *31*(1), 27–40. Descargado de https://revista.ibict.br/ciinf/article/view/975/1013

González de Gómez, M. N. (2012). Regime de informação: construção de um conceito. *Informação & Sociedade: Estudos*, *22*(3), 43–60. Descargado de https://www.brapci.inf.br/_repositorio/2015/12/pdf_3c42553162_0000011948.pdf

Huntington, S. P. (2010). *O choque de civilizações e a recomposição da ordem mundial.* Objetiva.

International Institute for Strategic Studies (IISS). (2021). *Cyber capabilities and national power: a net assessment.* IISS. Descargado de https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power/

Mazzucato, M. (2021). *O estado empreendedor: desmascarando o mito do setor público vs setor privado* (4. ed. ed.). Editora Schwarcz S.A. (Tradução de E. Serapicos)

Mbanaso, U. M., & Dandaura, E. S. (2015). The cyberspace: redefining a new world. *IOSR Journal of Computer Engineering (IOSR-JCE)*, *17*(3), 17–24. doi: 10.9790/0661-17361724

Nascimento, L. C. N., Souza, T. V., Oliveira, I. C. S., Moraes, J. R. M. M., Aguiar, R. C. B., & Silva, L. F. (2018). Theoretical saturation in qualitative research: an experience report in interview with schoolchildren. *Revista Brasileira de Enfermagem*, *71*(1), 228–233. Descargado de https://doi.org/10.1590/0034-7167-2016-0616 doi: 10.1590/0034-7167-2016-0616

OSIPTEL. (2023a). *Reporte estatístico.* Repositório Ospitel. Descargado de https://repositorio.osiptel.gob.pe/bitstream/handle/20.500.12630/832/Reporte%20E_MARZO_2023.pdf?sequence=1&isAllowed=y

OSIPTEL. (2023b). *Reporte estatístico.* Repositório Ospitel. Descargado de https://repositorio.osiptel.gob.pe/bitstream/handle/20.500.12630/838/Reporte%20E_MAYO_2023%20M.pdf?sequence=6&isAllowed=y

Patriau, E. (2018). Perú: redes ilegales y liderazgos políticos sin control. En J. M. Solís Delgadillo & M. Morriconi Bezerra (Eds.), *Atlas de la violencia en américa latina* (pp. 330–349). Universidad Autónoma de San Luis Potosí. Descargado de https://globalinitiative.net/wp-content/uploads/2018/04/Atlas-de-la-Violencia-en-Am%C3%A9rica-Latina-Juan-Mario-Sol%C3%ADs-Delgadillo-2018.pdf

Rädiker, S., & Kuckartz, U. (2020). *Análisis de datos cualitativos con maxqda.* MAXQDA Press. doi: 10.36192/978-3-948768003

Romero, O. (2019). Telecomunicaciones y dependencia en américa latina: retos para la integración autónoma. *Controversias y Concurrencias Latinoamericanas*, *11*(19), 137–155. Descargado de https://www.redalyc.org/journal/5886/588661549008/html/

Rozas Balbontín, P. (2003). *Gestión pública, regulación e internacionalización de las telecomunicaciones: el caso de telefónica s.a.* Instituto Latinoamericano y del Caribe de Planificación Económica y Social. Descargado de https://core.ac.uk/download/pdf/45621217.pdf

Voss, C., Tsikriktsis, N., & Frohlich, M. (2002). Case research in operations management. *International Journal of Operations & Production Management*, *22*(2), 195–212. Descargado de https://www.researchgate.net/publication/224952206_Case_Research_in_Operations_Management

World Economic Forum (WEF). (2022). *The global risks report 2022 (17th ed.).* World Economic Forum. Descargado de https://www.weforum.org/reports/global-risks-report-2022

Yin, R. K. (2001). *Estudo de caso: planejamento e métodos* (2. ed. ed.). Bookman.

Zibechi, R. (2012). *Anillo óptico sur americano.* MIRA. Descargado de https://www.americas.org/es/anillo-optico-suramericano/

Cómo citar este artículo (APA):
Cuba, A. C. H. & Moura, M. A. (2025). Estudio de caso de la Seguridad Cibernética Peruana: un panorama de sus configuraciones políticas y estratégicas. *AtoZ: novas práticas em informação e conhecimento, 14*, 1 – 18. Descargado de: http://dx.doi.org/10.5380/atoz.v14.91234

APÊNDICE 1 - CORPUS: DOCUMENTOS EN EL ÁMBITO DE LA SEGURIDAD Y DEFENSA NACIONAL CIBERNÉTICA DEL PERÚ

ÂMBITO	ID	NOME	ANO
1. Leis e Regulações Nacionais em PERU	LRN-001-PE	Ley Nº 27658: Ley Marco de Modernización de la Gestión del Estado.	2002
	LRN-002-PE	Ley Nº 27806: Ley Transparencia y Acceso a la Información Pública.	2002
	LRN-003-PE	Ley N° 27269: Ley de Firmas y Certificados Digitales.	2008
	LRN-004-PE	Ley N° 27291: Ley que modifica el código civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica.	2000
	LRN-005-PE	Ley N° 28493: Ley que regula el uso del Correo Electrónico comercial no solicitado (SPAM).	2005
	LRN-006-PE	Ley N° 29733: Ley de Protección de Datos Personales.	2011
	LRN-007-PE	Ley N° 28530: Ley de Promoción de Acceso a Internet para personas con discapacidad y adecuación del espacio físico en cabinas públicas de internet.	2012
	LRN-008-PE	Ley N° 30096 y su modificatoria Ley 30171: Ley de Delitos Informáticos.	2013
	LRN-009-PE	Ley Nº 30618, Ley que modifica el Decreto Legislativo 1141, decreto legislativo de fortalecimiento y modernización del sistema de inteligencia nacional - sina y de la dirección nacional de inteligência - DINI, a fin de regular la seguridad digital.	2017
	LRN-010-PE	Ley 29904: LEY DE PROMOCIÓN DE LA BANDA ANCHA Y CONSTRUCCIÓN DE LA RED DORSAL NACIONAL DE FIBRA ÓPTICA.	2012
	LRN-011-PE	Ley 29985. Ley que regula el uso del Dinero Electrónico como Instrumento de inclusión financiera.	2013
	LRN-012-PE	Ley 30035. Ley que regula el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto.	2013
	LRN-013-PE	Ley Nº 30036. LEY QUE REGULA EL TELETRABAJO.	2013
2. Política e Linhas de Ação Estratégica em PERU	PLA-001-PE	Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la R.M. N° 004- 2016-PCM referente al Comité de Gestión de Seguridad de la Información.	2017
	PLA-002-PE	Decreto Legislativo nº 1412, Ley de gobierno digital.	2018
	PLA-003-PE	Politica Nacional de Ciberseguridad.	2017
	PLA-004-PE	Lineamientos para la formulación del Plan de Gobierno Digital.	2018
	PLA-005-PE	Resolución Ministerial N° 119-2018-PCM, Resolución de creación del Comité de Gobierno Digital.	2018
	PLA-006-PE	Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.	2016
	PLA-007-PE	Resolución Ministerial N° 197-2011-PCM, que establece fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información".	2011
	PLA-008-PE	Resolución Ministerial N° 246-2007-PCM, que aprueba la Norma Técnica Peruana "NTPISO/ IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.	2007
	PLA-009-PE	Decreto Legislativo N° 1353, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses.	2017
	PLA-010-PE	Decreto Supremo N° 066-2011-PCM: Aprueba el "Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0"	2011
	PLA-011-PE	Decreto Supremo N° 004-2013-PCM: Aprueba la Política Nacional de Modernización de la Gestión Pública.	2013
	PLA-012-PE	Decreto Supremo N° 081-2013-PCM: Aprueba la Política Nacional de Gobierno Electrónico 2013-2017.	2013
	PLA-013-PE	Resolución Ministerial N° 179-2004-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2004 Tecnología de la Información. "Procesos del Ciclo de Vida del Software, 1ª Edición" en entidades del Sistema Nacional de Informática.	2004
	PLA-014-PE	Decreto Supremo Nº 072-2003-PCM. Aprueban el Reglamento de la Ley de Transparencia y Acceso a la Información Pública.	2003
	PLA-015-PE	Decreto Supremo N° 050-2018-PCM. Aprueban la definición de Seguridad Digital en el Ámbito Nacional.	2018
	PLA-016-PE	Decreto Supremo Nº 014-2013-MTC. Reglamento de la Ley Nº 29904, Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica.	2013
	PLA-017-PE	Resolución Ministerial N° 179-2004-PCM. Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información.	2012
	PLA-018-PE	Resolución Ministerial N° 179-2004-PCM. Aprueban lineamientos y mecanismos para implementar la interconexión de equipos de procesamiento electrónico de información entre las entidades del Estado.	2008
3. Publicações do Departamento da Defesa em PERU	PDD-001-PE	Proyecto de Ley 4228 de ciberdefensa.	2018
	PDD-002-PE	Decreto Legislativo Nº 1141, Fortalecimiento y Modernización del Sistema de inteligência Nacional - SINA y de la Dirección Nacional de inteligência - DINI.	2012
	PDD-003-PE	Resolución DIN Nº 033-DINI-2020-01, Norma técnica para protección de activos nacionales.	2020
	PDD-004-PE	Decreto Supremo N° 106-2017-PCM, Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales (ACN).	2017
	PDD-005-PE	Decreto Supremo N° 012-2017-DE. Decreto Supremo que aprueba la Política de Seguridad y Defensa Nacional.	2017

APÊNDICE 2 - GUION DE ENTREVISTA Y CUESTIONARIO A EXPERTOS PERUANOS

Universidad Federal de Minas Gerais (UFMG, Brasil)
Programa de Pós Graduación en Ciencia de la Información (PPGCI)
Investigación de Doctorado

Guion de entrevista a expertos gubernamentales

La presente guía de entrevista fue elaborada por el Autor 1, alumno de doctorado en Ciencia de la Información en la Universidad Federal de Minas Gerais (UFMG, Brasil), becario del programa de la Organización de Estados Americanos (OEA) y el Grupo Coímbra de Universidades Brasileras (GCUB), trabajando bajo la supervisión de la profesora Autor 2 (UFMG). El objetivo de la investigación es identificar, sistematizar y analizar en una perspectiva comparada las políticas y estrategias de seguridad cibernética implementadas en América del Sur, notablemente en Argentina, Brasil y Perú; con el objeto de disponer de un panorama actual de las configuraciones políticas y estratégicas en el ámbito de la seguridad cibernética que fueron definidas en los tres países estudiados. Gracias por su participación.

Observación: Las entrevistas serán conducidas vía online y grabadas, con la promesa de confidencialidad y anonimato. Por ese sentido, todo dato personal que relacione al entrevistado o a las personas que fueran descritas serán anonimizadas. De acuerdo con la Ley 13.709/2018 LGPD: "La anonimización de datos se trata de la utilización de medios técnicos razonables y disponibles en el momento del tratamiento, **por medio de los cuales un dato pierde la posibilidad de asociación, directa o indirecta, a un individuo**".

Nombres y apellidos:
Fecha:
Institución:
Cargo:
Correo:

En el aspecto de las amenazas y riesgos

1.1. ¿Cuáles son las prioridades que buscan alcanzar las estrategias en la seguridad y defensa cibernética, en el hipotético caso de ser activada una situación de crisis cibernética nacional?

1.2. ¿Qué actores son los involucrados, cuáles son las prioridades?

1.3. Finalmente, en su experiencia y de las funciones que viene ejerciendo actualmente, ¿Cuál es la principal amenaza (externa o interna) que puede dar origen a una crisis cibernética nacional?

Finalidad de la pregunta: Identificar los actores involucrados en las estrategias en seguridad y defensa cibernética.

En el aspecto de las capacidades y respuestas

2.1. Para la protección del espacio cibernético nacional, ¿Cuáles estrategias fueron direccionadas desde el nivel político-estratégico?

2.2. Desde su experiencia y de las funciones que viene ejerciendo actualmente, ¿Dónde se encuentran las mayores capacidades cibernéticas?

2.3. Desde la perspectiva de la seguridad y defensa nacional, ¿Qué se busca alcanzar con el Internet y/o Ciberespacio?

Finalidad de la pregunta: Identificar los actores involucrados en las estrategias en seguridad y defensa cibernética.

En el aspecto del poder y dominación

3.1. ¿Usted considera que las estrategias nacionales en el ámbito cibernético, impulsan la expansión y dominación en defensa de los intereses y objetivos nacionales de su país?

3.2. ¿Usted considera que las estrategias nacionales en el ámbito cibernético, regulan y sancionan toda acción tecnológica que pueda afectar a los intereses nacionales? ¿Se tiene algún caso de sanciones realizadas a las empresas desde la perspectiva de la seguridad y defensa nacional?

Finalidad de la pregunta: Analizar los elementos que constituyen una política de seguridad cibernética.

En el aspecto geopolítico y diplomático

4.1. La Política Nacional de Seguridad Cibernética trae iniciativas en el ámbito diplomático. ¿Puede usted mencionar algunas de esas iniciativas?

4.2. ¿Qué institución es responsable por la geoestrategia nacional en el ámbito espacial y cibernético? ¿Como funcionario público decisorio, conoce a cuáles intereses y objetivos nacionales se busca atender con la Política Nacional de Seguridad Cibernética?

Finalidad de la pregunta: Analizar la geopolítica en el ámbito cibernético y sus repercusiones en la consolidación de las políticas y estrategias en seguridad cibernética.

En el aspecto sociocultural y organizacional

5.1. ¿La Política Nacional de Seguridad Cibernética ha conducido o incentivado las reformas institucionales? ¿Considera que la Política Nacional de Seguridad Cibernética se complementa a otras políticas o leyes nacionales? ¿Cuáles específicamente?

5.2. ¿En qué forma la Política Nacional de Seguridad Cibernética ha incentivado beneficios, prosperidad y desarrollo en el ámbito sociocultural?

Finalidad de la pregunta: Comprender qué actores y elementos constituyen una política de seguridad cibernética, en el ámbito sociocultural e institucional.

En el aspecto socioeconómico y de mercado

6.1. ¿La Política Nacional de Seguridad Cibernética incentiva el consumo de las tecnologías de información y de la comunicación nacionales? ¿Se tienen iniciativas que equilibren la dependencia tecnológica extranjera?

6.2. ¿Los programas en seguridad y defensa cibernética orientan de forma centralizada la activación de esfuerzos conjuntos intersectoriales, en busca de una optimización de costos y beneficios?

6.3. ¿En qué forma la Política Nacional de Seguridad Cibernética ha impulsado la economía y mercado digital nacional?

Finalidad de la pregunta: Comprender qué agentes y elementos constituyen una política de seguridad cibernética, en el ámbito socioeconómico y de mercado.

En el aspecto tecnológico e industrial

7.1. ¿Se tienen en las estrategias nacionales una entidad pública responsable por normar y establecer los estándares en Tecnologías de la Información y de la Comunicación en la industria nacional o privada?

7.2. ¿En la Política Nacional de Seguridad Cibernética, también están incluidas las empresas multinacionales extranjeras? ¿Qué sector es el responsable de esa articulación y con qué finalidad?

7.3. ¿El acceso y conectividad al Internet es impulsada en las estrategias de seguridad y defensa cibernética? ¿El proveedor de Acceso a la Internet o Proveedor de Servicio de Internet (ISP) es una empresa estatal? ¿Qué órgano regula los ISPs?

Finalidad de la pregunta: Comprender qué actores y elementos constituyen una política de seguridad cibernética, en el ámbito tecnológico e industrial.

NOTAS DA OBRA E CONFORMIDADE COM A CIÊNCIA ABERTA

CONTRIBUIÇÃO DE AUTORIA

Papéis e contribuições	Arthur Christian Huamani Cuba	Maria Aparecida Moura
Concepção do manuscrito	X	
Escrita do manuscrito	X	
Metodologia	X	
Curadoria dos dados	X	
Discussão dos resultados	X	X
Análise dos dados	X	

EQUIPE EDITORIAL