ISSN 0719-4110

CIEE
CENTRO DE INVESTIGACIÓN Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL

CUADERNO DE TRABAJO N°5-2022

INFRAESTRUCTURA CRÍTICA EN CHILE: ¿ESTAMOS PREPARADOS PARA PROTEGERLA? UN ANÁLISIS A LA POLÍTICA NACIONAL DE CIBERSEGURIDAD

Academia Nacional
de Estudios Políticos
y Estratégicos
www.anepe.cl

CUADERNOS DE TRABAJO es una publicación orientada a abordar temas vinculados a la Seguridad y Defensa a fin de contribuir a la formación de opinión en estas materias.

Los cuadernos están principalmente dirigidos a tomadores de decisiones y asesores del ámbito de la Defensa, altos oficiales de las Fuerzas Armadas, académicos y personas relacionadas con la comunidad de defensa en general.

Estos cuadernos son elaborados por investigadores, académicos y colaboradores del CIEE de la ANEPE, pero sus páginas se encuentran abiertas a todos quienes quieran contribuir al pensamiento y debate de estos temas.

Recordamos a los autores que el Cuaderno de Trabajo está comprometido con la publicación de artículos originales e inéditos que difundan conocimiento actualizado en materias de seguridad, defensa y ciencias sociales afines, con el fin de aportar y transferir, con el propósito fundamental de aportar al debate académico múltiples enfoques que enriquezcan el análisis, la reflexión y la interpretación en torno a los temas disciplinares propios de la seguridad, la defensa y las ciencias sociales.

Antes de imprimir este Cuaderno, piense en el medio ambiente.

CUADERNO DE TRABAJO DEL CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS es una publicación electrónica del Centro de Investigaciones y Estudios Estratégicos de la Academia Nacional de Estudios Políticos y Estratégicos y está registrada bajo el **ISSN 0719-4110 Cuad. Trab., - Cent. Estud. Estratég.**
Dirección postal: Avda. Eliodoro Yáñez 2760, Providencia, Santiago, Chile.
Sitio Web www.anepe.cl. Teléfonos (+56 2) 2598 1000, correo electrónico ciee@anepe.cl

INFRAESTRUCTURA CRÍTICA EN CHILE: ¿ESTAMOS PREPARADOS PARA PROTEGERLA? UN ANÁLISIS A LA POLÍTICA NACIONAL DE CIBERSEGURIDAD

Maite Mella Díaz*

Resumen:

El ciberespacio se ha transformado en una herramienta de conectividad, lo que ha permitido incorporar gradualmente a las instituciones gubernamentales. La evolución digital representa un desafío para el Estado, no solo por avanzar de forma tecnológica, sino por lograr proteger a la Infraestructura crítica de constantes amenazas cibernéticas. En este trabajo se analizará cómo Chile se enfrenta a estos cambios a través del estudio de la Política Nacional de Ciberseguridad. Para ello se abordará una pregunta fundamental: ¿Dicha guía será suficiente para cubrir espacios de factibles amenazas a la Infraestructura crítica? Lo anterior se llevará a cabo considerando el nivel de desarrollo latinoamericano y los compromisos internacionales suscritos por Chile.

Palabras clave: Infraestructura crítica; ciberseguridad; cooperación internacional; Chile; Latinoamérica.

* Licenciada en Ciencia Política mención Relaciones Internacionales, de la Universidad Alberto Hurtado. ORCID: https://orcid.org/0000-0002-0050-6592

CRITICAL INFRASTRUCTURE IN CHILE: ARE WE PREPARED TO PROTECT IT? AN ANALYSIS OF NATIONAL CYBERSECURITY POLICY

Abstract:

Cyberspace has become a connectivity tool, which has allowed the gradual incorporation of government institutions. A digital evolution represents a challenge for the State, not only for technological advances but also to protect critical infrastructure from constant cyber threats. This paper will analyze how Chile is facing these changes through the study of the National Cybersecurity Policy. Because of it, a fundamental question arises: Will this guide be sufficient to cover potential threats to critical infrastructure? It is necessary to consider the Latin American level of development and the international commitments subscribed by Chile.

Key words: Critical Infrastructure; cybersecurity; international cooperation; Chile; Latin America.

I. Introducción

El acelerado desarrollo tecnológico ha permitido crear, conocer y utilizar redes y dispositivos en un entorno en el que se pensaba imposible hasta hace un par de décadas; la forma en que accedemos a la información y la capacidad de almacenarla ha sorprendido a diversas generaciones, no solo por su rapidez sino por la propia reducción del material físico a un aspecto digital. No obstante, el progreso también tiene sus desventajas.

Aunque cada persona tenga una noción sobre qué tan sensible es la información que busca o guarda, cuando se habla del Estado y, principalmente, de su Infraestructura crítica se transforma en un tópico aún más delicado. En este sentido, un ciberataque no solo afectaría a las instituciones gubernamentales, sino a las decisiones, estrategias y acciones que se comunican de forma interna y que podrían interferir en la seguridad nacional e incluso en las percepciones internacionales.

En abril de 2017 se aprobó en Chile la "Política Nacional de Ciberseguridad" (PNCS) que determina normas y metas para el año 2022 con el fin de establecer un ciberespacio l*ibre, abierto, seguro y resiliente*[1] *en el país*. La Política Nacional es una propuesta relativamente "nueva" y ambiciosa respecto al ciberespacio, creada y aplicada en un período de ciberataques en ascenso a las instituciones estatales.

[1] PNCS, Política Nacional de Ciberseguridad. 2017. Biblioteca Digital. bibliotegadigital.gob.cl. [En línea] 27 de abril de 2017. [Citado el: 29 de agosto de 2022.] https://biblioteca.digital.gob.cl/bitstream/handle/123456789/738/Pol%C3%ADtica%20Nacional%20de%20Ciberseguridad.pdf?sequence=1&isAllowed=y

Los riesgos y vulnerabilidades son cada vez mayores, por lo que se ha debido recurrir a la creación de otros instrumentos y normativas como la Política de Ciberdefensa (2018)[2] la Ley de Protección de Datos Nº 19.628; la Ley de Delitos Informáticos Nº 21.459 y, fundamentalmente, el reforzamiento de los convenios internacionales en un sentido de colaboración por conocimiento.

En el texto se pretende identificar algunos puntos débiles que la actual Política Nacional de Ciberseguridad (PNCS) posee, específicamente, al hablar sobre Infraestructura crítica. Estos puntos están sujetos al desempeño tecnológico del país frente a Latinoamérica, así como las expectativas que existen hacia Chile de acuerdo con los avances en ciberseguridad en términos internacionales, ya que "Chile se ha hecho de la cooperación y asistencia internacional una de las bases para la creación de capacidades en el ámbito de la ciberseguridad"[3]. A raíz de lo anterior surgen diversas interrogantes como ¿qué implica un ciberataque a inmediaciones estatales? ¿por qué es relevante entablar una conversación respecto a lo ciber a nivel nacional? ¿cuál es la situación latinoamericana en cuanto a ciberseguridad? Estas preguntas dan origen a la interrogante principal: ¿La Política Nacional de Ciberseguridad en Chile será suficiente para cubrir espacios de factibles amenazas a la Infraestructura crítica?

II. Cibercapacidad: escenario latinoamericano

Es común esperar que un país altamente digitalizado esté blindado de cualquier amenaza. En el caso de Latinoamérica, la agenda de ciberseguridad aún no se impone en cada nación, ya sea por brindar prioridad a otros asuntos internos o por no contar con suficientes recursos económicos.

"En el caso de Latinoamérica, la agenda de ciberseguridad aún no se impone en cada nación, ya sea por brindar prioridad a otros asuntos internos o por no contar con suficientes recursos económicos."

En el año 2020 la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID)[4] publicaron un Reporte de Ciberseguridad que daba cuenta de los desafíos y problemáticas que ha tenido la región. En este estudio se pudo corroborar que Latinoamérica aún posee una brecha digital inmensa, relacionándolo directamente a que "El nivel de madurez de los países en materia de educación, formación y desarrollo de capacidades sigue siendo extremadamente dispar, un hecho que está ligado a las importantes desigualdades económicas, sociales y culturales"[5].

Si bien este diagnóstico no es repentino para la zona, es "labor de las naciones de la región transformar estas debilidades en áreas de oportunidad y mejora en aras de encarar los retos y amenazas provenientes del ciberespacio"[6]. Es por esto que en el siguiente ranking se indica que los países con una política de ciberseguridad ya implementada tienen más capacidades y estrategias defensivas que aquellos países

[2] Nota del Autor: Al respecto véase: HORZELLA, Bárbara. 2021. Política Nacional de Ciberdefensa Revisión contrastada con la Guía de Ciberdefensa de la JID. Biblioteca del Congreso Nacional de Chile / BCN. [En línea] marzo de 2021. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/31943/1/Informe_BCN__Politica_Nacional_de_Ciberdefensa.pdf

[3] Minrel. Unidad de Ciberseguridad y Tecnologías Emergentes. minrel.cl. [En línea] [Citado el: 22 de 8 de 2022.] https://www.minrel.gob.cl/ministerio/direcciones/direccion-de-seguridad-internacional-y-humana/unidad-de-ciberseguridad

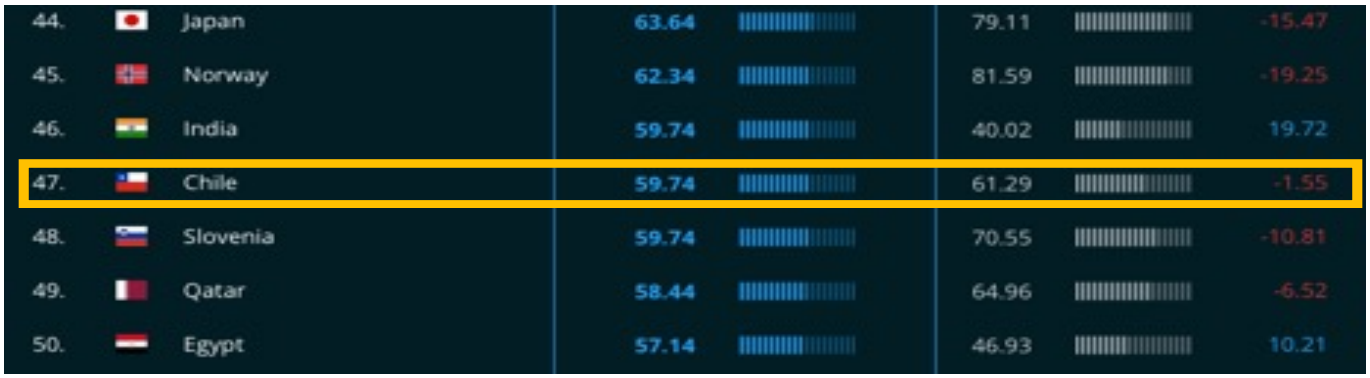
[4] BID. 2020. Reporte de ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y El Caribe. publications.iadb.org. [En línea] 2020. https://observatoriociberseguridad.org/#/final-report Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior

[5] Ibid.

[6] AGUILAR Antonio, Juan Manuel. Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estud. int. (Santiago, en línea) [online]. 2021, vol.53, n.198 [citado 2022-09-30], pp. 169-197. Disponible en: <http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-37692021000100169&lng=es&nrm=iso> ISSN 0719-3769. http://dx.doi.org/10.5354/0719-3769.2021.57067

que recién están trabajando en ello. Según los datos proporcionados por National Cyber Security Index (NCSI) en colaboración con e-Governance Academy Foundation de Estonia[7], Chile es el segundo país latinoamericano con mayor capacidad para enfrentar ciberataques y amenazas provenientes del ciberespacio, ubicado en el puesto Nº 47; solo le antecede Paraguay en el puesto Nº 41.

Figura 1: Ranking NCSI



Fuente: NCSI. 2022. National Cybersecurity Index NCSI. ncsi.ega. [En línea] e-Governance Academy Foundation. https://ncsi.ega.ee/ncsi-index/?order=rank&type=c

El adjuntar una clasificación a este trabajo tiene un objetivo en particular: demostrar que la actual Política de Ciberseguridad se ha quedado atrás para defender el propio desarrollo tecnológico. Los datos anteriores aseguran que Chile es uno de los países latinoamericanos que posee mayor preparación para combatir los peligros del ciberespacio; por tanto, se podría asumir que la PNCS se encuentra a la altura de dicho ranking.

Más allá de la crítica, es importante establecer una conversación respecto a una temática pública de gran importancia y complejidad que debiese estar instaurada en el lenguaje común, al considerar la dependencia que las personas y el Estado tienen hacia la tecnología, ya sea por elección o por la propia presión de la conectividad y la globalización. A continuación, se revisará en profundidad la PNCS que funciona como un procedimiento de seguridad cibernética y directriz gubernamental.

III. Chile: Política Nacional de Ciberseguridad (PNCS)

Debido a que es la primera estrategia que rige en el país como una pauta de Estado en ciberseguridad, es necesario conocer los motivos con los que fue elaborada la Política Nacional de Ciberseguridad y sus principales propuestas. La PNCS establece cuatro puntos que funcionan como justificación para su creación:

I. Existe para el resguardo y la protección de las personas dentro del ciberespacio.
II. Vela por la seguridad nacional y los servicios del país a nivel público y privado.
III. Busca generar espacios de cooperación y conversación entre instituciones u otros órganos públicos o privados.
IV. Por último, sirve para gestionar los riesgos del ciberespacio de forma resiliente y estable[8].

[7] NCSI. 2022. National Cybersecurity Index NCSI. ncsi.ega. [En línea] e-Governance Academy Foundation. https://ncsi.ega.ee/ncsi-index/?order=rank&type=c
[8] PNCS, Política Nacional de Ciberseguridad. 2017. Loc. Cit.

Como fue mencionado, la propuesta está pensada hacia el año 2022 y aún no se conoce oficialmente si se han alcanzado las metas establecidas para dicho año. Esto es una oportunidad de reflexión sobre el contexto nacional actual, sobre todo si se comprende que fue creada para generar resultados o cambios a largo plazo. En esta línea, la PNCS tiene cinco objetivos dirigidos hacia el 2022:

I. El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos.

II. El Estado velará por los derechos de las personas en el ciberespacio.

III. Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.

IV. El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales.

V. El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos[9].

Estos cinco objetivos abren un espacio para cuestionar si, en efecto, Chile adoptó o no una dirección semejante a lo que se aspiraba en 2017 cuando se publicó la estrategia. Al desglosarlos, se infiere que el punto dos ha estado sujeto a controversias; por un lado, aunque en Chile existe la Ley de Protección de Datos Nº 19.628[10], se ha debatido "cuán correcto o legítimo es entregar vía ley de transparencia —u obligar que se entregue por este medio— información de naturaleza privada que resguardan entidades de naturaleza pública"[11].

Por otro lado, los tres últimos objetivos coinciden con la situación actual de nuestro país, dada la cantidad de programas educativos que han surgido y que son impartidos y entregados en diversas modalidades; de igual forma, existe un incremento de instancias de cooperación internacional y compromisos de desarrollo que Chile ha adquirido en los últimos años y, por último, el crecimiento de una industria especialista en ciberseguridad.

"Es de suma relevancia comprender el panorama presentado sobre la Política Nacional de Ciberseguridad que, de alguna forma u otra, intenta abarcar una brecha digital demarcada no solo por la desigualdad económica, sino por la propia desigualdad tecnológica que se encuentra en instituciones públicas o privadas."

Es de suma relevancia comprender el panorama presentado sobre la Política Nacional de Ciberseguridad que, de alguna forma u otra, intenta abarcar una brecha digital demarcada no solo por la desigualdad económica, sino por la propia desigualdad tecnológica que se encuentra en instituciones públicas o privadas.

IV.Infraestructura crítica

Una vez realizado el desglose a los objetivos planteados queda uno sin resolver: 1. "El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos"[12]. Para

[9] Ibid.

[10] Entel. ¿En qué consiste la Ley de protección de datos en Chile? entel.cl. [En línea] Comunidad Empresas. https://ce.entel.cl/grandes-empresas/articulos/ley-de-proteccion-de-datos-en-chile

[11] CASTRO, Maritza. 2022. Algunas consideraciones sobre el proyecto de ley de tratamiento de datos personales. [Columna] Santiago : Idealex.press, 2022.

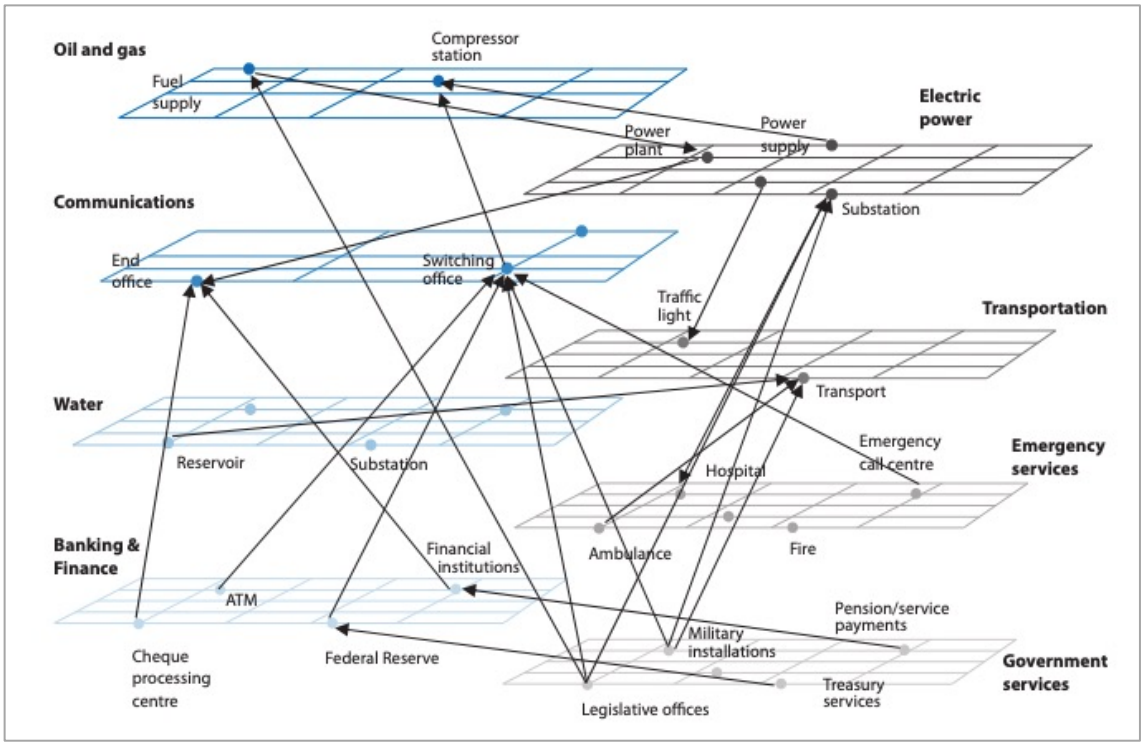
[12] PNCS, Política Nacional de Ciberseguridad. 2017. Loc. Cit.

tener una mejor aproximación a lo que se conoce por Infraestructura crítica, la Biblioteca del Congreso Nacional emitió un documento en 2019 en el que se consideran dos tipos de Infraestructura crítica:

(1)Infraestructuras estratégicas: las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.
(2) Infraestructuras críticas: las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales" (Ley 8/2011, Artículo 2)[13].

En este cuaderno se utiliza la definición (2), puesto que abarca tanto a los componentes como el funcionamiento de los servicios esenciales. La siguiente imagen expone una representación a nivel macro y micro, y permite dimensionar lo que significa una red de Infraestructura crítica y los servicios que afecta:

Figura 2: Interdependencias de Infraestructura crítica



Fuente: OECD. 2011. Future Global Shocks: Improving Risk Governance, OECD Reviews of Risk Management Policies. OECD Publishing [En línea] https://doi.org/10.1787/9789264114586-en

[13] HORZELLA, Barbara. 2019. Protección de Infraestructura Crítica y Fuerzas Armadas Conceptualización y experiencia comparada. bcn.cl. [En línea] diciembre de 2019. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/28141/1/BCN_Proteccion_IC_Conceptualizacion_y_experiencia_comparada.pdf

Ahora bien, la PNCS plantea entonces una *infraestructura robusta* y resiliente que proteja a la Infraestructura crítica, y es necesario preguntar ¿quién se encarga de dicha protección? La propia normativa define una serie de responsabilidades adjudicadas a diversos organismos que administran, previenen y responden ante amenazas a la ciberseguridad[14], siendo las siguientes:

- Ministerio de Interior y Seguridad Pública: Red de Conectividad del Estado CSRIT.
- Ministerio de Defensa: Fuerzas Armadas, Estado Mayor Conjunto.
- Policía de Investigaciones: Brigada Investigadora del Ciber crimen.
- Carabineros de Chile: Departamento OS-9.
- Ministerio de Transportes y Telecomunicaciones.
- Ministerio de Relaciones Exteriores: Dirección de Seguridad Internacional y Humana.
- Agencia Nacional de Inteligencia.
- Ministerio Secretaría General de la Presidencia: Modernización del Estado.
- Universidad de Chile: NIC Chile, CLCert.
- Instituto Nacional de Normalización.
- Ministerio Público.
- Poder Judicial.

Con todo esto ¿Chile está preparado para adversidades cibernéticas a gran escala? Si bien son más de 10 los órganos mencionados, es importante hacer una mirada panorámica y realista. El hecho de que algunas de estas instituciones posean unidades dedicadas a cubrir áreas de seguridad y ciberespacio no significa, necesariamente, un dominio absoluto en la temática. Factores como la capacitación humana o la adquisición de herramientas de mayor nivel podrían ser fundamentales al momento de tomar acción, y es en donde se han observado fallas en los últimos años al no ser una prioridad de Estado: "Las organizaciones públicas y privadas deberían tener en cuenta la seguridad digital en sus actividades de gestión de riesgos y no considerarla un riesgo técnico específico al que debe darse una respuesta aislada"[15].

"Con todo esto ¿Chile está preparado para adversidades cibernéticas a gran escala?"

Ahora bien, tal como se menciona en el listado, se debe reconocer a una de las principales instituciones que coordina, lidera y proporciona herramientas de ciberseguridad: el Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT encargado de "proveer servicios de seguridad a las instituciones del Estado que forman parte de la Red de Conectividad del Estado, RCE"[16].

Como se menciona, el CSIRT es una pieza fundamental en la infraestructura que busca proteger pero, ¿cuáles son sus principales logros? Además de conformar un Comité Interministerial de Ciberseguridad que permite asesorar a subsecretarías, se ha mantenido constante desde su consolidación en 2018; el CSIRT podría ser el eslabón más fuerte de la PNCS en la red estatal. El problema es que no todas los establecimientos públicos que están bajo la supervisión de este equipo siguen las indicaciones, "finalmente la responsabilidad siempre recae en las instituciones en su deber de realizar las actualizaciones que correspondan"[17].

En este sentido, se puede observar que aunque funcionen todas las piezas que corresponden en un sistema, basta que falle una pequeña

[14] Ibid.

[15] OECD. 2020. Perspectivas económicas de América Latina 2020: Transformación digital para una mejor reconstrucción, OECD Publishing [En línea] https://doi.org/10.1787/f2fdced2-es

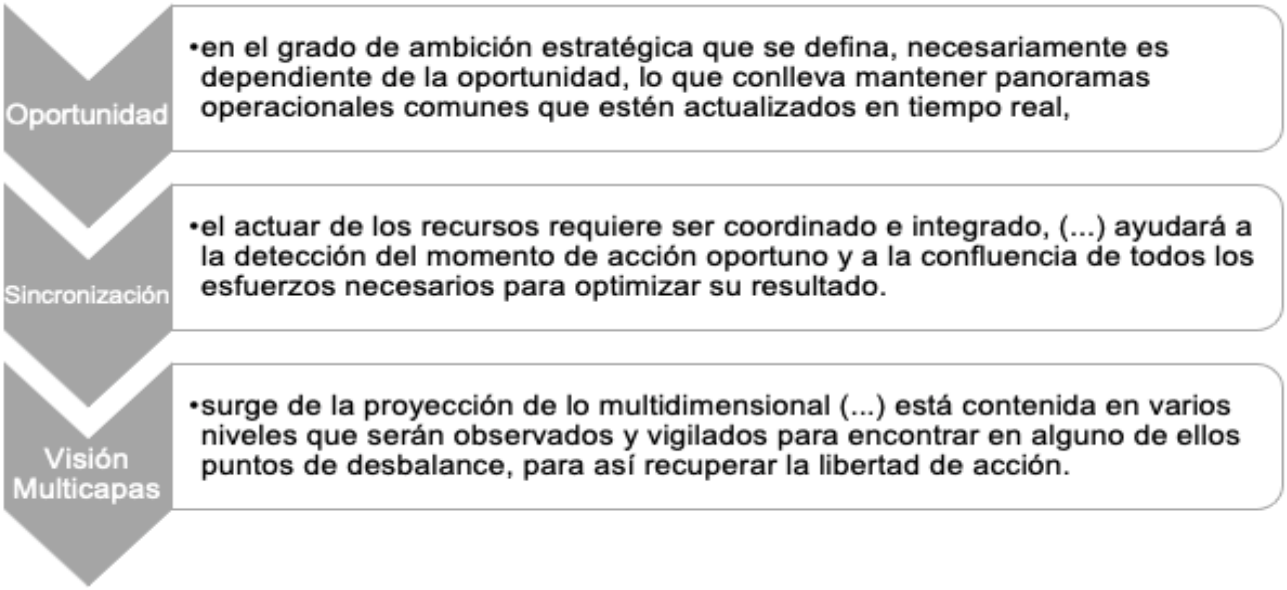
[16] TRENDTIC. 2022. trendTIC-Tendencias tecnológicas & Negocios. Trendict.cl [en línea] 21 de noviembre de 2022. Disponible en: https://www.trendtic.cl/2022/11/el-csirt-de-gobierno-representa-la-continuidad-y-transversalidad-de-un-proyecto-y-de-una-vision-que-involucra-a-varios-actores-y-sectores-del-mundo-privado-y-publico/.

[14] Ibid.

para ralentizar al sistema completo. A diferencia de la defensa marítima, aérea o terrestre, delimitar estrategias que enfrenten algún tipo de ciberamenaza o ciberguerra puede sonar lejano a nuestra realidad física o puede significar carecer de experiencia, pero es esencial proteger hoy la seguridad de la Infraestructura crítica y al mismo tiempo el propio sistema democrático como lo es el caso de la Red de Conectividad del Estado.

Así, se precisa de tres elementos que sirven para gestionar con responsabilidad las labores de ciberseguridad en instituciones gubernamentales[18] y que podrían generar objetividad y determinación en la división de tareas.

Figura 3: Elementos de gestión gubernamental



Fuente: Elaboración propia con datos de LEIVA Villagra, René. 2019. Loc. Cit.

Términos como oportunidad, sincronización y visión multicapas son parte de una serie de necesidades que deben ser cubiertas y que aportan al desarrollo de la conectividad entre las unidades de trabajo. Es menester insistir en esta problemática debido a que el país no ha estado ajeno a ciberataques.

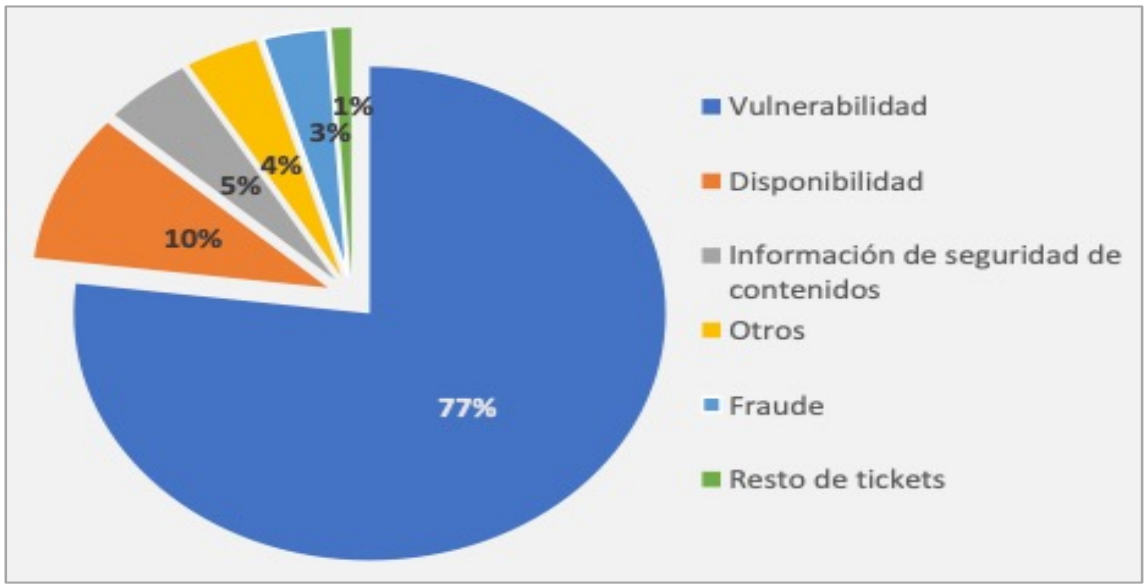
Antes de ejemplificar, se debe comprender que existe la amenaza cibernética entendida como "la posibilidad de que un sistema vulnerable sea atacado y sufra daños"[19], aquella amenaza desprende diferentes formas de que se lleve a cabo y se pueden identificar como phishing, malware, fraude, vulnerabilidad, fuerza bruta, entre otros. Esto puede afectar a múltiples instituciones o dispositivos causando daños materiales, económicos o de alteración personal a través del robo de información -por ejemplo-. En relación a lo anterior, el

[18] LEIVA Villagra, René. 2019. Evolución tecnológica y ciberseguridad. Revista Ensayos Militares. [En línea] 2019. https://www.revistaensayosmilitares.cl/index.php/tica/article/view/157/173

[19] AMBIT TEAM. 2022. Diferencias entre amenaza, vulnerabilidad y riesgo. ambit. Building solutions together. [En línea] 22 de febrero de 2022. https://www.ambit-bst.com/blog/diferencias-entre-amenaza-vulnerabilidad-y-riesgo

CSIRT emitió las estadísticas de septiembre de 2022 que contienen los tipos de incidentes reportados desde el sector público y privado hacia el organismo gubernamental, encargado de analizar y publicar la siguiente información:

Figura 4: Tipo de Incidente



Fuente: CSIRT. 2022. INFORME DE GESTIÓN MENSUAL SEPTIEMBRE 2022. Ministerio del Interior y Seguridad Pública. Santiago : Gobierno de Chile, 2022. p. 11.

Tal como se observa en la imagen, el mayor tipo de incidencias que afectó a instituciones gubernamentales y no gubernamentales fue vulnerabilidad, lo que significa una debilidad propia de un sistema que permite ser atacado y recibir un daño[20]. Lo anterior llevó a que el CSIRT recomendara la actualización urgente de *software* y sus respectivos parches de seguridad.

Antes de continuar, es necesario hacer un paréntesis y recordar que en 2016 Chile le solicitó a la OCDE asesoría sobre la transición y transformación digital del gobierno y sus servicios, lo que se vio reflejado en un estudio de Gobernanza Digital en Chile publicado por este órgano internacional. Son dos las recomendaciones que en ese entonces la OCDE le entregó al país, siendo las siguientes:

1) Una agencia dedicada a la digitalización del sector público que dependa de un ministerio
2) La Subsecretaría de Gobierno Digital en un mismo ministerio[21].

De igual forma, LA OCDE aconsejó revisar las instituciones que algunos países como Australia, España, Portugal o Estonia -por nombrar algunos- han utilizado y obtenido efectos positivos en la gobernanza digital. ¿Por qué es necesario realizar este paréntesis? Porque en 2020 la propia OCDE felicitó al país por sus avances en materias de modernización estatal y

[20] Ibid.
[21] Nota del Autor: En el siguiente enlace se puede revisar la síntesis publicada por el Ministerio de Relaciones Exteriores, así como el link a este reporte: https://www.chile.gob.cl/chile/blog/todos/gobierno-digital-en-chile-nuevo-reporte-ocde

transformación digital del Estado; es decir, Chile recogió y adoptó las recomendaciones.

No obstante, así como se reconocieron los avances de Chile en ámbitos de servicios y procesos digitales para la ciudadanía, se le solicitó un liderazgo y gobernanza que sea capaz de transmitir valor y confianza en la población[22]. Lo que se intenta insertar en medio de la explicación sobre incidentes ocurridos en el mes de septiembre de 2022, es la contradicción en la entrega de servicios gubernamentales como algo expresamente eficiente desde la OCDE y la carencia de seguridad que tienen las instituciones que proveen hoy dichos servicios, lo que se puede traducir en la pérdida de valor y confianza que la OCDE pide.

"No obstante, así como se reconocieron los avances de Chile en ámbitos de servicios y procesos digitales para la ciudadanía, se le solicitó un liderazgo y gobernanza que sea capaz de transmitir valor y confianza en la población."

Sin retroceder tanto tiempo, en septiembre de 2022, se dio a conocer un ataque cibernético de gravedad hacia el Estado Conjunto Mayor (EMCO) adjudicado a un grupo de *hackers* llamado "Guacamaya". La irrupción a los computadores de EMCO se realizó por años, fueron robados cientos de correos electrónicos y documentos con información confidencial y conversaciones privadas. El suceso no solo involucró a personal militar y de defensa, sino también a la seguridad del país debido al contenido del material interceptado. El mismo mes, el Poder Judicial de Chile fue víctima de un *malware* que dejó sin acceso a los dispositivos electrónicos de la institución. Los perpetuadores secuestraron datos y dejaron sin acceso a funcionarios y dispositivos del servicio público[23].

Ambos casos no representan la cantidad de ciberataques que el país sufre diariamente[24], pero sí demuestra que servicios que irónicamente corresponden a Defensa y Justicia son completamente vulnerables ante cualquier tipo ciberataque. Además, representan a un porcentaje de los organismos vinculados al Estado y que son blanco de amenazas cibernéticas.

Ante esto, es relevante nombrar y recordar uno de los primeros ciberataques de proporción a la Infraestructura crítica como lo fue *Stuxnet,* un "gusano" que en 2015 se introdujo en una planta nuclear iraní con orden de autodestrucción[25]. Lo aterrador no solo es la orden, sino la magnitud de la transgresión hacia una instalación nuclear y sus posibles consecuencias. En términos generacionales, es posible que el ciberespacio sea algo reciente, pero no se pueden esconder las huellas que los ciberataques o el ciberterrorismo han dejado, por el contrario, es momento de aprender y afrontarlas.

V. Política Nacional de Ciberdefensa (PNCD)

En concordancia a lo anterior, no se puede ignorar al principal complemento de la PNCS y el amparo defensivo de la Infraestructura crítica y la soberanía del país. Como su nombre lo

[22] FUENTES, Jesús. 2020. OCDE reconoce que Chile tiene una ley robusta y habilitante en materia de transformación digital. Apiux. [En línea] 8 de julio de 2020. https://www.api-ux.com/2020/07/08/ocde-reconoce-que-chile-tiene-una-ley-robusta-y-habilitante-en-materia-de-transformacion-digital/

[23] Véase en: LABORDE, Antonia. 2022. Un ciberataque pone en alerta al Poder Judicial de Chile. El País. [En línea] 27 de septiembre de 2022. [Citado el: 29 de septiembre de 2022.] https://elpais.com/chile/2022-09-27/un-ciberataque-pone-en-alerta-al-poder-judicial-de-chile.html

[24] Nota del autor: En la siguiente página web se pueden observar ciberataques en tiempo real https://cybermap.kaspersky.com/es

[25] Véase en: NEWS, BBC. 2015. El virus que tomó control de mil máquinas y les ordenó autodestruirse. BBC. [En línea] 11 de octubre de 2015. [Citado el: 15 de septiembre de 2022.] https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

indica, la Política Nacional de Ciberdefensa fue aprobada en 2017 como resultado de uno de los objetivos de la PNCS y es hoy "la respuesta del Estado de Chile a los nuevos riesgos y amenazas que el ciberespacio genera para las capacidades de la Defensa Nacional, las cuales incluyen, entre otros elementos, la información, infraestructura y operaciones de defensa"[26].

En términos breves, la Política Nacional de Ciberdefensa cuenta con seis capítulos que comienzan en un análisis hacia la situación del país y su respectivo diagnóstico, para continuar con los principios que la rigen y su marco institucional; y termina con las orientaciones internacionales y los tratados firmados por Chile. En sí, "el documento configura la respuesta del Estado de Chile a los nuevos riesgos y amenazas que el ciberespacio genera para las capacidades de la defensa nacional, las cuales incluyen, entre otros elementos, la información, infraestructura y operaciones de defensa"[27].

"... la Política Nacional de Ciberdefensa fue aprobada en 2017 como resultado de uno de los objetivos de la PNCS y es hoy "la respuesta del Estado de Chile a los nuevos riesgos y amenazas que el ciberespacio genera para las capacidades de la Defensa Nacional, las cuales incluyen, entre otros elementos, la información, infraestructura y operaciones de defensa."

Considerando lo expresado y los ejemplos descritos sobre ciberataques en el país, la PNCD se ha transformado en una temática de renovación y de urgente innovación para el gobierno actual, delimitando un plan de revisión entre 2022 y 2023.

A continuación, serán presentados los principales tratados de los que Chile es parte, como un símbolo de conectividad externa entre el país y el mundo, y de la búsqueda por mejorar los sistemas nacionales.

VI. Acuerdos Internacionales

Una cualidad de la Política Exterior en Chile es la constante apertura al diálogo internacional, lo que ha permitido fortalecer lazos bilaterales y multilaterales en beneficio de las naciones. Según el Ministerio de Relaciones Exteriores[28], el país se encuentra adscrito a tres acuerdos internacionales en materias "ciber", además de pertenecer a los programas de ciberseguridad que impulsa la Organización de Estados Americanos. De este modo, los tratados son los siguientes:

(1) Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional 2021 – 2025 (OEWG)[29].
(2) Comité Especial para la elaboración de una Convención Internacional integral para contrarrestar el uso indebido de las tecnologías de la información y las comunicaciones con fines delictivos[30].

[26] HORZELLA, Bárbara. 2021. Loc. Cit

[27] ALVAREZ Valenzuela, Daniel. Ciberseguridad en América Latina y ciberdefensa en Chile. Rev. chil. derecho tecnol. [En línea]. 2018, vol.7, n.1 [citado 2022-12-15], pp.1-2. Disponible en: <http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842018000100001&lng=es&nrm=iso> ISSN 0719-2584. http://dx.doi.org/10.5354/0719-2584.2018.50416.

[28] Minrel. Unidad de Ciberseguridad y Tecnologías Emergentes. Loc. Cit.

[29] Nota del Autor: El siguiente documento insta a la unidad en términos de ciberamenaza. Ciberseguridad, Dirección de Seguridad Internacional y Humana. 2022. Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (OEWG 2021 – 2025) Segunda Reunión Sustantiva (28 de marzo – 1 de abril, 2022). s.l. : Ministerio de Relaciones Exteriores, 2022.

[30] Nota del Autor: Para mayor debate, visite el siguiente enlace: DE SOUZA, Roberto. 2022. Las ruedas que mueven al mundo: el futuro tratado de "ciberdelincuencia" de las Naciones Unidas. derechos digitales.org. [En línea] Derechos Digitales América Latina, 1 de abril de 2022. https://www.derechosdigitales.org/18230/las-ruedas-que-mueven-al-mundo-el-futuro-tratado-de-ciberdelincuencia-de-las-naciones-unidas/

(3) Grupo de Expertos Gubernamentales sobre las Tecnologías Emergentes en el Ámbito de los Sistemas de Armas Autónomos Letales (GGE)[31].

Es importante recalcar uno de los marcos internacionales más importantes en términos de ciberseguridad del que Chile y gran cantidad de países latinoamericanos participa: el Convenio de Budapest. En primer lugar, la distinción que implica que los Estados se integren al Convenio de Budapest demuestra y establece el compromiso que han adquirido ante la ciberdelincuencia y los ciberataques, al pertenecer a un acuerdo internacional que ha intentado establecer normas y leyes que guíen, desde la perspectiva jurídica, a las naciones que participan de esta Convención. Es coherente señalar que Chile se incorporó como Estado miembro a este tratado en el año 2017.

En segundo lugar, ayuda a progresar a los Estados que tienen una Estrategia Nacional de Ciberseguridad ya que, además de entablar la cooperación internacional como la instancia nombrada en el párrafo anterior, potencian garantizar la protección de los derechos de las personas e incluso blindar al país frente a un ataque que amenace la seguridad de la nación.

En la siguiente imagen se pueden observar en color verde aquellos países que ya cuentan con una Política Nacional de ciberseguridad, y en rojo los cuatro países que se encuentran desarrollándola.

Figura 5: Miembros y Observadores del Convenio de Budapest

Fuente: BID. 2020. Loc.Cit.

[31] Nota del autor: Cruz Roja proporciona una mirada interesante en esta temática. Visitar en CICR. 2021. Sistemas de armas autónomos letales: el CICR recomienda la adopción de nuevas reglas. icrc.org. [En línea] Comité Internacional de la Cruz Roja, 23 de septiembre de 2021. https://www.icrc.org/es/document/sistemas-armas-autonomos-letales-cicr-recomienda-adopcion-nuevas-reglas

A nivel judicial, cabe señalar la reciente Ley Nº 21.459 sobre Delitos Informáticos que deroga la Ley Nº 19.223 sobre "Figuras penales relativas a la informática."

La importancia de esto reside en que la reciente ley determina nuevos delitos adecuados al contexto actual como: falsificación informática, fraude informático, acceso ilícito, entre otros, y define nuevas herramientas para perseguir estos delitos a nivel nacional y transnacional. Lo más importante es que ha sido modificada a los lineamientos del Convenio de Budapest y sus exigencias[32].

Es probable que el contexto político-global inicie, incluso dentro del ciberespacio, nuevas oportunidades de diálogo. En cierta medida no percibimos naturalmente la velocidad en que se desenvuelve lo ciber y lo que compone a este territorio; por ende, los mismos tratados mencionados podrían tener vacíos el día de mañana. No obstante, es de suma relevancia impulsar el diálogo político y técnico.

Es un hecho que "Chile expresa una fuerte voluntad de cooperación internacional en su estrategia, incluyendo la política cibernética dentro de la Política Exterior chilena, y promueve normativas internacionales que fomentan la confianza y la seguridad en el ciberespacio"[33] pero, a su vez, es importante mantener elocuencia al demostrar confianza y seguridad, ya que es evidente la ausencia de cooperación nacional frente a situaciones de vulnerabilidad, precisamente por no contar con instancias de diálogo interno, de manera que sea el unilateralismo el que resulte en un multilateralismo fructífero y no en aislacionismo[34]. Es necesario adoptar una "diplomacia tecnológica" propulsada por la Política Exterior chilena, que se adapte al desarrollo y se niegue a la obsolescencia[35].

"…. es importante mantener elocuencia al demostrar confianza y seguridad, ya que es evidente la ausencia de cooperación nacional frente a situaciones de vulnerabilidad, precisamente por no contar con instancias de diálogo interno, de manera que sea el unilateralismo el que resulte en un multilateralismo fructífero y no en aislacionismo."

Conclusión

Puede ser esperanzador encontrar en segundo lugar a Chile en el ranking de mayor capacidad de defensa cibernética, en comparación a otros países de Latinoamérica. De igual forma, la habilidad y eficacia que la reciente Política Exterior ha tenido para incluir al país en diversas instancias de participación y diálogo a nivel mundial se podría impulsar por el anhelo de alcanzar un nivel más alto en términos de ciberseguridad.

Los ciberataques no solo se cubren desde la adquisición de sistemas de defensa, sino desde el conocimiento, capacitación y proyección a escenarios futuros. Dicho esto, es que la Política Nacional de Ciberseguridad no es suficiente para proteger a la Infraestructura crítica del país. No se puede depender de los acuerdos de cooperación internacional para difundir conocimiento, es necesario complementar a

[32] CSIRT. 2022. La nueva Ley de Delitos Informáticos entró en vigor. CSIRT. [En línea] 2022. https://csirt.gob.cl/noticias/nueva-ley-de-delitos-informaticos-entro-en-vigor/

[33] URBANOVICS, Anna y GUAJARDO, Rodrigo. 2022. Estrategias de ciberseguridad en los paises latinoamericanos – un análisis comparativo. IV, Budapest: Universidad de Szeged, Departmento de Estudios Hispanicos, 1 de septiembre de 2022, ACTA HISPANICA SUPPLEMENTUM 4. Aspectos de la defensa y seguridad en América del Sur y Europa del Sur: fronteras, conflictos y cooperación internacional, pp. 89–104.

[34] MARTABIT Tellechea, Pía. 2019. Infraestructura crítica, usuarios y contenido: ¿Qué se busca proteger en el ciberespacio? En: Cuadernos de Trabajo Nº9-2019. Septiembre. [en línea] Disponible en: https://anepe.cl/wp-content/uploads/2020/10/Cuaderno-de-Trabajo-N°9-2019.pdf. ISSN 0719-4110

[35] LODEIRO, Andrea. Fraguando Escenarios. Balance Estratégico 2020-2021. [En línea] 2021. https://www.publicacionesanepe.cl/index.php/balance/article/view/942.

mayor escala lo internacional con lo nacional, priorizando que la integración resulte en cooperación y viceversa.

Asimismo, los sucesos ocurridos en el mes de septiembre del año 2022 son la clara respuesta a que la PNCS no logra fiscalizar el estado tecnológico de las instituciones y no garantiza la comunicación entre quienes componen la Infraestructura crítica. Se necesita de interacción entre organismos, profesionales y de herramientas actualizadas, no solo por el bien de uno o más dispositivos, sino por responsabilidad hacia la Seguridad Nacional.

Además, se debe generar consciencia sobre la infinidad evolutiva del ciberespacio a una escala nacional, a través de la educación e inclusión cibernética y la alfabetización digital, tanto para ciudadanos como funcionarios de instituciones gubernamentales y establecimientos relacionados. Si bien existen campañas propias de CSIRT -por ejemplo- que buscan explicar el vocabulario ciber desde una forma sencilla, es necesario que el Estado y otros organismos sean partícipes de la difusión de este tipo de campañas, así como de impulsar una educación o cultura digital desde temprana edad a generaciones que han crecido con acceso a internet y que están insertos en una sociedad tecnológica. En esta línea, el CSIRT podría necesitar de mayor protagonismo y recursos en caso de que SE democratice el conocimiento técnico por sí solo.

Por último, es de suma relevancia el fortalecer la Política Nacional de Ciberseguridad y reconocer a la Política Nacional de Ciberdefensa como su complemento y principal apoyo cuando se habla de resguardo hacia la Infraestructura crítica. Es probable que estas políticas nunca estén niveladas en su totalidad a la actualidad ciber dados los constantes avances tecnológicos, pero necesita destacar en el presupuesto nacional y obtener voluntades políticas que trabajen a favor del futuro y de la estabilidad del país, con el fin de generar capacidades jurídicas, defensivas y técnicas que permitan enfrentar en conjunto posibles ciberataques, hackeos, apagones cibernéticos e incluso conflictos internacionales a gran escala, y que involucren la difusa “soberanía” de Chile en el ciberespacio.

BIBLIOGRAFÍA

AGUILAR Antonio, Juan Manuel. Retos y oportunidades en materia de ciberseguridad de América Latina Frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estud. Int. (Santiago, en línea) [Online]. 2021, Vol.53, N.198 [Citado 2022-09-30], pp.169-197. Disponible en: <http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-37692021000100169&lng=es&nrm=iso>. ISSN 0719-3769.

ÁLVAREZ Valenzuela, Daniel. Ciberseguridad en América Latina y ciberdefensa en Chile. Rev. Chil. Derecho tecnol. [En línea]. 2018, Vol.7, N.1 [Citado 2022-12-15], pp.1-2. Disponible en: <http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842018000100001&lng=es&nrm=iso>. ISSN 0719-2584. http://dx.doi.org/10.5354/0719-2584.2018.50416.

ÁLVAREZ Valenzuela, Daniel. LA paz y la seguridad internacional en el ciberespacio.Rev. Chil. Derecho tecnol. [online]. 2019, Vol.8, N.2 [Citado 2022-09-30], pp.1-3. Disponible en: <http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842019000200001&lng=es&nrm=iso>. ISSN 0719-2584. http://dx.doi.org/10.5354/0719-2584.2019.55827.

AMBIT TEAM. 2022. Diferencias entre amenaza, vulnerabilidad y riesgo. Ambit. Building solutions together. [En línea] 22 de febrero de 2022. https://www.ambit-bst.com/blog/diferencias-entre-amenaza-vulnerabilidad-y-riesgo

BID. 2020. REporte de ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y El Caribe. publications.iadb.org. [En línea] 2020. https://observatoriociberseguridad.org/#/final-report. Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior.

CASTRO, Maritza. 2022. Algunas consideraciones sobre el proyecto de ley de tratamiento de datos personales. [Columna] Santiago : Idealex.press, 2022.

CICR. 2021. Sistemas de armas autónomos letales: el CICR recomienda la adopción de nuevas reglas. icrc.org. [En línea] Comité Internacional de la Cruz Roja, 23 de septiembre de 2021. https://www.icrc.org/es/document/sistemas-armas-autonomos-letales-cicr-recomienda-adopcion-nuevas-reglas.

Ciberseguridad, Dirección de Seguridad Internacional y Humana. 2022. Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional (OEWG 2021 – 2025) Segunda Reunión Sustantiva (28 de marzo – 1 de abril, 2022). s.l. : Ministerio de Relaciones Exteriores, 2022.

CSIRT . 2022. INFORME DE GESTIÓN MENSUAL SEPTIEMBRE 2022. Ministerio del Interior y Seguridad Pública. Santiago : Gobierno de Chile, 2022. p. 11.

CSIRT. 2022. La nueva Ley de Delitos Informáticos entró en vigor. CSIRT. [En línea] 2022. https://csirt.gob.cl/noticias/nueva-ley-de-delitos-informaticos-entro-en-vigor/.

Entel. ¿En qué consiste la Ley de protección de datos en Chile? entel.cl. [En línea] Comunidad Empresas. https://ce.entel.cl/grandes-empresas/articulos/ley-de-proteccion-de-datos-en-chile/.

LODEIRO, Andrea. Fraguando Escenarios. BALANCE ESTRATÉGICO 2020-2021. [En línea] 2021. https://www.publicacionesanepe.cl/index.php/balance/article/view/942.

FUENTES, Jesús. 2020. OCDE reconoce que Chile tiene una ley robusta y habilitante en materia de transformación digital. Apiux. [En línea] 8 de julio de 2020. https://www.api-ux.com/2020/07/08/ocde-reconoce-que-chile-tiene-una-ley-robusta-y-habilitante-en-materia-de-transformacion-digital/.

HORZELLA, Barbara. 2019. Protección de Infraestructura Crítica y Fuerzas Armadas Conceptualización y experiencia comparada. bcn.cl. [En línea] diciembre de 2019. http://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/28141/1/BCN_Proteccion_IC_Conceptualizacion_y_experiencia_comparada.pdf.

HORZELLA, Bárbara. 2021. Política Nacional de Ciberdefensa, Revisión contrastada con la Guía de Ciberdefensa de la JID. obtienearchivo.bcn.cl. [En línea] marzo de 2021. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/31943/1/Informe_BCN__Politica_Nacional_de_Ciberdefensa.pdf.

LABORDE, Antonia. 2022. Un ciberataque pone en alerta al Poder Judicial de Chile. El País. [En línea] 27 de septiembre de 2022. [Citado el: 29 de septiembre de 2022.] https://elpais.com/chile/2022-09-27/un-ciberataque-pone-en-alerta-al-poder-judicial-de-chile.html.

MARTABIT Tellechea, Pía. 2019. Infraestructura crítica, usuarios y contenido: ¿Qué se busca proteger en el ciberespacio? En: Cuaderno de Trabajo Nº9-2019 CIEE-ANEPE [En línea] septiembre de 2019. https://anepe.cl/wp-content/uploads/2020/10/Cuaderno-de-Trabajo-N°9-2019.pdf ISSN 0719-4110.

Minrel. Unidad de Ciberseguridad y Tecnologías Emergentes. minrel.cl. [En línea] [Citado el: 22 de 08 de 2022.] https://www.minrel.gob.cl/ministerio/direcciones/direccion-de-seguridad-internacional-y-humana/unidad-de-ciberseguridad.

NCSI. 2022. National Cybersecurity Index NCSI. ncsi.ega. [En línea] e-Governance Academy Foundation. https://ncsi.ega.ee/ncsi-index/?order=rank&type=c.

NEWS, BBC. 2015. El virus que tomó control de mil máquinas y les ordenó autodestruirse. BBC. [En línea] 11 de octubre de 2015. [Citado el: 15 de septiembre de 2022.] https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet.

OECD. 2011. Future Global Shocks: Improving Risk Governance, OECD Reviews of Risk Management Policies. OECD Publishing [En línea] https://doi.org/10.1787/9789264114586-en

OECD “et al.” 2020. Perspectivas económicas de América Latina 2020: Transformación digital para una mejor reconstrucción, OECD Publishing [En línea] https://doi.org/10.1787/f2fdced2-es

PNCS, Política Nacional de Ciberseguridad. 2017. Biblioteca Digital. bibliotegadigital.gob.cl. [En línea] 27 de abril de 2017. [Citado el: 29 de agosto de 2022.] https://biblioteca.digital.gob.cl/bitstream/handle/123456789/738/Pol%C3%ADtica%20Nacional%20de%20Ciberseguridad.pdf?sequence=1&isAllowed=y.

DE SOUZA, ROBERTO. 2022. Las ruedas que mueven al mundo: el futuro tratado de "ciberdelincuencia" de las Naciones Unidas. Derechos digitales.org. [En línea] Derechos Digitales América Latina, 1 de abril de 2022. https://www.derechosdigitales.org/18230/las-ruedas-que-mueven-al-mundo-el-futuro-tratado-de-ciberdelincuencia-de-las-naciones-unidas/.

TRENDTIC. 2022. trendTIC-Tendencias tecnológicas & negocios. trendtic.cl. [En línea] 21 de noviembre de 2022. https://www.trendtic.cl/2022/11/el-csirt-de-gobierno-representa-la-continuidad-y-transversalidad-de-un-proyecto-y-de-una-vision-que-involucra-a-varios-actores-y-sectores-del-mundo-privado-y-publico/.

URBANOVICS, Anna y GUAJARDO, Rodrigo. 2022. Estrategias de ciberseguridad en los paises latinoamericanos – un análisis comparativo.IV, Budapest : Universidad de Szeged, Departmento de Estudios Hispanicos, 01 de septiembre de 2022, ACTA HISPANICA SUPPLEMENTUM 4. Aspectos de la defensa y seguridad en América del Sur y Europa del Sur: fronteras, conflictos y cooperación internacional, págs. 89–104.

LEIVA Villagra, René. 2019. Evolución tecnológica y ciberseguridad. Revista Ensayos Militares. [En línea] 2019. https://www.revistaensayosmilitares.cl/index.php/tica/article/view/157/173.


CENTRO DE INVESTIGACIÓN Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL