Dossier sobre Ciberseguridad:

Construyendo una Cultura de Ciberseguridad

En Chile el mes de la Ciberseguridad, ha sido establecido en la Ley 21.113, promulgada el 24 de septiembre y publicada el primero de octubre de 2018. En el marco de nuestro compromiso con la generación de una "Cultura de Ciberseguridad", ponemos a disposición un repositorio de documentos sobre el tema con la finalidad de facilitar la información, concienciación y sensibilización en la materia.

En este espacio denominado como "Dossier" se ofrece un repositorio con las principales publicaciones nacionales e internacionales en Ciberseguridad, clasificadas según su origen. Además, son colocados los links de estos documentos, como asimismo, de entidades y expertos que se han especializado y publicado en esta materia. El tema de la ciberseguridad actualmente es de interés público y se encuentra incorporado en la agenda gubernamental en muchos países del mundo, siendo abordado al más alto nivel bajo un enfoque de política pública.

Este aporte inicial que tendrá una ampliación y una permanente actualización, permitirá encontrar documentación histórica y reciente que facilitará conocer la evolución, actualidad y tendencias en Ciberseguridad. En efecto, se ofrece una sistematización de información que se encuentra en su mayoría dispersa en diversas páginas web.

Respecto a la metodología de su elaboración, en una primera instancia se ha contemplado colocar: los principales documentos chilenos sobre la materia; recientes publicaciones de la OEA y resoluciones claves de este organismo sobre el tema; y publicaciones de ANEPE en el tema. Sin embargo, se irá incrementando periódicamente el contenido de este Dossier. En cuanto a la descripción del contenido de los documentos referenciados, en la mayor parte de ellos se ha optado por mantener lo que sus autores, patrocinadores o promotores oficiales han señalado.

Origen	Documento	Contenido	Link	Año de Publicación
Chile	Política Nacional de Ciberseguridad	Política Nacional de Ciberseguridad de Chile	http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf	2017
Chile	Aprueba Política de Ciberdefensa	Describe Política de Ciberdefensa de Chile	http://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf	2018
Chile	Ley N° 21.113	Declara el mes de octubre como el mes nacional de la Ciberseguridad	http://www.diariooficial.interior.gob.cl/publicaciones/2018/10/01/42169/01/1471012.pdf	2018
Chile	Bases para una política de ciberseguridad	Explicita principales lineamientos para una política de ciberseguridad	http://ciberseguridad.interior.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf	2015
Chile	Crea comité interministerial sobre ciberseguridad	Describe el Comité Interministerial sobre Ciberseguridad de Chile: integrantes, funciones y atribuciones, entre otros.	http://www.ciberseguridad.gob.cl/media/2015/12/DTO-533_17-JUL-2015-Crea-Comit%C3%A9-Interministerial-sobre-Ciberseguridad.pdf	2015
Chile	Declara la promulgación del Convenio sobre la Ciberdelincuencia	Promulga el Convenio sobre la Ciberdelincuencia en Chile y adhiere a éste ante el Consejo de Europa	https://www.leychile.cl/Navegar?idNorma=1106936	2017
Consejo de Europa	Convención sobre la Ciberdelincuencia o Convenio de Budapest	Tratado internacional sobre la Ciberdelincuencia	https://www.oas.org/juridico/english/cyb_pry_convenio.pdf	2001
Chile	Minuta de BCN sobre Convenio de Budapest	Síntesis de los principales aspectos del Convenio de Budapest	file:///C:/Users/CSancho/Downloads/Convenio%20N%20185%20del%20Consejo%20de%20Europa%20sobre%20la%20Ciberdelincuencia%20(Convenio%20de%20Budapest)%20(2).pdf	2014
Chile	Ley 19.223	Tipifica figuras penales relativas a la informática	https://www.leychile.cl/Navegar?idNorma=30590	1993

Chile	Ley N° 19.628	Ley sobre protección de la vida privada, regula protección de datos personales	https://www.leychile.cl/Navegar?idNorma=141599	1999
OEA	OEA/Ser.L/X.2.12 Declaración: "Fortalecimiento de la Seguridad Cibernética en las Américas"	Renueva compromiso para implementar la Estrategia Interamericana de Seguridad Cibernética y promueve asuntos relacionados al tema.	http://www.oas.org/es/sms/cicte/documents/declaraciones/DEC%201%20rev%201%20DECLARACION%20CICTE00749S04.pdf	2012
OEA	AG/RES. 2004 Estrategia de Seguridad Cibernética	Aborda el tema de la "Adopción de una Estrategia Interamericana Integral de Seguridad Cibernética: Un Enfoque Multidimensional y Multidisciplinario para la Creación de una Cultura de Seguridad Cibernética"	https://www.sites.oas.org/cyber/Documents/Estrategia-seguridad-cibernetica-resolucion.pdf	2004
OEA	AG/RES. 1939 (XXXIII-O/03) Desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética	Insta al desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética. Asunto abordado en 2004.	http://www.oas.org/juridico/spanish/agres_1939.pdf	2003
OEA	Informe "Estado de la Ciberseguridad en el sector bancario en América Latina y el Caribe"	Describe el Estado de la Ciberseguridad en el sector bancario en América Latina y el Caribe, elementos de convergencia y desafíos a enfrentar.	http://www.oas.org/es/sms/cicte/sectorbancariospa.pdf	2018
OEA / AWS	White paper series Edición 1: "Un llamado a la acción para proteger a Ciudadanos, Sector Privado y Gobiernos"	Esta publicación analizar el estado de la ciberseguridad en las Américas e incrementar el nivel de conciencia de los líderes gubernamentales, del sector privado y de la sociedad en general en torno a la ciberseguridad.	https://www.oas.org/es/sms/cicte/awswhitepaper.pdf	2018
OEA / AWS	White paper series Edición 2: "*Gestión del Riesgo Cibernético Nacional*".	Esta publicación es la segunda de una serie que busca, junto con otras iniciativas, analizar el estado de la ciberseguridad en las Américas e incrementar el nivel de concientización de los líderes gubernamentales, empresas y de la sociedad en general en torno a la ciberseguridad. Iincorpora el análisis de cuatro marcos estratégicos (gubernamentales, internacionales,	https://www.oas.org/es/sms/cicte/ESPcyberrisk.pdf	2018

		académicos y técnicos) para que los gobiernos puedan implementar estrategias que garanticen la seguridad en el ciberespacio a ciudadanos, empresas y administraciones. El informe también plantea una metodología para la gestión del ciber riesgo a largo plazo, así como unas recomendaciones para la definición e implementación de indicadores de desempeño.		
OEA / AWS	White paper series Edición 3: "Oportunidades y desafíos para las PYME en el contexto de una mayor adopción de las TICs".	Esta publicación aborda los desafíos y oportunidades que la ciberseguridad plantea a las pequeñas y medianas empresas (pymes). El reporte incorpora aspectos clave para la gestión de la ciberseguridad en las pymes, como por ejemplo la privacidad de los datos, la sensibilización de la seguridad cibernética en el entorno de las pymes, el rol del gobierno para la creación de un ecosistema de ciberseguridad saludable para este tipo de empresas, así como medidas o recomendaciones activas para que estas empresas refuercen su ciberseguridad.	http://www.oas.org/es/sms/cicte/docs/white-papers/ESP_Digital_-_white_paper_3.pdf	2018
OEA / Microsoft	"Protección a infraestructura critica en Latinoamérica y el Caribe 2018"	Formula recomendaciones para desarrollar un marco de trabajo o política de infraestructura crítica adecuada en la región. El documento sugiere que, aunque existe una colaboración entre el sector público y privado, y una creciente conciencia referente a los problemas de ciberseguridad, aún se puede hacer más para proteger los recursos vitales. El informe incluye una encuesta que recolecta respuestas de cerca de 500 dueños y operadores de infraestructura crítica	https://www.oas.org/es/sms/cicte/ciprepport.pdf	2018
OEA / BID	"Ciberseguridad ¿Estamos Preparados en América Latina y el Caribe?"	Estudio que tiene como objetivo profundizar en el conocimiento de los riesgos de seguridad cibernética, los retos y oportunidades en América Latina y el Caribe. Mediante la utilización de encuestas y otros datos aportados por expertos y funcionarios de treinta y dos Estados Miembros de la OEA, el informe examina la "madurez cibernética" de cada país en cinco dimensiones: 1) política y estrategia de seguridad cibernética; 2) cultura y sociedad cibernética; 3) educación, formación y competencias en seguridad cibernética; 4) marcos jurídicos y reglamentarios; y 5) normas, organizaciones y tecnologías.	file:///C:/Users/CSancho/Downloads/Ciberseguridad-Estamos-preparados-en-America-Latina-y-el-Caribe.pdf	2016

OEA / Trend Micro	Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas	Describe la situación de Seguridad Cibernética e Infraestructura Crítica en las Américas	https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf	2015
ANEPE / Instituto da Defesa Nacional (Portugal)	Investigación internacional: "Cibersegurança e Políticas Públicas Análise comparada dos casos chileno e portugués".	Este estudio analiza las políticas de ciberseguridad en Chile y Portugal hasta 2017 e identifica sus principales características y desafíos. Comienza por presentar un enfoque conceptual y contextual del ciberespacio, en particular sus principales características y tendencias, amenazas y riesgos. En el marco de la cooperación multilateral, se abordan los principales foros en los que Chile y / o Portugal participan - es decir, las Naciones Unidas (ONU), la Unión Europea (UE), la Organización del Tratado del Atlántico Norte (OTAN) y Organización de los Estados Americanos (OEA) - cuyos instrumentos normativos o posición oficial reflejan los consensos alcanzados e influencian las respectivas políticas nacionales en el ámbito en cuestión. El estudio describe factores mínimos para una política de ciberseguridad - conceptos, legislación especializada, arquitectura de ciberseguridad, cooperación, cultura y políticas públicas - así como otros elementos a considerar en el marco de una política nacional de ciberseguridad. Las políticas de ciberseguridad de cada uno de los países se estudian individualmente y posteriormente son comparadas.	https://www.idn.gov.pt/publicacoes/cadernos/idncadernos_29.pdf	2018
ANEPE	Cuaderno de trabajo: "Ciberterrorismo ¿Realidad o Mito?"	La llamada era de la "post-verdad" entrega a la academia de la seguridad internacional especial consideración a la teoría constructivista. Cuando este se utiliza para estudiar el fenómeno "ciberterrorismo", revela que, debido a una falta de evidencia empírica que sustenta la realidad del fenómeno y en contraposición con un elevado uso del concepto tanto en prensa como en la academia, el ciberterrorismo es una realidad discursiva en primera medida y una posiblemente profecía auto cumplida en segundo lugar. Parte importante de la problemática recae	https://www.anepe.cl/wp-content/uploads/Cuaderno-de-Trabajo-N%C2%B05-2018.pdf	2018

		en las dificultades descriptivas encontradas en el concepto terrorismo que emigraron con ellas en su camino al ciberespacio. Este trabajo busca esclarecer la problemática señalada por medio de un análisis de la discusión descriptiva del fenómeno terrorismo y ciberterrorismo en la academia.		
ANEPE	Cuaderno de trabajo: ""Seguridad versus libertad en el ciberespacio".	En el invierno de 2018 una institución financiera fue víctima de dos ataques informáticos, dando pie a un importante debate público sobre cómo estar a la altura de las amenazas globales en el ciberespacio. Las teorías clásicas de las relaciones internacionales aplicadas a la ciberseguridad permiten dilucidar diferentes problemáticas que conlleva la penetración digital en el mundo, y cuáles son las formas de comprender el ciberespacio. En esta búsqueda de seguridad en el espacio cibernético, se presenta una dicotomía entre potenciar la libertad de los individuos y asegurar la red global contra amenazas reales y potenciales al Estado. Este cuaderno tiene por objetivo plantear consideraciones iniciales para dar pie a establecer un equilibrio entre seguridad y libertad, al que pronto Chile tendrá que afrontar.	https://www.anepe.cl/wp-content/uploads/Cuaderno-de-Trabajo-N%C2%B09-2018.pdf	2018
ANEPE	Cuaderno de trabajo: ""Ciberinteligencia: Contextualización, aproximación conceptual, características y desafíos".	Este documento aborda la noción de "ciberinteligencia" como término que emerge en el marco de la existencia de una nueva dimensión en la que se efectúan las relaciones entre las personas, organizaciones e instituciones: el ciberespacio. En este contexto, es efectuada una aproximación teórica al término, identificándose el fenómeno al cual hace referencia, como también, describiendo algunas de las características que presenta y desafíos a abordar para el desarrollo de la ciberinteligencia.	https://www.anepe.cl/wp-content/uploads/Cuaderno-Trabajo-N%C2%B01-2018.pdf	2018
XVII Conferência dos Diretores dos Colégios de Defesa Ibero-Americanos - 2016	Libro: "Ciberdefesa e Cibersegurança: Novas Ameaças à Segurança Nacional"	Recopilación de artículos en los que se basaron las presentaciones efectuadas en el marco de la XVII Conferencia de Directores de Colegios de Defensa Ibero Americanos en 2016	http://www.asociacioncolegiosdefensaiberoamericanos.org/acdibero/LibrosReunionesDirectores/LIBRO+XVII+CONFERENCIA+-+CIBERDEFESA+E+CIBEREGURAN%	2016

			C3%87A+NOVAS+AMEA%C3%87AS+%C3%80+SEGUR....pdf	