AulaVirtual
Generando Conocimiento

ISSN: 2665-0398

Tipo de Publicación: Articulo Científico
Recibido: 30/11/2021
Aceptado: 18/12/2021
Autor: Jorge Luis Suarez Campos
Ingeniero Civil Electrónico
Especialista en Gerencia. Mención: Empresarial
Doctor en Gerencia Avanzada
Universidad Mayor
Santiago - Chile
https://orcid.org/0000-0002-7080-1423
E-mail: jorge.suarez@umayor.cl

VIGENCIA ONTOLÓGICA DE LA CIBERSEGURIDAD EN EL MARCO DE LA SEGURIDAD INFORMÁTICA CHILENA. CONVENIO DE BUDAPEST

Resumen

La evolución de la información y la comunicación ha traído cambios en la capacidad de acumular, transmitir y usar dicha información. Dentro de este contexto, el modo en que hoy día crecen los datos en volumen, celeridad y diversidad, debido al avance vertiginoso y el uso de las Tecnologías de la Información y la Comunicación (TIC) ha generado la necesidad de ayudar a las organizaciones a aprovechar sus datos y, de esta manera, utilizarlos para identificar nuevas oportunidades. La situación planteada demanda una visión de la ciberseguridad como tema obligatorio en cualquier empresa u organización. Desde esta perspectiva, el interés de la revisión documental, es dilucidar de forma crítica, la conceptualización de la ciberseguridad como un tema pertinente en la sociedad chilena, específicamente, en el ámbito de la seguridad informática; de allí la perentoriedad de que la misma, se encuentre inserta en la política nacional.

Palabras Clave: Ciberseguridad, seguridad informática, legislación chilena.

ONTOLOGICAL VALIDITY OF CYBERSECURITY IN THE FRAMEWORK OF CHILEAN COMPUTER SECURITY. BUDAPEST CONVENTION

Abstract

The evolution of information and communication has brought changes in the ability to accumulate, transmit and use such information. Within this context, the way in which data today grows in volume, celerity and diversity, due to the vertiginous advance and the use of the Technologies of the Information and Communication (ICT) has generated the need to help organizations to take advantage of their data and, in this way, use them to identify new opportunities. The proposed situation demands a vision of cybersecurity as a mandatory issue in any company or organization. From this perspective, the interest of the documentary review is to elucidate critically, the conceptualization of cybersecurity as a relevant topic in Chilean society, specifically, in the field of computer security; hence the urgency that it is inserted into national politics.

Keywords: Cybersecurity, computer security, Chilean legislation.

Preámbulo

Hoy en día, se percibe la necesidad de redimensionar la visión de las Tecnologías de la Información y la Comunicación (TIC), centrada en la incorporación de contenidos, métodos, prácticas y manejo de los datos pertinentes con el arribo de la sociedad de la información, las redes entre computadoras y la Internet. Este último fenómeno se ha caracterizado por convertirse, sin dejar lugar a dudas, en un factor clave para el crecimiento económico societal, así como también, en un recurso fundamental del cual, otros sectores económicos y productivos dependen, a saber, operaciones bancarias y financieras, tanto nacionales como internacionales, instalaciones y medios de transporte, el sector de energía y salud.

Ahora bien, los mencionados sectores están supeditados de forma directa e inmediata a la Internet, así como a las tecnologías de la información y de la comunicación (TIC), por lo cual, una debilidad en la red o una incidencia sobre la misma, pudiese significar una vulnerabilidad en cuanto a la seguridad. En consecuencia, es tácita la necesidad de planificar acciones que revistan a estos ciberespacios de una estrategia de ciberseguridad.

Dentro de este contexto, se hace inminente afrontar la complejidad de la ciberseguridad desde el discurrir reflexivo de un abordaje ontológico, que no deje de lado la realidad tecnológica inserta en estos tiempos de cambios. Es así como, la vertiginosa aceleración en el ritmo de creación y diseminación de los datos, hace que la protección de los mismos sea ineludible. Esta protección de la información o ciberseguridad incluye la compilación de estrategias y procesos que se encargan de la seguridad de los usuarios que intercambian información entre sistemas informáticos.

De tal manera que, esta sociedad del conocimiento les impone a las naciones, el reto de garantizar la seguridad de la información por vía tecnológica. En este transitar por el escenario innovador que involucra el manejo de la información, así como la protección de los datos de naturaleza informática, bien vale la pena formular la siguiente inquietud: ¿Es pertinente la significancia de la ciberseguridad como un tema vigente en la sociedad chilena, específicamente, en el ámbito de la seguridad informática?

En atención con la pregunta formulada, procuraré develar los significados sobre la asunción de la ciberseguridad, como acción fundamental para resguardar la seguridad de las personas y de sus derechos en el ciberespacio, por parte del gobierno chileno, además de la accesibilidad masiva a la información desde un entorno seguro y confiable, supeditado al uso pertinente de la Internet.

Hacia la Significancia de la Ciberseguridad

ISSN: 2665-0398

En la cotidianidad hablar sobre Ciberseguridad implica la vinculación de la información digital con las formas de proteger y mantener a resguardo, información en formato digital que nutre los sistemas de redes informáticas a nivel mundial. Por tanto, la protección se basa en el tratamiento de cualquier amenaza que pudiera generar riesgo en el trato de la información almacenada y empleada en diversos sistemas de datos enlazados en redes informáticas que se interconectan a través de una diversidad de dispositivos tecnológicos dentro del ciberespacio.

Desde esta óptica, Curtis (2011), describe al espacio cibernético, o ciberespacio, como un:

> Dominio artificial construido por el hombre, diferenciado de los otros cuatros dominios de guerra (tierra, aire, mar y espacio); aunque se haya formalizado recientemente, el ciberespacio puede afectar a las actividades en los otros dominios y viceversa. Además, el ciberespacio no está aislado sino profundamente vinculado y apoyado por medios físicos, por ejemplo, las redes eléctricas.

Entonces, el ciberespacio viene a constituir un espacio virtual en el cual se suscitan situaciones que, de alguna forma, inciden en el manejo de los datos. En esta dimensión se está creando la sociedad de la información en una espiral infinita que está confluyendo en la llamada sociedad del conocimiento. No obstante, este mismo hecho, ha generado vulnerabilidades en el tratamiento de los datos, lo que ha hecho susceptible al ciberespacio de amenazas informáticas y riesgos.

De tal modo que, surge la imperiosa necesidad de empresas, compañías tecnológicas, corporaciones, así como gobiernos, de evitar ataques cibernéticos, los cuales incluyen el robo de datos de clientes. Aduce Subijana (citado por Pons, 2017:82):

> A partir del desarrollo acelerado de la internet, también emerge el lado oscuro y surgen nuevos términos como cibercrimen, ciberdelito o ciberdelincuencia, que describen de forma genérica los aspectos ilícitos cometidos en el ciberespacio y que tienen cuatro características específicas: se cometen fácilmente; requieren escasos recursos en relación al perjuicio que causan; pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma; y se benefician de lagunas de punibilidad que pueden existir en determinados Estados, los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas.

Puede afirmarse que, el ataque cibernético se puede realizar desde cualquier parte del mundo, lo que ofrece al ciberdelincuente, varias ventajas, principalmente el anonimato. Sumado a lo expresado, se hace pertinente proporcionar privacidad a la información, a través de un conjunto de tecnologías, protocolos y procedimientos informáticos que protejan los

Volumen: 3, Número: 6, Año: 2022
Pp.: 132-148
http://www.aulavirtual.web.ve

datos. Por lo anterior, se puede tomar como referencia a Mendoza (2015: 1), quien argumenta:

> La norma ISO 27001 define el activo de información como los conocimientos o los datos que tienen valor para una empresa, mientras que los sistemas de información comprenden a las aplicaciones, servicios, activos de tecnología u otros componentes que permiten el manejo de la misma.

Desde esta perspectiva, la ciberseguridad abarca la protección de los activos de información o, lo que es lo mismo, la información digital que emerge y se comparte en los sistemas interconectados. En consecuencia, está comprendida dentro de la seguridad de la información. De tal manera que, cualquier tipo de ataque malicioso como: robos y brechas de seguridad, además de filtración de datos deben ser contrarrestados, con el fin último de dar seguridad al usuario y, por otro lado, llevarlo paso a paso en el continuo aprendizaje hacia la manera de identificar ataques que pretendan suplantar la identidad (phishing). También, se procura disminuir la cantidad de amenazas latentes, mediante el empleo de medidas ofensivas contra elementos dentro del mundo infinito de la virtualidad.

Detrás de los planteamientos anteriores destaca el hecho de que, el arma más destructiva hoy por hoy, en los medios informáticos e Internet son los ciberataques de diversa índole; estos producen una afectación a los usuarios particulares a nivel mundial, y causan pérdidas millonarias a empresas y gobiernos en todo el orbe. La Encuesta Mundial de Seguridad de la Información (2018), elaborada por PwC, refiere: “Las empresas de todo el mundo sufren, de media, 3,4 incidentes de seguridad al año, y unas pérdidas de 4,8 millones de dólares”.

Las cifras antes mencionadas están supeditadas al hecho de que, la masificación del fenómeno denominado Internet, así como también, la multiplicación de redes informáticas e información digital, han traspasado cualquier frontera imaginable. El constante auge en servicios de alojamiento de datos en la “nube”, además del envío de cantidades ingentes de data entre computadoras que se encuentran ubicadas en los cuatro (4) puntos cardinales de este planeta pero que, sin embargo, no dejan de enlazarse con infinidad de equipos informáticos repartidos en la inmensa geografía de los cinco (5) continentes, trae consigo la posibilidad de que individuos inescrupulosos usen esas distancias físicas y la inmediatez digital para cometer delitos y fechorías con el amparo del anonimato, sumado a una forma bastante complicada para rastrear de qué sitio de este gigantesco mundo se cometen dichos delitos.

En atención con estos planteamientos, Sullivan (2018:1), hace mención a siete (7) elementos de uso ineludible en la preparación en

ISSN: 2665-0398

seguridad cibernética, los cuales se parafrasean a continuación:

1. Plan de seguridad cibernética, que consiste en resguardar información personal de los clientes, así como la información financiera e información médica, toda ella protegida contra la sustracción y divulgación sin la debida y correcta autorización; además, la posibilidad de prevenir los cambios y modificaciones externas no realizadas por los autores originales de los datos dentro de la red.
2. Otra preparación a tener en cuenta es la gestión del riesgo, que pretende identificar información sensible, mediante un programa para identificar a personas, procesos de negocios y tecnologías críticas; esta gestión debe partir de la evaluación del entorno de inseguridad o riesgo que pudiese amenazar los activos críticos.
3. En el mismo tenor, se encuentra la gestión de la identidad, destinada a proporcionar un acceso adecuado a los recursos de información, mediante el empleo de planes, políticas, procedimientos y tecnología, entre ellos: control de acceso, autenticación, autorización y rendición de cuentas.
4. Monitorización de la red: una fuerte arquitectura en la seguridad de la red, el control de activos, configuración y cambios, como también, la creación de mapas de gestión de incidencias, prepara a cualquier organización para que adquiera un alto nivel de seguridad de los datos que transitan por su red interna. Asimismo, lo que sale de ésta hacia internet también va blindado contra los ciberdelincuentes y, por ende, contra las pérdidas voluntarias o involuntarias de los clientes y administradores de dicha red.

Los objetivos planteados inherentes a la preparación en seguridad cibernética son elementos esenciales que una empresa u organización requiere; lo antes expuesto, permite denotar que dado el caudal de información que emerge en las operaciones y uso de la red, se hace necesario un conocimiento absoluto de sus activos de información más relevantes; develar cómo funcionan sus sistemas de información y sus redes; comprender cómo sus sistemas de información apoyan las operaciones de negocios y, además, qué información está fluyendo hacia dentro, hacia fuera y a través de sus redes. Al estar cubiertos estos aspectos, una organización puede lograr la preparación en seguridad cibernética.

Adicional a los planteamientos anteriores, debe añadirse lo engorroso de recoger y procesar evidencia cuando el rastro del delito se pasea en cuestión de segundos entre un país y otro o, entre un continente y otro, pues la manera de llevar una investigación se vuelve un tanto compleja a nivel

Volumen: 3, Número: 6, Año: 2022
Pp.: 132-148
http://www.aulavirtual.web.ve

legal, fundamentalmente, si las legislaciones de los Estados implicados no están en consonancia, es decir, si cada país juzga los delitos dentro de su territorio completamente independiente de como lo pueda juzgar otra nación. Por esta razón, nace la iniciativa denominada Convenio de Budapest sobre Ciberdelincuencia.

El Convenio de Budapest sobre Ciberdelincuencia, desde la perspectiva de la Biblioteca del Congreso Nacional de Chile (2018:1), es un pacto de más de cincuenta y seis (56) países, la mayoría de Europa, que tiene por fin central, reglamentar una serie de legislaciones en diversas naciones, las cuales persigan, sancionen y castiguen a las personas que asuman conductas delictivas, a través del uso de medios electrónicos, digitales y virtuales. De manera remota, estos ciberdelincuentes pueden infringir Leyes en países donde físicamente no se encuentran, pero digitalmente sí. Este convenio sobre ciberdelincuencia, plantea la existencia de un estándar internacional; por ejemplo, se plantean los delitos mediante los siguientes puntos: acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataque a la integridad del sistema, abuso de los dispositivos, falsificación informática y fraude informático.

En relación con el ámbito chileno, la entrada por parte de este gobierno en el Convenio de Budapest, se da con la puesta en marcha de un proyecto de Ley que otorga una clasificación de los delitos informáticos y un abanico de sanciones, entre las que destaca la perturbación informática, la cual impone un castigo a los individuos que, de manera alevosa, actúen maliciosamente para obstaculizar o alterar el normal funcionamiento de los sistemas informáticos. Asimismo, al ser un instrumento internacional que pretende homogeneizar la forma en que los países signatarios definen los delitos cibernéticos, este convenio reúne de manera extensa las gestiones de los Estados, en pro de crear un marco que establezca en la legislación la manera de combatir estos flagelos. No todos los Estados enfrentan las mismas dificultades, ni poseen la misma transparencia y no todos los Estados garantizan el respeto a los derechos humanos.

El aludido acuerdo internacional establece la designación de un responsable que estará encargado de la ciberseguridad en cada uno de los servicios, así como la ejecución y constante evolución de procedimientos técnicos en cuanto a ciberseguridad. En este sentido y según el Convenio sobre Cibercrimen, los principales objetivos de este tratado son los siguientes:

1. La armonización de los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones conectadas al área de los delitos informáticos.

ISSN: 2665-0398

2. La prevención de los poderes procesales del derecho penal interno es necesaria para la investigación y el enjuiciamiento de esos delitos, así como otros delitos cometidos por medio de un sistema informático o pruebas en formato electrónico.
3. Establecimiento de un régimen rápido y eficaz de la cooperación internacional.

Al tomar en cuenta los anteriores objetivos, destaca, particularmente, la elaboración de una política penal común para proteger a las sociedades de ciberdelitos, a través de disposiciones afines al derecho penal; por mencionar algún ejemplo se encuentra la estafa informática, así como también, las diversas violaciones a la seguridad en los sistemas informáticos. De igual manera, incluye aspectos judiciales acerca de cómo conseguir evidencia en medios digitales y disposiciones de cooperación internacional.

Ciberseguridad en el Contexto Chileno

No puede negarse el compendio de ventajas que ha significado el avance de las tecnologías de la información en el contexto global. Sumado a la situación planteada, este progreso en el área informática ha traído consigo, el riesgo de que personas inescrupulosas se introduzcan sin autorización en dominios de sistemas de datos, así como también, exploten vulnerabilidades de seguridad de entornos digitales. Justamente es este escenario, el que demanda a los gobiernos instaurar una política de ciberseguridad que prevenga los riesgos, amenazas y ciberataques, pues en Chile, en la actualidad, aproximadamente el 70% de la población, además de navegar en la Internet en la búsqueda de información y utilizar las redes sociales, efectúan infinidades de operaciones bancarias, realizan compras on-line, cancelan sus impuestos y gestionan a diario, trámites en la web.

Dadas las ideas anteriores, es perentorio destacar que la seguridad en los espacios virtuales es un elemento esencial para la protección de los usuarios. Lo expresado encuentra explicación en el hecho de que, el debate sobre ciberseguridad está supeditado a la importancia de consolidar los valores democráticos, proteger los derechos humanos y respetar el derecho internacional. En la nación chilena, la Política Nacional de Ciberseguridad constituye una estrategia indispensable en el proceso de desarrollo de competencias, acciones y políticas inherentes a la seguridad informática.

No obstante, Sancho (2018), aduce lo siguiente respecto a la situación de la ciberseguridad en las naciones:

> El Índice Mundial de Ciberseguridad 2015, elaborado por la Unión Internacional de Telecomunicaciones (UIT) junto a la empresa ABI Research, ofrece una manera de medir el grado de desarrollo de la ciberseguridad en los países y busca promover una cultura de ciberseguridad y su incorporación

Volumen: 3, Número: 6, Año: 2022
Pp.: 132-148
http://www.aulavirtual.web.ve

> como factor clave de las Tecnologías de la Información y Comunicación (TIC). Se orienta a la cuantificación del compromiso de los países con relación a cinco factores: medidas jurídicas; medidas técnicas; medidas organizativas; creación de capacidades y cooperación internacional. Su finalidad es dar cuenta sobre la presencia de estructuras nacionales para implementar y promover la ciberseguridad. En esta medición, Chile se sitúa en el lugar N.º 16 del ranking, ubicándose después de varios países suramericanos como Argentina (N.º 15), Colombia (N.º 9), Uruguay (N.º 8) y Brasil (N.º 5). Este resultado es reflejo de la carencia de una Política Nacional de Ciberseguridad (PNCS) que se ha postergado por demasiado tiempo y varios gobiernos.

En cuanto a Chile, dentro de las estrategias contempladas en la Política Nacional de Ciberseguridad se tomó en cuenta una Política de Ciberdefensa para establecer las metas perentorias, a ser cumplidas progresivamente hasta el año 2022, por las organizaciones encargadas de la Defensa Nacional. Ahora bien, estas acciones de Ciberdefensa han estado supeditadas a una planificación propuesta desde el año 2015, la cual incluyó seminarios y plenarias en las que participaron miembros de las organizaciones de las Fuerzas Armadas, instituciones pedagógicas, sectores estatales, expertos en la temática y, representantes de la sociedad civil organizada.

Es oportuno señalar que el documento escrito referente a la Política de Ciberdefensa se compone de seis (6) apartados; al inicio se presenta el preámbulo, además de una diagnosis en la que se ponen de manifiesto, los peligros e inseguridades que está trayendo consigo el ciberespacio. Seguidamente, se estructuran las acciones estratégicas basadas en la Política de la Defensa Nacional con el propósito de minimizar los riesgos y amenazas del ciberespacio a la Seguridad Nacional. Dentro de estos principios se tomaron en cuenta aspectos como el uso de los medios, instrumentos y capacidades de Ciberdefensa, compromisos en su aplicabilidad y estrategias para la cooperación internacional. En síntesis, este texto compendia las acciones que el estado de Chile consideró pertinente para abordar los crecientes riesgos e inseguridades que representa el ciberespacio para la seguridad nacional, entiéndase, información, operaciones tácticas de defensa e infraestructura.

Desde esta perspectiva, Muñoz, director de la Academia Nacional de Estudios Políticos y Estratégicos de Chile (2018: 1), argumenta que, algunas líneas de acción que no deberían estar ausentes en la planificación del Estado Chileno en ciberseguridad, muchas de las cuales ya están en pleno desarrollo, se condensan en los siguientes planteamientos:

1. Establecer un organismo del Estado que centralice y lidere la ciberseguridad, con facultades y capacidades para lograr la

ISSN: 2665-0398

integración de todas las instituciones públicas y privadas que encabezan las áreas de infraestructura crítica.

2. Considerar en una estrategia global, la implementación en cada una de las áreas de infraestructura crítica, el diseño de planes y programas que permitan fortalecer la prevención, protección, mitigación, respuesta y recuperación.
3. Fomentar el desarrollo del capital humano y una cultura de ciberseguridad que llegue a todas las capas de la estructura social.
4. Fomentar la investigación y el desarrollo de soluciones tecnológicas propias, desarrolladas en Chile, asociadas a la ciberseguridad.
5. Desarrollar un marco legal que permita regular el uso responsable del ciberespacio.

Dado lo planteado, vale mencionar que la política de Ciberdefensa chilena se apoya esencialmente en la Política de Defensa del Estado, por lo que se regula por sus mismos axiomas y principios, aplicables, en su totalidad, al ciberespacio, a saber: preservar el territorio nacional; respeto a los derechos ciudadanos, a la soberanía y democracia, además del respeto a las relaciones jurídicas con otras naciones, ceñido también, a la abstención del uso y/o amenaza del empleo de la fuerza y a la legítima defensa; amparo y defensa de la población, sumado a la preservación de los intereses nacionales. Como emerge en las líneas anteriores, estas estrategias de Ciberdefensa tienen como norte, la puesta en práctica de maniobras y acciones basadas en la confianza y la transparencia que deben permear el uso del ciberespacio, situación ineludible para la mantención de la paz y la seguridad en Latinoamérica.

No obstante, a pesar de la mencionada Política Nacional de Ciberseguridad que se ha establecido en Chile, Partarrieu (2018: 1), aduce lo siguiente:

> Chile está bajo la media en inversión en ciberseguridad. De acuerdo con la International Data Corporation (IDC), en el 2017, apenas alcanzó un 0,07% del PIB, mientras que los países desarrollados superaron el 0,12%. A su vez, el crecimiento chileno en esta materia fue solo del 4,1% del 2016 al 2017, muy por debajo de aquellos que lideran la transformación digital a nivel mundial y que alcanzaron el 22%. Sumado a lo anterior, la baja inversión también se refleja en el índice de ciberseguridad global 2017 publicado por el ITU. En este, Chile, con un índice de 0,367, ocupa en América el puesto 12 y el 80 a nivel mundial. Mientras tanto, las principales deudas están en: definiciones estratégicas, agencias nacionales de gestión de incidentes, definición y cumplimiento normativo, programas de investigación y desarrollo, métricas de ciberseguridad, programas de formación y educación y la falta de programas de colaboración entre países, organismos y multisectoriales.

Volumen: 3, Número: 6, Año: 2022
Pp.: 132-148
http://www.aulavirtual.web.ve

Como se percibe en el planteamiento del anterior autor, los datos estadísticos permiten visualizar que la ciberseguridad chilena ostenta marcadas fisuras que suponen un riesgo nacional. Esta situación se vio evidenciada en los primeros meses de 2018, al registrarse diversos acontecimientos de ciberseguridad que propiciaron infinidades de reseñas, informes, declaraciones y acciones a realizar. Dentro de estos incidentes informáticos, relacionados con instituciones bancarias, destaca el asalto millonario al Banco de Chile, la fuga de datos de catorce mil (14.000) tarjetas de crédito, así como también, la filtración de una lista de usuarios de Banco Estado.

Lo anterior originó que se pusiera en marcha, un plan para cimentar un Sistema Nacional de Ciberseguridad, de la mano con otras acciones estratégicas, tales como designar a Jorge Atton como Asesor Presidencial de Ciberseguridad; la Superintendencia de Bancos e Instituciones Financieras (SBIF) pronunció un conjunto de procedimientos para fomentar la Ciberseguridad y, posteriormente, Chile y EEUU firmaron un acuerdo inherente a esta temática informática. De tal manera que, estos ataques cibernéticos permitieron evidenciar dos aspectos puntuales: en relación con la ciberseguridad, no se ha establecido una normativa jurídica específica que rija esta materia y, además, se hace necesario profundizar el interés en las empresas y organizaciones públicas y privadas sobre la relevancia de proteger el capital informático.

Convenio de Budapest: Inserción de Chile

El Convenio sobre Ciberdelincuencia, manejado ampliamente como Convenio de Budapest, es un acuerdo internacional inherente al ámbito penal, que determina los procedimientos jurídicos para luchar contra el crimen organizado; específicamente, tienen como propósito combatir los delitos cometidos, bien sea hacia sistemas o medios informáticos o, a través del empleo de los mismos. Este convenio establece en su preámbulo, la necesidad primordial de aplicar una política penal común entre sus miembros, así como de mejorar la cooperación internacional entre ellos con el fin de proteger a la sociedad frente a la ciberdelincuencia. Este tratado es calificado como un acuerdo que califica los esfuerzos de la Comunidad Internacional para fortificar el Estado de Derecho en el ciberespacio.

En tal sentido, la Biblioteca del Congreso Nacional de Chile (2018: 2), refiere que el principal objetivo del Convenio de Budapest:

> … es llegar a establecer una política penal común para proteger a la comunidad internacional frente a la cibercriminalidad. Junto al propósito de lograr una legislación específica, también busca la creación de nuevos mecanismos de cooperación transnacional frente a los delitos cibernéticos.

ISSN: 2665-0398

De lo expresado puede colegirse que, este convenio sobre Ciberdelincuencia es un acuerdo internacional que tiene como propósito, contrarrestar los ciberdelitos, en otras palabras, las transgresiones perpetradas por medio de Internet. Asimismo, persigue instaurar una reglamentación jurídica, además de las estrategias y procedimientos afines entre los países integrantes del Consejo de Europa y los invitados a participar en el mismo.

La mencionada biblioteca hace mención a que, el Convenio de Budapest tiene cuatro (4) capítulos, en los que, además de definirse una serie de terminologías en común, se establecen tres (3) ejes esenciales para hacer frente a los delitos informáticos, los cuales se destacan a continuación:

1. En el primer eje se aborda el tema de los delitos informáticos, y tiene como objetivo establecer un catálogo de figuras dedicadas a penar las modalidades de criminalidad informática. Es decir, en este capítulo se definen los delitos y se los clasifica en cuatro (4) categorías:
    a. Delitos que tienen a la tecnología como fin: son aquellos que atentan contra la confidencialidad, integridad o disponibilidad de la información. Por ejemplo, el daño informático, el acceso ilícito a un sistema, entre otros.
    b. Delitos que tienen a la tecnología como medio: se refiere a delitos ya conocidos, que se cometen a través de un sistema informático. Son delitos comunes, que ya se encuentran tipificados en la mayoría de las legislaciones, ampliados a los medios digitales. Por ejemplo, el fraude informático o la falsificación de datos digitales.
    c. Delitos relacionados con el contenido: establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil.
    d. Delitos relacionados con infracciones a la propiedad intelectual: se refiere a la reproducción y difusión en Internet de contenido protegido por derechos de autor, sin la debida autorización. Por ejemplo: infracciones a la propiedad intelectual, piratería, entre otros.
2. En el segundo eje se abarcan las normas procesales: aquí se establecen los procedimientos para salvaguardar la evidencia digital, así como también, las herramientas relacionadas con la manipulación de esta evidencia. El alcance de esta sección va más allá de los delitos

Volumen: 3, Número: 6, Año: 2022
Pp.: 132-148
http://www.aulavirtual.web.ve

definidos en el punto anterior, dado que aplica a cualquier delito cometido por un medio informático o cualquier tipo de evidencia en formato electrónico. Entre otras cosas, determina la obtención y conservación de datos digitales para ser utilizados como pruebas.

3. El último eje contiene las normas de cooperación internacional, que son reglas de cooperación para investigar cualquier delito que involucre evidencia digital, ya sean delitos tradicionales o informáticos. Incluye, entre otras, disposiciones acerca de la localización de sospechosos, recolección o envío de evidencia digital, e incluso lo referente a extradición.

En consecuencia, en los países que ya son parte del Convenio, las acciones deberían estar centradas en la ejecución de cada uno de los ejes establecidos en este acuerdo internacional. La prioridad es instaurar de forma específica, las medidas, garantías y protecciones que no han sido contempladas en el texto de la Convención; lo anterior, amerita tener presente las normas constitucionales de cada país, del sistema interamericano y de resguardo de datos personales que permiten diseñar el resguardo de los derechos humanos de los ciudadanos, con la finalidad de que las pericias de investigación de las naciones no converjan en una violación de la privacidad, la libertad de expresión y demás derechos expuestos a la luz pública.

En atención con la temática que atañe a la presente revisión documental, es pertinente mencionar lo planteado por el Ministerio de Relaciones Exteriores de Chile (2017: 1), en cuanto a que, en sesión del 16 de noviembre de 2016, el Senado aprobó la entrada de Chile al Convenio de Budapest por veintidós (22) votos a favor. A la fecha ha sido ratificado por cincuenta y tres (53) Estados:

> La adhesión a este instrumento internacional constituye uno de los compromisos del Gobierno de Chile y es una de las medidas comprometidas en la Política Nacional de Ciberseguridad. Permitirá al país ser parte de un sistema rápido y eficaz de cooperación internacional, además de recibir asistencia para el desarrollo de capacidades nacionales para enfrentar de mejor manera las amenazas en el ciberespacio. A partir del 1° de agosto del 2017, tres meses después del depósito, Chile fue el miembro número 54 del Tratado y el primero en Sudamérica.

La directiva o gerencia que se encargará de cada uno de los aspectos inherentes a la Ciberseguridad, en el espacio chileno país será la Fiscalía de Chile y sólo lo que tiene que ver con extradiciones de personas estará a cargo del Ministerio de Relaciones Exteriores, aunque, claro está, su única competencia estará vinculada con el hecho de redirigir cada uno de los casos a la

ISSN: 2665-0398

fiscalía. Chile, al convenir acogerse al mencionado acuerdo internacional de Ciberseguridad, se ha comprometido a incorporar los artículos 2 al 10 del mismo, a la legislación interna, pero ha determinado algunas excepciones que pudiesen ocasionar diversas problemáticas en materia jurídica, dada la situación planteada.

De lo expresado se deduce la relevancia de que Chile haya firmado el Convenio de Budapest, como primer acuerdo internacional que combate los ataques cibernéticos, vigente desde 2004. En tal sentido, el Estado Chileno, a raíz de su adherencia a este convenio de ciberseguridad, se ha planteado la transformación de los procedimientos y estrategias para prevenir la vulneración de sus sistemas de seguridad, dado que, entre los años 2009 y 2013 se registraron tres mil sesenta y tres (3.063) casos de delitos tecnológicos. Lo anterior, pudiese estar supeditado a la poca normativa jurídica, tanto en el contexto chileno como internacional, que entorpece juzgar y castigar a los ciberdelincuentes, al cometer estas infracciones informáticas, no sólo en el espacio chileno, sino fuera de éste, lo que dificulta el trabajo y la acción de los cuerpos de seguridad.

Marco Jurídico Chileno Vinculante a la Ciberseguridad

En Chile, está presente la Ley 19.223, que sanciona los delitos informáticos. Esta normativa jurídica se compone de cuatro (4) artículos:

Artículo 1º. El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2º. El que, con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3º. El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4º. El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

Es oportuno señalar que, el mencionado documento legal fue refrendado en 1993, por lo que ha quedado rezagado respecto con el vertiginoso avance de la tecnología en los últimos tiempos. A tal situación se suma que, desde la

Volumen: 3, Número: 6, Año: 2022
Pp.: 132-148
http://www.aulavirtual.web.ve

referida fecha, la Ley no ha recibido ninguna modificación. De hecho, Maldonado (citado por Zapata, 2018:1), acota que Chile no se ha manifestado de forma perentoria respecto con la legislación de ciberseguridad y señala lo siguiente:

> La Ley N.º 19.223, que es la que tipifica aquellas acciones constituyentes del ámbito informático, fue creada en 1993 y desde esa fecha hasta hoy no ha sufrido ningún tipo de modificación, lo que implica que la normativa, en definitiva, ya no da el ancho respecto de aquellas acciones que han aparecido en el último tiempo. Reconoce que el Convenio de Budapest obligará al país, a realizar mejoras, porque es necesario que todas estas Leyes sean actualizadas o creadas para dar respuesta a este nuevo escenario de cibercrimen.

Dado lo planteado, en Chile, la Ley N.º 19.223 se creó con la intención de regular y sancionar los diferentes delitos de carácter informático mediante un solo instrumento jurídico. No obstante, al procurar cubrir sin excepción las diferentes formas de delincuencia informática, por exceso ha llegado a cubrir otras conductas que no tienen nada que ver con ataques cibernéticos, mientras que, por otro lado, ha sido insuficiente en el ámbito tecnológico.

Otro aspecto que debe tomarse en cuenta es que, a pesar de que Chile, en su momento, fue la primera nación latinoamericana precursora en incluir en su normativa jurídica, una legislación que regulara los delitos del ámbito digital o informático, esta circunstancia se ha visto asediada por una transformación verdaderamente radical en lo que a avance tecnológico se refiere. A tal referimiento, Díaz (citado por Herrera, 2018:1), argumenta:

> En la actualidad, lamentablemente, la informática se mueve mucho más rápido que la legislación, por lo que Chile necesariamente va a tener que actualizarse en relación a las figuras que, al día de hoy operan pero que la legislación no las cubre.

En tal sentido, puede colegirse que los estatutos chilenos vigentes no tienen tipificadas infracciones habituales, tales como la clonación de la banda magnética de tarjetas, entiéndase “phishing”, delito que implica una substitución digital para obtener claves e información privada de un usuario. Dicha situación genera que los cuerpos de seguridad, al enfrentarse a un delito informático no plasmado en la Ley respectiva, deban procurar acercarse a la figura penal que sea colindante con la contravención suscitada y, de esta manera, determinar sus causas. Ahora bien, si la infracción traspasa las fronteras, se requerirán instrumentos jurídicos sólidos para que el delito o ataque cibernético no quede impune.

Consideraciones Reflexivas de Cierre

Las personas, habitantes y ciudadanos de cualquier país amparado en Leyes, requieren un nivel de seguridad informática, un resguardo de redes y sistemas informáticos dentro de los

ISSN: 2665-0398

sectores público y privado que garantice un fluido desarrollo de sus actividades personales, sociales y profesionales en el ciberespacio, además de velar por la continuidad operacional de los servicios básicos. Al mismo tiempo, estos usuarios deben ejercer sus derechos fundamentales como residentes de esa nación, entre ellos: la libertad de expresión, el acceso a la información, la protección de la vida privada y la propiedad.

Desde este punto de referencia, la construcción cognoscente presente se interpreta en el aporte académico y reflexivo desde los párrafos antes reseñados, en los cuales se destaca la actual situación de la ciberseguridad en el ámbito chileno. En tal sentido, la Política Nacional de Seguridad, es la norma legal y reglamentaria que establece, entre otros aspectos, el proceder legal para las acciones que se encuentren enmarcadas como ataques a la seguridad de las personas, de las instituciones, organismos adscritos al gobierno nacional y la seguridad de la nación. Dichos estatutos reglamentarios los constituyen, la Ley N.º 19.223, la cual actúa frente a los delitos informáticos y la otra es la Ley N.º 19.628, que se refiere a la protección de la vida privada de los ciudadanos.

Sumado a lo expresado, los sistemas de información relacionados con la defensa nacional chilena establecen una infraestructura primordial para la soberanía de la nación; por ello, en el año 2017, el Ministerio de Defensa preparó y publicó políticas específicas de Ciberdefensa, así como también, definió acciones en torno a la protección de redes, además de la colaboración para formar un espacio en lo cibernético que sea de carácter libre y seguro para cada uno de los usuarios.

A modo de síntesis, vale referir que es deber del Estado chileno, concebir la ciberseguridad como un tema pertinente en la sociedad chilena que, por tanto, amerita de un marco regulatorio específico, el cual tipifique cada uno de los delitos informáticos, así como también, el alcance de las sanciones en atención con el tipo de infracción. Adicional a este planteamiento, deben establecerse estándares y exigencias supeditados al ciberespacio dentro del país. Lo expresado amerita, además, tipificar suficientemente las infracciones cibernéticas, así como también, determinar las sanciones y penas acordes a los delitos informáticos, en atención con la relevancia y alcance de los mismos.

Visión Crítica de la Ciberseguridad en el Escenario Chileno

La relevancia de la temática planteada, producto de la comprensión e interpretación que emergió de la revisión bibliográfica pertinente, en relación con el abordaje de la ciberseguridad, como acción fundamental para resguardar la seguridad de las personas y de sus derechos en el ciberespacio, por parte del gobierno chileno, refleja la opinión del autor en cuanto a los aspectos siguientes:

Volumen: 3, Número: 6, Año: 2022
Pp.: 132-148
http://www.aulavirtual.web.ve

1. El Estado debe organizar la elaboración de informes sobre ciberseguridad que permitan edificar una legislación pertinente y cónsona con la nueva sociedad de la información, por lo cual, se hace necesario realizar una revisión exhaustiva de la regulación jurídica vigente inherente a los delitos e infracciones informáticas, así como también, efectuar un análisis minucioso de la infraestructura crítica que posee Chile, es decir, cuáles son sus vulnerabilidades y, por ende, la forma en cómo se va a abordar la ciberseguridad, dados los continuos avances en materia informática.

2. En la misma línea, es perentorio garantizar que el entorno digital sea de acceso libre; además, el camino al mismo debe ser seguro, por lo que los ciudadanos chilenos necesitan contar con las herramientas suficientes y prácticas para que el intercambio de información en las redes sea confiable. Para ello, deben estructurarse acciones y propuestas asociadas a materias legislativas, consustanciadas con las tácticas y estrategias operativas para lograr una mejor seguridad en el ciberespacio.

3. Otro aspecto a tener en cuenta es que, el gobierno chileno debe ponerse como principal objetivo estratégico, crear un plan que permita obtener respuestas efectivas y reales ante la falta de seguridad en las redes. Esto precisamente por la frecuencia, cantidad y, además, los efectos en los incidentes de seguridad informática que van cada vez en mayor incremento y, en consecuencia, pasan a formar una amenaza total para el correcto y normal funcionamiento de los sistemas de información y comunicación.

4. En síntesis, la ciberseguridad nacional debe ser coordinada al más alto nivel de gobierno, dado que se amerita un ente que coordine, posea atribuciones y maneje los recursos necesarios para llevar a cabo, planes que potencien el intercambio de información; para ello, es menester actualizar toda la infraestructura tecnológica del Estado, con la finalidad de realizar luego, una campaña masiva por los diversos medios de comunicación, llamando a la ciudadanía a emplear los fundamentos legales contra los ciberdelitos.

Referencias

Biblioteca del Congreso Nacional de Chile. (2018). Convenio N.º 185, del Consejo de Europa, sobre la Ciberdelincuencia (Convenio de Budapest). Disponible en: https://www.widefense.com/ciberseguridad-en-donde-esta-chile/.

ISSN: 2665-0398

Curtis, L. (2011. Introduction to cyberspace operations. Disponible en: https://doctrine.af.mil/download.jsp?filename=312-D01-CYBER-Introduction.pdf.

Herrera, C. (2018). Ciberseguridad: ¿Es suficiente la actual legislación para evitar y sancionar delitos informáticos? Disponible en: https://www.diarioconcepcion.cl/ciudad/2018/08/06/ciberseguridad-es-suficiente-la-actual-legislacion-para-evitar-y-sancionar-delitos-informaticos.html.

Ley N.º 19.628 sobre protección de la vida privada. (1991).

Ley N.º 19.223. (1993). 7 de junio de 1993.

Mendoza, M. (2015). ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia. Disponible en: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/.

Muñoz, L. (2018). Ciberseguridad, un nuevo desafío para Chile. Disponible en: http://www.estrategia.cl/texto-diario/mostrar/1183990/ciberseguridad-nuevo-desafio-chile.

Partarrieu, C. (2018). Ciberseguridad: ¿en dónde está Chile? Disponible en: https://www.widefense.com/ciberseguridad-en-donde-esta-chile/.

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *Revista Latinoamericana de Estudios de Seguridad*, N.º 20, Quito, junio 2017, pp. 80-93. RELASEDOR y FLACSO Sede Ecuador.

PwC. (2018). Encuesta Mundial de Seguridad de la Información. Disponible en: https://www.pwc.es/es/digital/encuesta-mundial-ciberseguridad-2018.html.

Sancho, C. (2018). Ciberseguridad y política pública en Chile: Avances recientes, ¿optimismo futuro? Disponible en: https://www.anepe.cl/ciberseguridad-y-politica-publica-en-chile-avances-recientes-optimismo-futuro/.

Sullivan, P. (2018). Lograr la preparación en ciberseguridad: Qué deben saber las empresas. Disponible en: https://searchdatacenter.techtarget.com/es/consejo/Lograr-la-preparacion-en-ciberseguridad-Que-deben-saber-las-empresas.

Zapata, L. (2018). Las deudas de Chile en materia de ciberseguridad. Disponible en: https://www.latercera.com/nacional/noticia/las-deudas-chile-materia-ciberseguridad/199971/.