ISSN 0798 1015

REVISTA ESPACIOS

HOME Revista ESPACIOS ÍNDICES / Index A LOS AUTORES / To the AUTHORS

Vol. 39 (Nº 39) Año 2018 • Pág. 31

# Seguridad hemisférica latinoamericana adaptada a las nuevas tecnologías: Ciberseguridad y avances de cooperación regional e internacional para la sanción del ciberdelito

## Latin American hemispheric security adapted to new technologies: Cybersecurity and advances in regional and international cooperation for the sanction of cybercrime

Hugo J. CASTRO Valdebenito 1; Alessandro MONTEVERDE Sánchez 2

Recibido: 05/04/2018 • Aprobado:30/05/2018

**Contenido**



**RESUMEN:**
El estudio centra su atención en la evolución y transformación del concepto de Seguridad Hemisférica, desarrollándolo histórica y conceptualmente, pretendiendo profundizarlo al utilizar las Teorías de las Relaciones Internacionales y vincularlo con la aparición de la Ciberseguridad como preocupación regional y mundial. Haciendo hincapié en las estrategias de Seguridad latinoamericanas y la Política Hemisférica al efecto, se argumenta utilizando fuentes de primer y segundo orden, respecto de los usos, niveles, modelos y dimensiones de la Ciberseguridad en la Política Hemisférica Latinoamérica, en el marco de las estrategias diseñadas para la detección, persecución y sanción del ciberdelito, así como también, los problemas presentes en aspectos de homogenización jurídica de los países de la región.
**Palabras-Clave:** Ciberseguridad; Ciberdelincuencia; Política hemisférica; Latinoamérica

**ABSTRACT:**
The study focused on the attention and transformation of the concept of Hemispheric security, developing it historically and conceptually, intending to deepen it by using the Theories of International Relations and linking it with the emergence of Cybersecurity as a regional and global concern. Emphasizing the strategies of security policy and politics, the use, arguments, uses, levels, models, the dimensions of Cybersecurity in Politics, the strategies of Latin America , to the framework of the strategies for the detection, prosecution and sanction of cybercrime, as well as, the present problems in the aspects of legal homogenization of the countries of the region.
**Keywords:** Cybersecurity; Cybercrime Hemispheric policy; Latin America

# 1. Introducción

Hoy y hace varios años ya, el mundo está marcado por el proceso de la globalización. Y por ende, es difícil no considerar dicho proceso como una variable dependiente, frente a cualquier análisis en Relaciones Internacionales. Es innegable - por cierto - la importante y veloz interacción entre las dimensiones políticas, económicas, incluso sociales y étnicas, de carácter mundial, que modifican las estructuras por sobre los procesos de carácter local. Aunque no se trata de un fenómeno reciente, ya

que la globalización posee sendas raíces históricas, el efecto que ha provocado en las últimas décadas ha sido de gran relevancia en las diferentes transformaciones que han vivido las relaciones entre actores los internacionales.

No cabe duda de que la globalización entrega buenas oportunidades para el desarrollo de los países. Y éstos con el tiempo, han comprendido que deben diseñar sus estrategias nacionales en virtud de este proceso, considerando las diversas oportunidades que les ofrece. No obstante ello, la globalización plantea grandes riesgos originados en nuevas fuentes de inestabilidad tanto económica como socio-política. Existiendo riesgos de exclusión para aquellos países que no están bien preparados para las fuertes demandas de competitividad, propias del mundo contemporáneo, y riesgos de acentuación de la heterogeneidad estructural, entre empresas, sectores sociales y regiones dentro de los países que se integran de manera segmentada a la economía mundial. Muchos de estos riesgos obedecen al carácter sesgado e incompleto de la agenda internacional que acompaña al proceso de globalización (Ocampo, 2004: 3).

En ese contexto de riegos y amenazas, producidos mayormente por la globalización, se situá el problema de las Nuevas Amenazas o Amenazas-No Convencionales (Chillier y Freeman, 2005), que afectan la seguridad de los Estados, a partir de la utilización de los espacios de vulnerabilidad producidos por la dependencia de las sociedades contemporáneas a los sistemas de información (Bejarano,2011: 52-54). A pesar de los diferentes riegos que significan para una sociedad cada vez más interconectada digitalmente y cada vez más alejada de los tradicionales procedimientos, la tendencia parece ser imparable.

Los riesgos y amenazas son numerosos y dinámicos. Entre ellos destacan, una mayor y más compleja actividad delictual que se desarrolla transnacionalmente por organizaciones o incluso individuos y que afectan directamente la seguridad nacional (Artiles, 2010: 169). También, se observa el aumento de actividades terroristas, de espionaje y sabotaje o robos de información privilegiada, que utilizan el Ciberespacio y las plataformas de información para enriquecerse afectando no solo la seguridad nacional de los Estados, sino también a Empresas Multinacionales (EMN), Organismos Internacionales Gubernamentales (OIG), No Gubernamentales (ONG) e incluso a los mismos individuos nacionales.

De esta manera, la globalización ha significado una dicotomía en cuanto al desarrollo de los países, pues por un lado, incentiva las relaciones políticas y comerciales beneficiando a los países más competitivos, y por el otro, se plantea como un escenario propicio para el desarrollo de actividades atentatorias contra la Seguridad de los Estados y sus nacionales.

En el presente estudio centra su atención en la evolución y transformación del concepto de Seguridad Hemisférica, desarrollándolo histórica y conceptualmente, pretendiendo profundizarlo al utilizar las Teorías de las Relaciones Internacionales y vincularlo con la aparición de la Ciberseguridad como preocupación regional y mundial. Haciendo hincapié en las estrategias de Seguridad latinoamericanas y la Política Hemisférica al efecto, se argumenta utilizando fuentes de primer y segundo orden, respecto de los usos, niveles, modelos y dimensiones de la Ciberseguridad en la Política Hemisférica Latinoamérica, en el marco de las estrategias diseñadas para la detección, persecución y sanción del ciberdelito, así como también, los problemas presentes en aspectos de homogenización jurídica de los países de la región

## 1.1. Desde un concepto de seguridad tradicional a una política hemisférica de seguridad multidimensional.

La seguridad hemisférica posee múltiples dimensiones. Algunos fenómenos como la transnacionalidad, la delincuencia cibernética, el ciberespacio, el terrorismo, entre otros elementos, no solo han modificado y condicionado la agenda internacional actual, sino que resumen, en materia de Ciberseguridad las características complejas de la sociedad internacional globalizada, por tanto se convierten obligadamente en un foco de reflexión, análisis y critica de gran relevancia para las Relaciones Internacionales.

Uno de los aspectos más destacables del siglo XXI, es la llamada revolución de las comunicaciones (Morandé & Aguirre, 2016). Dicha revolución, ha puesto en evidencia la necesidad de observar con mayor atención las interacciones humanas en el ciberespacio, al mismo tiempo que pone el foco en la seguridad de estas interacciones. La tradicional Seguridad se ha adaptado tras un largo proceso internacional, al punto que hoy las principales preocupaciones de los bloques regionales y los Estados, es resguardar, legislar y combatir las amenazas que subsisten en dicho Ciberespacio. El proceso de transformación de un concepto de Seguridad unidimensional a uno multidimensional obedece a esta transformación y tiene una evolución histórica que es importante considerar.

Desde el principio de la Guerra Fría (1947 – 1991), se inició en América Latina la construcción de un sistema interamericano, que a instancias del *Tratado Interamericano de Asistencia Recíproca* (TIAR), la

*Organización de Estados Americanos* (OEA) y bajo el patrocinio de Estados Unidos como potencia hegemónica occidental, fue incorporando en la política hemisférica una noción de Seguridad de especiales características para la región. Desde la conformación de la *Junta Interamericana de Defensa* (JID) en 1942, hasta la Declaración de Bridgetown en 2002, la noción de "Seguridad Hemisférica", emanada de aquel sistema ha sufrido una notoria evolución (Ibarra & Nieves, 2016: 3-4).

Desde la conformación de *la Conferencia Especial de Seguridad de México* de 2003, los Estados Miembros de la OEA acordaron ampliar el concepto de seguridad, adoptando un enfoque multidimensional, lo que ha permitido cubrir y categorizar un amplio abanico de nuevas amenazas o amenazas no-convencionales. Particularmente – y teniendo como antecedente principal los trabajos de la *Convención Interamericana contra el Terrorismo* de 2002-, se ha asumido que el terrorismo, los ataques a la seguridad cibernética, el Ciberdelito/ Cibercrimen y las amenazas de la utilización ilegal y maliciosa del ciberespacio en general como elementos centrales en la preocupación de los Estados americanos.

En esa misma línea, la OEA desde la creación del *Comité Interamericano contra el Terrorismo* (CICTE) ha impulsado diferentes instancias con el objeto de cohesionar la participación de los gobiernos de los Estados miembros, en conjunto con el sector privado y la sociedad civil para identificar las necesidades regionales y nacionales de Ciberseguridad y la formulación de estrategias ad hoc con las realidades y desigualdades de cada Estado Miembro, respecto al avance de las TIC y sus escenarios de vulnerabilidad cibernética.

El mundo actual, el de la globalización y la mundialización de los mercados, el comercio y las finanzas, está indudablemente, altamente interconectado digitalmente. Los Estados necesitan resguardar las libertades y asegurar el libre ejercicio de los derechos de los ciudadanos. Bajo esa misma idea, el Estado depende y se apoya inevitablemente en la tecnología, se adecua y actualiza sus procedimientos en pos del Internet. La preocupación de los Estados, entonces se ve en las implicancias de Ciberespacio en los asuntos internacionales. Esto ya era anticipado por algunos teóricos de las Relaciones Internacionales en los años 90s, tales como Keohane, Nye y Castells (Morandé y Aguirre, 2016).

La tendencia, según el Informe de Ciberseguridad 2016, elaborado por la OEA y el BID, asegura que la vigilancia estatal sobre las actividades y plataformas públicas y privadas que utilizan el ciberespacio condiciona su efectividad en la utilización eficiente y confiable de los recursos tecnológicos disponibles.

La Seguridad, como tal, tanto interna como externa, es responsabilidad intrínseca del Estado. La Seguridad fue, es y será un objetivo ineludible en la actuación del Estado, a pesar de que su significado y alcance se hayan modificado al compás de las transformaciones de la sociedad internacional y la globalización. Como señalábamos, anteriormente, entre 1942 (JID) y 2002 (Bridgetown), la noción de "Seguridad Hemisférica" emanada de aquel sistema, ha sufrido una importante y evidente evolución histórica. Bajo la triada TIAR–OEA-EE. UU se fue cimentando una noción de Seguridad mucho más amplia y compleja para la región.

En pocas palabras se construyó una arquitectura de Seguridad como reflejo de la polarización fáctica de la Guerra Fría (Leal,2003: 77). En la actualidad, el concepto de Seguridad, entendido como un elemento fundamental en la agenda internacional, se compone de nuevas y diversas dimensiones conceptuales, que se suman a las consideradas tradicionales, como son la militar y la política. Incluso hoy podemos decir que la Seguridad, es el elemento de análisis preponderante en las Relaciones Internaciones.

En estos términos, es fácil percatarse que las políticas públicas de los Estados -cada vez más impregnadas por la variedad de elementos que hacen y conciben a la Seguridad-, están obligadas a observar los cambios impuestos por la sociedad de la información, cada vez más llena de riesgos. Luego de los atentados terroristas del 11 de setiembre de 2001 (11-S) en New York, el terrorismo se ha posicionado como una de las prioridades de la seguridad nacional de Estados Unidos, se *"reorientaron sus prioridades en términos de prevención de conflictos y de la construcción de paz",* y la OEA inició el camino de la multidimensionalidad de la seguridad (Serbin, 2010).

La idea de la *Sociedad de la Información*, en la que es fundamental la noción de autodeterminación y autonomía en línea, respecto de la libertad informática de los individuos, implica contemplar y vigilar los elementos del ciberespacio, procurando alcanzar la gobernanza de Internet.

En 2002 fue aprobada en el seno de la OEA, la Convención Interamericana contra el Terrorismo, cuyo objetivo es "*prevenir, sancionar y eliminar el terrorismo". Para tal efecto, los Estados Parte "se comprometen a adoptar las medidas necesarias y fortalecer la cooperación entre ellos, de acuerdo con lo establecido en esta Convención (CICT, 2002)"*

En la Declaración de Bridgetown de 2002, los Estados miembros de la OEA concilian una Seguridad Hemisférica, e incluyen un enfoque multidimensional en el que reconocen: *"(...) que las amenazas, preocupaciones y otros desafíos a la seguridad del hemisferio son de naturaleza diversa y alcance*

*multidimensional y que el concepto y enfoque tradicionales deben ampliarse para abarcar amenazas nuevas no tradicionales, que incluyen aspectos políticos, económicos, sociales, de salud, ambientales*" (AG/DEC. 27 (XXXII-O/02), 2002)

En la *Declaración sobre Seguridad en las Américas de la Conferencia Especial de Seguridad de México* de 2003, se amplío el concepto de "seguridad hemisférica" aplicando el encuadre multidimensional, y colocando su eje en la protección de la persona humana.

De esta forma comenzó a cimentarse una arquitectura flexible de Seguridad, con miras al futuro tecnológico y contextualizado en la globalización contemporánea. Existe consenso académico en que el fin de la Guerra Fría marcó una perspectiva de defensa hemisférica diferente a la de los años cuarenta (Salazar; 2002: 34-35). El concepto de *nuevas amenazas o amenazas no convencionales,* se alineo con el de la sociedad de la información (Flores et al, 2007:19-20) y sus vulnerabilidades para la Seguridad Nacional. En la citada Declaración sobre Seguridad en las Américas, se listan no taxativamente lo que se considera por *"nuevas amenazas, preocupaciones y otros desafíos de naturaleza diversa".*

Armerding (2006) entiende que en realidad la denominación "nuevas amenazas" debiera corresponder a "amenazas no tradicionales" y pone como ejemplo el terrorismo, el narcotráfico y el crimen organizado. Afirma que a pesar de haber cierta aquiescencia sobre la denominación, no son fenómenos "estrictamente" nuevos en la región. Lo que puede realmente considerarse nuevo es el contexto mundial globalizado, algunos actores internacionales, la tecnología para transmitir sus efectos y la "multiplicación de sus consecuencias".

Asegura que *"lo novedoso de dichos fenómenos entonces, no es su existencia, sino el hecho de que se han transnacionalizado, y han asumido una magnitud y un alcance que trascienden las previsiones y pautas con que tradicionalmente se enfocan las cuestiones de seguridad interior, defensa nacional y seguridad internacional."* (Armerding, 2006)

Reconociendo la transnacionalidad de los riesgos que afectaban la región, el Consejo Mercado Común (CMC) aprobó en 1999 el *Plan General de Cooperación y Coordinación Recíproca para la Seguridad Regional* en el MERCOSUR, la República de Bolivia y la República de Chile, en el que involucró a las Fuerzas de Seguridad y Policiales, a fin de propender a la generación de mecanismos de prevención y control en materia de seguridad. Identificando especialmente dentro del ámbito delictivo - entre otros - al terrorismo y al Cibercrimen.

Incluir al terrorismo transnacional y el Cibercrimen en la agenda de Seguridad en MERCOSUR, fue una decisión que se tomó a raíz de los ataques contra la embajada israelí en Buenos Aires en 1992, y la Asociación Mutual Israelita Argentina (AMIA), en 1994. Aunque la mayor trascendencia del GTE fue resultado de la Declaración conjunta de los Ministerios de Interior y Justicia del Mercosur, el 28 de setiembre de 2001, en la que rechazaban los ataques terroristas del 11-S y anunciaban la extensión del trabajo conjunto en contra de las nuevas formas de amenazas al sistema internacional. A través de la modificación del Plan General para la Seguridad Regional, el GTE fue complementado por el Grupo de Trabajo Permanente, al que a partir de ese momento se encontrará subordinado (Flemes,2004: 23-25).

Además de casi una veintena de variados temas en los que puso su énfasis la Tercera Cumbre de las Américas en la ciudad de Québec en abril de 2001, su Plan de Acción incluyó la seguridad hemisférica y la lucha contra el terrorismo. A raíz de los atentados del 11S, el 21 de setiembre de 2001 en la XXIII Reunión de Consulta de Ministros de Relaciones Exteriores, se adoptó la Resolución para el Fortalecimiento de la Cooperación Hemisférica para Prevenir, Combatir y Eliminar el Terrorismo, condenando los ataques terroristas perpetrados, y recordando la Declaración de Principios de las Cumbres de las Américas de Miami, la de Santiago y la de Quebec. En 2002 se aprobó en el seno de la OEA - a impulso de Estados Unidos -, la Convención Interamericana Antiterrorista, en la que los Estados se comprometen a colaborar en la lucha contra el terrorismo. Dentro del ámbito de acción militar en defensa -considerada un área básica y tradicional en el ejercicio soberano de un Estado- la lucha contra el terrorismo que se inició el 11-S, ya difícilmente distingue entre la seguridad interna y externa de un Estado. De hecho, la guerra contra el terrorismo se ha ampliado de tal manera que implica lo que Wæver denomina "redes directas de apoyo", incorporando a la agenda de seguridad variados temas incentivando la coordinación internacional (Wæver, 2009: 96).

El yihadismo global reinventándose a través del ciberterrorismo, suma a la agenda internacional de seguridad actual, un nuevo reto a la sociedad de la información. El autodenominado "Ciber Ejército del Califato", rama de guerra cibernética del Estado Islámico, declaró estar preparado para provocar un "Armagedón cibernético" con el fin de hacer colapsar infraestructuras informáticas críticas occidentales que sin duda afectarían nuestra región. En respuesta a este escenario, en 2015 EE.UU. presentó su nueva política de Ciberdefensa, una estrategia de disuasión que permite determinar el origen de toda agresión que provenga desde Internet de cara a proteger información sensible. Esta estrategia,

ejecutada por el Comando Cibernético creado en el 2009 con objetivos ofensivos- defensivos, también contempla la posibilidad de ejecutar acciones defensivas, siempre y cuando, se haga para "proteger los intereses de Estados Unidos."

Resulta interesante recurrir al análisis de Kaldor (2001), en el considera la noción de "guerras virtuales y del ciberespacio" en función de lo que califica como revolución en las relaciones sociales de la guerra, como consecuencia del desarrollo tecnológico. Después de los atentados de París de 2015, varios Estados se abocaron a diseñar productos que les permitiera monitorear las comunicaciones de los extremistas (Kaldor, 2001).

Según Peter Sommer, estos grupos suelen identificar, y atraer a su causa, a jóvenes desarrolladores de sistemas fáciles de manipular. Cita como ejemplo SureSpot, un sistema que permite cifrar mensajes con facilidad dejando de lado el uso de sistemas que ofrecen las grandes corporaciones tecnológicas (SOMMER, 2004: 8-12). Aun así las corporaciones juegan un rol importante en este combate facilitando a los Estados "metadatos". En esta línea el Reino Unido debate a nivel parlamentario el proyecto de instrucción Powers Bill, que permitirá solicitar a los proveedores de servicios de internet guarden metadatos durante un año. Esto no prohibiría el cifrado, pero obligaría a las empresas a renunciar a las claves de descifrado para que los mensajes codificados puedan ser leídos.

Ante esta propuesta empresas como Facebook, Google, Microsoft, Twitter y Yahoo han expresado su preocupación ante el Parlamento sobre dicho proyecto, ya que consideran que significaría vulnerar la seguridad de sus productos, y trae a debate la vulnerabilidad del derecho de privacidad en internet.

---

## 2. Ciberseguridad en América Latina. Orientación actual de la política hemisférica de seguridad.

La Ciberseguridad es definida en líneas generales como la seguridad de la información digital almacenada en redes electrónicas, aunque aún hoy no hay un consenso en su definición. La noción de Ciberseguridad debe distinguirse del concepto de seguridad de la información, ya que, si bien generalmente refieren a lo mismo, este último apunta a la actividad de las organizaciones y profesionales de las tecnologías de la información, mientras que la Ciberseguridad tiene un alcance más político o vinculado a la seguridad nacional (Comnimos; 2013).

Particularmente en esta dimensión de la seguridad, la colaboración entre el sector público y privado es fundamental, es decir junto al Estado deberán trabajar las corporaciones vinculadas de alguna manera a las tecnologías de la información, las ONG's y la sociedad civil. Bajo esta línea, en junio de 2004 fue aprobada la Adopción de una Estrategia Interamericana Integral de Seguridad Cibernética: Un Enfoque Multidimensional y Multidisciplinario para la Creación de una Cultura de Seguridad Cibernética de la OEA (AG/RES. (XXXIV-O/04), 2004). En ese marco, el Secretario de Seguridad Multidimensional de la OEA, Adam Blacwell, ha afirmado que "*las autoridades deben promover la creación de una cultura de la seguridad cibernética",* y para ello es necesaria la colaboración de todas las partes interesadas a nivel nacional (ITSC, 2014).

En este sentido, es paradigmática la Cumbre Mundial sobre la Sociedad de la Información (CMSI) [3] en la que se reunieron por primera vez en igualdad de condiciones en una cumbre de la ONU, actores públicos -Estados- y privados -empresas e individuos. Entre las discrepancias que aparecieron en la fase de Ginebra en 2003 (RAMONET, 2003) está aquella que versa sobre las libertades públicas, en lo que refiere al respeto de la privacidad de los usuarios de Internet.

Como consecuencia del desarrollo en Ciberseguridad aparece un efecto poco deseado por los usuarios de Internet, y es la vigilancia sobre los ciudadanos que arremete contra el derecho a la privacidad. Al respecto Nyst (2013) señala "*mucho hacen los Estados en pos de la protección de la libertad de expresión en términos de bien común, promoviendo el acceso a Internet y las nuevas tecnologías, aunque se soslayan las consecuencias sobre el derecho a la privacidad"*.

Al tradicional fin de vigilancia del Estado avivado por distintas amenazas reales o no, acompañado por la tecnología con capacidad de vigilar un mundo "hiperconectado" (Osaba,2015: 8), se suma el poder que las grandes corporaciones vinculadas a la tecnología ostentan con el dominio de la información en Internet. Esta situación conforma un escenario particular en el que un atributo esencial de la soberanía del Estado como es el de vigilancia, se ata a la decisión de actores transnacionales que han incrementado su poder a pasos agigantados, desde que se privatizó el uso de Internet.

En el marco de la OEA, en 2004 la Asamblea General de la OEA aprobó la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética (OEA, 2016) mandatando a la Secretaría del CICTE a entender sobre asuntos de Seguridad Cibernética. El programa de seguridad cibernética de la OEA contempla las particularidades de las amenazas cibernéticas para cada Estado, así como las capacidades nacionales para enfrentarlas, promoviendo la participación directa de los gobiernos, el sector privado y la sociedad civil en la formulación de las políticas de seguridad

cibernética.

Con la aprobación de la *Estrategia Integral de Seguridad Cibernética Interamericana*, (OEA, 2017) la OEA se transformó en el primer organismo regional en adoptar una estrategia en esa materia. En pos de la construcción de nuevas y mejores capacidades de seguridad cibernética entre los Estados partes, la Secretaría del CICTE utiliza un enfoque integral, para el que existe una responsabilidad nacional y regional en la materia, con la participación de variados actores públicos y privados, que desde lo político y lo técnico trabajarán para asegurar el ciberespacio (OEA, 2017).

En este contexto, surgen en a nivel nacional los *Equipos de Respuesta a Incidentes* (CSIRT) de "alerta, vigilancia y prevención" en materia de Ciberseguridad. Se apunta a la creación de una red de alerta hemisférica que brinda formación al personal competente en la materia, de los distintos gobiernos de los Estados Miembros, buscando "*promover el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética; y fomentar el desarrollo de una cultura que permita el fortalecimiento de la Seguridad Cibernética en el Hemisferio*." (OEA, 2017).

Es fundamental la consideración de las particularidades de cada país, en el entendido de que las necesidades son diferentes, por ese motivo, la Secretaría del CICTE ha implementado un sistema de evaluaciones frente a la solicitud de asistencia técnica de un Estado Miembro que permiten identificar los requerimientos nacionales a fin de instrumentar herramientas específicas que faciliten el fortalecimiento en la materia.

De acuerdo al Informe de 2014 de la OEA y Symantec sobre Tendencias de Seguridad Cibernética en América Latina y el Caribe, y en el entendido de que tanto usuarios, operadores y reguladores de Internet requieren de acceso a una información oportuna, precisa y segura a fin de hacer frente a las amenazas y vulnerabilidades cibernéticas, se ha intentado presentar un ecosistema informático para América Latina y el Caribe. Es importante recalcar que en este sentido la OEA se ha enfocado en favorecer la cooperación entre el sector público, privado, académico y los usuarios finales, recalcando que los Estados deben promover una cultura de seguridad cibernética y actuar en pos de la protección de los usuarios individuales que en definitiva son los actores más vulnerables.

A pesar de los esfuerzos, el Informe de Ciberseguridad 2016 demuestra que la región presenta vulnerabilidades "potencialmente devastadoras".En palabras del presidente del BID Luis Alberto Moreno: "*Si los lectores han de llevarse un sólo mensaje de este Informe 2016 del Observatorio de la Ciberseguridad en América Latina y el Caribe, es que una enorme mayoría de nuestros países aún están poco preparados para contrarrestar la amenaza del ciberdelito”*. (OEA-BID, 2016:9)

## 2.1. La agenda internacional de Ciberseguridad: actores y proyecciones

En la agenda internacional para el desarrollo de la Ciberseguridad, se deben distinguir cuatro grupos de discusión que lideran la temática a nivel mundial. Se trata del Grupo de Expertos Gubernamentales de las Naciones Unidas (GEG), la Organización para la Seguridad y la Cooperación en Europa (OSCE), el Foro Regional de la Asociación de Naciones del Sureste Asiático (ASEAN), y la Organización de Estados Americanos (OEA).

También se destaca el rol de liderazgo del *Proceso de Londres*, puesto en marcha en 2011 por el entonces secretario de Relaciones Exteriores del Reino Unido, William Hague (SYMANTEC, 2014). Esta serie de reuniones internacionales tienen como objetivo generar un consenso sobre un comportamiento responsable en el ciberespacio. Hasta el momento se han realizado cuatro reuniones, la penúltima, realizada en La Haya, emitió un Informe muy completo que recomienda una serie de posibles normas y estableció el *Foro Mundial sobre Experticia Cibernética (FMEC)*.  Importante es considerar que la OEA es miembro fundador de este Foro.

El FMEC facilita el intercambio de experiencias, conocimientos y buenas prácticas entre los responsables políticos y expertos cibernéticos de diferentes países y regiones. La última reunión se realizó en Bruselas en mayo 2017.

Los Grupos de Expertos Gubernamentales de las Naciones Unidas (GEG) han sido muy importantes para la construcción de una agenda global en Ciberseguridad. Estos GEG se han reunido cuatro veces durante la última década. El tercer grupo de expertos gubernamentales en 2013, fue un éxito inesperado y definió un cambio histórico que alteró el panorama político de la Internet. Implicó el reconocimiento de que la soberanía nacional, la Carta de la ONU y el derecho internacional se aplican al ciberespacio.

La Asamblea General de la ONU aprobó esta aplicabilidad de la soberanía, el derecho y la Carta de la ONU, y esto cambió la política de la Internet y su gobernanza y de manera muy provechosa insertó el debate internacional sobre la seguridad cibernética en el marco actual de las obligaciones y el entendimiento entre los Estados.

El cuarto GEG, que concluyó en junio de 2015, contó con la participación de Colombia, México y Estados Unidos. Se pudo llegar a un consenso, pero el Informe aún no ha sido aprobado por la Asamblea General. Este Grupo de Expertos Gubernamentales aprobó un conjunto adicional de normas y medidas para desarrollar capacidad y definió una serie de medidas de generación de confianza voluntarias para aumentar la transparencia y fortalecer la cooperación. Sorprendentemente, no fueron las normas las que resultaron ser el tema más polémico, sino más bien la aplicación del derecho internacional para el ciberespacio.

En su labor, el Grupo de Expertos Gubernamentales de 2015 se guió por los precedentes creados por un acuerdo de la Organización para la Seguridad y la Cooperación en Europa (OSCE) en 2014, que verso sobre algunas medidas de fomento de confianza. Después de difíciles negociaciones, la OSCE adoptó un conjunto fundamental e inicial de medidas voluntarias para aumentar la transparencia y la cooperación. Entre las medidas voluntarias acordadas en la OSCE se incluyen la provisión de opiniones nacionales sobre la doctrina, estrategia y amenazas cibernéticas.

Los miembros de la OSCE también compartieron información sobre organizaciones, programas o estrategias nacionales pertinentes a la seguridad cibernética, identificando un punto de contacto para facilitar la comunicación y el diálogo sobre cuestiones de seguridad relacionadas con TIC y estableciendo vínculos entre los *Equipos de Respuesta ante Emergencias Informáticas* nacionales. El trabajo de los Grupos de Expertos Gubernamentales y la OSCE tiene implicaciones útiles para otras regiones del mundo, incluida América Latina y el Caribe, y para seguir avanzando en la construcción de la seguridad cibernética a nivel regional y nacional.

La OEA ostenta un rol líder a nivel mundial en el desarrollo de la cooperación internacional en materia de Ciberseguridad. Su trabajo sobre el desarrollo de capacidades es un modelo a seguir para otras regiones. La OEA ha implementado un número importante de medidas para mejorar la Ciberseguridad en todo el hemisferio. El *Comité sobre Seguridad Hemisférica* de la OEA publicó una *Lista Consolidada de Medidas de Generación de Confianza y Seguridad* que incluye intercambios voluntarios de información sobre la organización, la estructura, el tamaño de las entidades cibernéticas del gobierno, el intercambio de documentos de política y doctrina, el establecimiento de puntos de contacto nacionales en materia de protección de infraestructuras críticas e intercambio de investigación entre Estados Miembros. Esta institución también ha organizado una extensa serie de talleres y eventos de capacitación sobre estrategias nacionales, medidas de fomento de confianza y el desarrollo de experticia cibernética. Su gestión para vincular la Ciberseguridad a las iniciativas de gobernanza eficaces les ayuda a los Estados Miembros en el trabajo de implementar el gobierno electrónico de forma segura. Este objetivo se ha logrado medianamente con la colaboración del Banco Interamericano de Desarrollo.

Una de las áreas a considerar es y también de frecuente cuestionamiento, es cómo extender aún más la labor de la OEA y el BID sobre las medidas de generación de confianza de manera que cubra asuntos de Ciberseguridad. Estos esfuerzos se orientan en facilitar el desarrollo de estrategias nacionales y para potenciar la capacidad hemisférica como referente global en Ciberseguridad.

Sin embargo, en América Latina y el Caribe, como en todas las regiones, los esfuerzos para lograr la estabilidad y la seguridad del ciberespacio están en una etapa temprana. Los principales desafíos que enfrenta la región en Ciberseguridad son el desarrollo de capacidades en todos los países, la mejora de la cooperación en la detección, persecución y punición de los delitos cibernéticos y el intercambio de información sobre mejores prácticas, amenazas y vulnerabilidades. Hacer frente a estos desafíos requiere de esfuerzos diplomáticos e incentivos a la cooperación internacional.

La cooperación internacional en materia de Ciberseguridad es esencial. Esto hace que las gestiones regionales sean aún más eficaces, especialmente teniendo en cuenta los vínculos entre la Ciberseguridad, el desarrollo y el crecimiento económico. Las economías nacionales que están conectadas a la Internet global y que aprovechan el servicio de Internet crecen más rápidamente y se van enriqueciendo, al mismo tiempo que generan espacios vulnerables para los ataques delictuales en el ciberespacio.

Una mejor Ciberseguridad les permite a los países aprovechar al máximo estas oportunidades. Por esta razón, es útil considerar qué medidas adicionales se podrían realizar en el marco de la OEA sobre una base regional, no solo entre los gobiernos sino también entre las comunidades académicas y empresariales.

Según James A. Lewis (2016), director del Centro de Estudios Estratégicos e Internacionales (CSIS), en América Latina y el Caribe, las proyecciones y acciones en materia de Ciberseguridad deberían centrarse en cuatro pasos.

**En primer lugar,** la región debería continuar su labor en la creación de una base jurídica armonizada para abordar los delitos cibernéticos. Según su análisis, el mejor medio para dicha cooperación es la *Convención de Budapest* sobre el delito cibernético, pero hay obstáculos políticos para poder llegar a

un acuerdo. Algunos países se oponen a la Convención alegando motivos justificables de que no participaron en la negociación. Estas naciones no se han manifestado acerca de qué cambiarían en la Convención; sin embargo, y vale la pena señalarlo, los países con leyes de delitos cibernéticos débiles sufren mayores pérdidas económicas (LEWIS, 2016: 6). Esto lo analizaremos posteriormente, al estudiar el caso de Chile y su relación con el delito cibernético en la judicatura nacional.

**En segundo lugar,** sería útil seguir avanzando para llegar a un entendimiento común sobre las infraestructuras críticas y sus vulnerabilidades, incluyendo una definición compartida de infraestructuras cruciales [4].

**En tercer lugar,** sería beneficioso contar con un enfoque regional más formal para la generación de confianza, a partir de la *Lista Consolidada de Medidas de Fomento de Confianza y Seguridad* y basándose en el trabajo de la OSCE.

Esto implicaría el intercambio de documentos nacionales de políticas y leyes, reuniones periódicas entre funcionarios relevantes, incluidos los funcionarios a nivel político, para discutir temas de la estabilidad, comercio y seguridad y el fortalecimiento de redes de cooperación de funcionarios responsables a disposición para consulta inmediata o asistencia en caso de una emergencia.

**En cuarto lugar,** la región se beneficiaría de una formulación continua de estrategias nacionales en Ciberseguridad. Ya ha habido avances en este sentido, pero este progreso no es universal (LEWIS, 2016: 7-8).

El contar con una estrategia aporta cierto grado de organización y coherencia a los esfuerzos nacionales y ofrece transparencia y seguridad tanto para ciudadanos como para países vecinos. El desarrollo de una estrategia es, por supuesto, una prerrogativa nacional, pero hay muchas ventajas en un enfoque de colaboración internacional para el debate y desarrollo de este tipo de estrategias.

A su vez, los elementos generales de una estrategia nacional en Ciberseguridad, según Lewis (2016), se pueden resumir brevemente en las siguientes premisas:

> Los países necesitan un órgano de coordinación en las oficinas de la Presidencia o del Primer Ministro para supervisar la aplicación, coordinar las gestiones de las entidades y, a veces, resolver disputas.
>
> La estrategia seguridad nacional debe asignar responsabilidades para la Ciberseguridad entre los ministerios pertinentes y estos ministerios deben desarrollar fuertes lazos con el sector privado para crear un enfoque de colaboración, en particular con la energía eléctrica, las telecomunicaciones y las finanzas.
>
> Los gobiernos nacionales necesitan organizaciones de seguridad cibernética adecuadamente atendida que incluyan como mínimo un CERT nacional y una policía cibernéticamente capaz.
>
> Por último, debe haber un esfuerzo para generar la confianza y relaciones de cooperación con los países vecinos y que contribuya al esfuerzo global para hacer que el ciberespacio sea más seguro.

En conclusión, la creación de una capacidad estratégica en Ciberseguridad sigue siendo esencial y todas las naciones se benefician del intercambio de mejores prácticas y de información sobre amenazas y vulnerabilidades. Tener una estrategia nacional Ciberseguridad es esencial para la generación de confianza y seguridad entre las naciones de la región latinoamericana. Hasta el momento pareciere existir un buen avance hemisférico, en términos de comprender la *Seguridad* multidimensionalmente, sin embargo los gobiernos aun ignoran, o subestiman la Ciberseguridad como urgencia nacional, lo cual es muy riesgoso. A medida que todas las sociedades se vuelvan más dependientes del ciberespacio, la necesidad de adelantar acciones y desarrollar estrategias nacionales coordinadas regionalmente, crecerá.

---

# 3. Estrategias y tendencias de seguridad cibernética en América Latina

Según la Fundación Getúlio Vargas los objetivos perseguidos por las estrategias de seguridad cibernética son por lo general dos: i) proteger a la sociedad frente a las amenazas cibernéticas; y ii) fomentar la prosperidad económica y social en un contexto en el que las principales actividades se basan en el uso de Tecnologías de la Información y de la Comunicación (TIC) (Foditsch, 2016: 8).

Con el fin de alcanzar plenamente estos objetivos, las estrategias nacionales de Ciberseguridad latinoamericanas, deben – además de ser construidas a través de la cooperación internacional- ser armonizadas con los valores y derechos fundamentales desarrollados a nivel socio-cultural en cada país, tales como la privacidad, la libertad de expresión y el debido proceso, así como con los principios técnicos clave que han permitido la innovación en Internet, como la apertura, la universalidad y la interoperabilidad (DAIGLE, 2015). El respeto de los derechos humanos y de dichos principios rectores

es clave para fortalecer la confianza y fomentar el desarrollo de los países.

En los países desarrollados, las estrategias de Ciberseguridad se caracterizan por poseer un enfoque integral, que considera aspectos económicos, sociales, educativos, jurídicos, técnicos, diplomáticos, militares y relacionados con la inteligencia (OCDE, 2012: 14). Las consideraciones de soberanía en la formulación de políticas de Ciberseguridad son cada vez más relevantes y se puede notar una mayor participación de los militares, las policías, los privados y las ramas de inteligencia de los gobiernos (OCDE, 2012: 14).

Como se ha señalado anteriormente, la conciencia de la importancia de desarrollar estrategias regionales en Ciberseguridad está aumentando entre los países de América Latina. Algunos de ellos, ya tienen estrategias de Ciberseguridad implementadas en sus agendas, como Colombia, Chile (Agenda Digital 2020, 2017), Jamaica, Panamá y Trinidad y Tobago. Otros países están en proceso de discusión legislativa para su desarrollo, como Costa Rica, Dominica, Perú, Paraguay y Surinam. El nivel de madurez de estas estrategias varía, incluso en términos de proporcionar un marco para la cooperación entre los organismos gubernamentales y con actores externos.

En América Latina, el ejército y las entidades de Seguridad nacional no han sido ampliamente establecidos como los coordinadores del desarrollo de la política de Ciberseguridad de sus países, porque muchos de ellos, aún no ven la Ciberseguridad – como adelantamos antes- como un elemento de urgencia en la agenda nacional. Esto proporciona una ventana de oportunidades para el desarrollo actividades y enfoques de Ciberseguridad, desarrolladas en plataformas derivadas de múltiples actores del ciberespacio transnacional. Desde las diferentes ramas de la administración pública, el sector privado, la sociedad civil, etc. generando una descoordinación peligrosa y perjudicial en la efectividad de la estrategia de Ciberseguridad del país.

La cooperación entre múltiples interesados es notable en muchos países de América Latina. Por ejemplo, la creación de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) [5], que se han generalizado en toda la región, a nivel gubernamental como en el sector privado, financiero y empresarial.  La colaboración entre los CSIRT nacionales ha permitido el intercambio de conocimientos y buenas prácticas, lo que ha llevado a la creación de sistemas de comunicación más seguros y robustos. La mejora de las capacidades nacionales reviste de gran importancia para aumentar la confianza en los servicios digitales públicos y privados, que allanan el camino para una economía digital emergente y la gobernanza del internet.

Otras de las principales preocupaciones planteadas en los países de América Latina ha sido la definición y penalización de los delitos cibernéticos, ya sea por la creación de nuevas leyes o actualización de las ya existentes. Brasil ofrece un caso interesante. Un proyecto de ley draconiana que contiene disposiciones de delincuencia cibernética se propuso ante el Congreso [6] y tuvo una fuerte oposición por parte de los académicos y la sociedad civil. El gobierno estaba convencido de que, en lugar de una ley penal, Brasil necesitaba definir los derechos y responsabilidades de los usuarios de Internet. Esto culminó en la aprobación del Marco Civil de Internet, que trata temas como la protección de los derechos fundamentales en línea, la neutralidad de la red, la responsabilidad de los intermediarios, las responsabilidades del sector público y la retención de datos.

Otra tendencia regulatoria en la región de América Latina es una creciente preocupación por la protección de la privacidad en línea y los datos personales. Después de las revelaciones de Snowden [7], en 2013, la conciencia de la intersección entre la Ciberseguridad y los datos personales ha quedado más clara, ya que se trataba de comunicaciones electrónicas diarias. A medida que Internet se ha vuelto esencial para el desarrollo socioeconómico de América Latina, la consecuencia de no protegerla puede afectar la confianza de las actividades en línea, que tiene consecuencias potencialmente negativas para la economía de Internet y en la sociedad en su conjunto.

Nelson Remolina, en un estudio realizado en 2014, sostiene que el 70% de los países de América Latina tienen algún tipo de protección de datos en sus constituciones (REMOLINA, 2014). Por otra parte, distintos países, por ejemplo, Antigua y Barbuda, Argentina, Colombia, Costa Rica, México, Perú y Uruguay, ya han promulgado leyes de protección de datos y otros, como Brasil, están en proceso de redacción de estas. Chile – y lo analizaremos en el último capítulo – también está en proceso de legislar frente a esta materia. Su única ley data de 1993, momento histórico que difiere de lo que hoy se concibe como ciberespacio y dimensiones de seguridad.

Aunque las legislaciones nacionales regulan aún más los casos especiales, esto se debe hacer de una manera que no menoscabe estos principios básicos. El procesamiento de la información también debe ser adecuado, pertinente y no excesivo en relación con el propósito para el que fue almacenada [8]. Si no se establecen límites para la retención de datos, se seguirán reduciendo las reglas de privacidad y esto puede poner en grave peligro los derechos fundamentales de los usuarios de Internet. Por otra parte, esto podría representar una carga regulatoria costosa para las empresas, especialmente las pequeñas y medianas.

Deben utilizarse los principios como la necesidad y proporcionalidad para evaluar lo adecuado de estas disposiciones. La creación de plataformas nacionales multisectoriales sostenibles Es importante tener en cuenta los diferentes aspectos y consecuencias, así como la viabilidad técnica de la promulgación de nuevas regulaciones. Grupos de la sociedad civil, la academia y la comunidad técnica, así como representantes de la industria pueden proporcionar valiosa experiencia desde sus perspectivas, y ayudar a diseñar un marco reglamentario racional de una manera sostenible.

Estas redes de múltiples partes interesadas podrían ayudar a desarrollar un enfoque con visión de futuro para la Ciberseguridad en la región, que tiene en cuenta los avances tecnológicos, como datificación, grandes datos y la Internet de las cosas, y que tiene en cuenta el impacto de estas tecnologías en la seguridad y privacidad.

En consecuencia, se puede apreciar que la Ciberseguridad se ha ido integrando cada vez más en el plano internacional y regional [9]. En este sentido la naturaleza sin fronteras de Internet aumenta la importancia de la cooperación internacional y la armonización de los marcos legales, así como se posiciona como un elemento fundamental en la agenda nacional de seguridad, desde su perspectiva multidimensional.

---

# 4. Conclusiones

En este estudio se trataron  sistemáticamente varios temas relativos al desarrollo de la ciberseguridad en el ámbito hemisférico y nacional. Se abordaron diversos conceptos a partir de lo que se conoce como ciberdelito, ciberespacio y ciberseguridad, además de presentarse un contexto histórico que problematizó y analizó la experiencia hemisférica a propósito de la evolución del concepto de seguridad en las relaciones internacionales. En este recorrido se complejizó el análisis incorporando la problemática de la disparidad en los ordenamientos jurídicos internos de los países con relación al marco internacional y los avances en cooperación hemisférica, para la persecución y sanción de los ciberdelitos. Se evidenció al mismo tiempo, el impacto del ciberdelito como nueva amenaza de carácter transnacional, a la luz de la teoría de la transnacionalización e internacionalización de los delitos.

Lamentablemente, la realidad y el desarrollo de la ciberdelincuencia es mucho más vertiginosa que los avances que logra alcanzar la cooperación internacional para detenerla. Las actualizaciones de los modus operandi, y las disyuntivas que provocan las controversias de jurisdicción en la persecución y sanción de los ciberdelitos, son mayoritariamente los puntos más críticos de este escenario.

Por ello es necesario comprender, en primer lugar, que a diferencia de los ilícitos que se cometen en el espacio físico, en el ciberespacio existen muchas dificultades para la persecución y sanción de estos delitos. Entre otros, destacan la identificación de los autores, el tiempo que pasa entre la ejecución del ilícito y la reacción de la víctima, las bajas tasas de denuncia y la escasa posibilidad de perseguir a los infractores, pues los organismos persecutores operan en los límites territoriales del Estado mientras el ciberespacio es esencialmente un lugar sin fronteras, un lugar transnacional.

Es por ello que a modo de conclusión se enumerarán algunas premisas que surgen del estudio realizado, y en consideración a los elementos abordados y analizados latamente en los capítulos precedentes, permiten recoger ciertas consideraciones, que pueden observarse como afirmaciones y que tienen el objeto de contestar las preguntas de la investigación. En este sentido, y para el caso de la Política Hemisférica de Ciberseguridad en América latina, podemos concluir lo siguiente:

1. El estado de desarrollo de la ciberseguridad como preocupación hemisférica es de muy reciente data, y por ende su desarrollo es imperfecto. El atraso y desigualdad entre el desarrollo de los países y su acceso a la red ha provocado grandes trabas al avance de la ciberseguridad en la región. No existiendo, por ejemplo, un marco regulatorio común para los países, sin embargo, la OEA y el BID, que son los actores más relevantes en la elaboración de parámetros para una política hemisférica de ciberseguridad, han trabajado contantemente para suministrar insumos a los países, en el sentido de generar un bloque frontal contra la ciberdelincuencia, fomentando la coordinación regional. Así también, la participación del sector privado, en especial el empresarial ha desarrollado una dimensión de seguridad digital que ha podido en parte hacerse frente ante la Nueva Amenaza, mientras que los Estados están haciendo las modificaciones internas para ingresar al siglo XXI, ya que muy pocos de los países latinoamericanos cuentan con un marco regulatorio actualizado sobre el ciberespacio.
2. América latina presenta grandes problemas de coordinación entre los actores internacionales involucrados en la seguridad del ciberespacio. Los esfuerzos han sido canalizados a partir de la creación de CIRST, y las reuniones periódicas en los foros internacionales. No logrando reducir los altos índices de ciberataques, ni aumentas las bajas tasas de reacción oportuna.
3. También se destaca positivamente la cooperación entre las organizaciones internacionales como INTERPOL en el combate efectivo de la delincuencia cibernética, potenciando las capacidades para combatir la delincuencia mediante el desarrollo de marcos legislativos, pero también la formación investigadora especialista, el tratamiento de pruebas electrónicas y la formación de jueces y la fiscalía.
4. Por último, los Estados han empezado a aprovechar la capacidad de sus fuerzas armadas nacionales y/o

agencias de defensa relacionadas para defender a su país cinéticamente y proporcionar una defensa similar a través del ciberespacio, en respuesta a las amenazas de seguridad cibernética. Brasil, por ejemplo, ya ha desarrollado capacidades avanzadas de defensa cibernética y, recientemente, estableció un Comando de Defesa Cibernética y una Escuela de Defensa Cibernética Nacional, que contará con representantes de las tres fuerzas armadas brasileñas.

Finalmente, es del caso señalar que en este estudio se pretendió sistematizar la mayor cantidad de información relativa a la ciberseguridad, siguiendo ciertas coordenadas que podían complejizar la temática. En este sentido el eje problemático, se generó en base a las disparidades jurídicas y los problemas de la transnacionalización de los delitos, en tanto dificultan las estrategias nacionales, por la poca coordinación de los ordenamientos jurídicos de los países afectos a la ciberdelincuencia.

En este sentido recordar que América latina cuenta con las mayores tasas de nuevos ingresos a la red, contando hoy con mas de la mitad de la población conectada, y un 50 % de esta población ya ha vivido la experiencia del ciberdelito.

Queda mucho por hacer y discutir, no solo por parte de los países y el sector privado interesado, sino también se sugiere mantener el debate en la esfera academia para ir viendo paulatinamente los errores y falencia en la interpretaciones conceptuales frente al desarrollo de las TICs y la vertiginosa globalización.

---

# Referencias bibliográficas


ARÓSTEGUI, Julio. (2001) Ver bien la propia época (nuevas reflexiones sobre el presente como historia.  Sociohistórica, , vol: 9-10: pág.13-43.

SEGER Alexander. (2016). El estado actual de la legislación sobre el delito cibernético en América Latina y el Caribe: algunas observaciones. En: Informe Ciberdelito 2016. OEA-BID.

ARMERDING, Gisela, et al. (2006)Una mirada a la Declaración sobre Seguridad en las Américas. Centro Argentino de Estudios Internacionales. Disponible en: http://www.caei.com.ar/sites/default/files/14_3.pdf

SPRING, Ursula Oswald; BRAUCH, Hans Günter (ed.). (2009) Reconceptualizar la seguridad en el siglo XXI. Universidad Nacional autónoma de México. Recuperado de: http://bibliotecavirtual.clacso.org.ar/Mexico/crimunam/20100329020502/Reconceptualizarlaseguridad.pdf

BUZAN, Barry; WÆVER, Ole; DE WILDE, Jaap. (1998) Security: a new framework for analysis. Lynne Rienner Publishers.

MONTAÑÉS, Carmen Sánchez. (2017) Valoración de intangibles para la ciberseguridad en la nueva economía.. Tesis Doctoral. Universidad de Sevilla. Recuperado de: https://idus.us.es/xmlui/bitstream/handle/11441/63996/COPIA%20TESIS.pdf?sequence=1&isAllowed=y

CARRASCO, Óscar Navarro; PUERTA, Antonio Villalón. (2013) Una visión global de la ciberseguridad de los sistemas de control. Revista SIC: ciberseguridad, seguridad de la información y privacidad.

CASTELLS, Manuel. (2004)La era de la información: economía, sociedad y cultura. siglo XXI.

AZÓCAR, Daniel Aguirre; LAVÍN, José Morandé. (2016) El ciberespacio y las relaciones internacionales en la era digital. En: Espacios del conocimiento: Sujeto, verdad y heterotopias. A 30 años de la muerte de Fucault. LOM.

CHILLIER, Gaston; FREEMAN, Laurie. (2005) Potential threat: the new OAS concept of hemispheric security. Washington, DC: Washington Office on Latin América,.

DAIGLE, Leslie. (2015) On the Nature of the Internet. Global Commission on Internet Governance Paper series N.7. Recuperado de: https://www.cigionline.org/sites/default/files/gcig_paper_no7.pdf

DE ARMIÑO, Karlos Pérez. (2006) El concepto y el uso de la seguridad humana: análisis crítico de sus potencialidades y riesgos. Revista CIDOB d'afers internacionals.

FICARRA, Francisco. (2002) Los virus informaticos. Revista Latinoamericana de Comunicación CHASQUI, no 78.

FLEMES, Daniel. (2004) Creación de instituciones en el sector de defensa y seguridad del MERCOSUR (I). La cooperación de defensa de Brasil: entre los servicios armados dominantes y marcado bilateralismo. Instituto de Estudios Iberoamericanos (IIK), Hamburgo (Alemania), Working Paper IIK, no 20. Disponible en: https://www.files.ethz.ch/isn/46976/arbeitspapiere22e.pdf

FLORES PACHECO, Ana Luz; GALICIA SEGURA, Graciela; SÁNCHEZ VANDERKAST, Egbert. (2007)Una aproximación a la Sociedad de la Información y del Conocimiento. Revista Mexicana de Orientación Educativa, vol. 5, no 11.

FLOREZ, María Eugenia Rodríguez. (2013) América Latina,¿ debe crear un sistema de normas

armonizadas para el cibercrimen?. Recuperado de: http://www.econ.uchile.cl/uploads/publicacion/9ba7739a0ac26598402dab53c990c58e49fc259a.pdf

IBARRA, Virginia; NIEVES, Mónica. (2016) La seguridad internacional determinada por un mundo on-line: el Estado ante el desafío del terrorismo y la ciberseguridad. En VIII Congreso de Relaciones Internacionales (La Plata, 2016).

LEWIS, James A. (2016) Fomento de confianza cibernética y diplomacia en América Latina y el Caribe. OEA-BID.

KALDOR, Mary; TAPIA, María Luisa Rodríguez. (2001) .Las nuevas guerras: violencia organizada en la era global. Tusquets.

KEOHANE, Robert O; NYE JR, Joseph S. (1998) Poder e interdependencia en la era de la información. Asuntos exteriores

LEAL, Francisco. (2003) La doctrina de Seguridad Nacional: materialización de la Guerra Fría en América del Sur. Revista de estudios sociales, no 15.

MACIEL, Marília, FODITSCH Nathalia, Luca Belli y Nicolás Castellón. (2016) Fundación Getúlio Vargas. Informe Ciberseguridad 2016. OEA-BID.

MARKOVICTH, Claudio Paul Magliona; MEDEL, Macarena López. (1999) Delincuencia y fraude informático: derecho comparado y ley n° 19.223. Editorial Jurídica de Chile.

MENDOZA BREAMUTZ, E. (2005) Globalización, Internacionalización del Delito y Seguridad. Estudios en Homenaje a D. Jorge Fernández Ruiz.

MORENO, Luis. (2016) BID/OEA. Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad. Observatorio de la Ciberseguridad en América Latina y el Caribe. 2016. Recuperado de: https://publications.iadb.org/handle/11319/7449.

NYST, C. (2013) El derecho a la privacidad y a la libertad de expresión: dos caras de la misma moneda. Cuestión de Derechos. *Revista Electrónica*. No 4 –. Recuperado de: https://www.apc.org/es/system/files/ADC%20-%20Cuestion%20de%20derechos%20-%20Revista-numero4%20-%202013.pdf

OECD. (2012) Cyber security policy making at a turning point: Analyzing a new generation of national cybersecurity strategies for the Internet economy. OCDE.

OROZCO, Gabriel.(2005) El concepto de la seguridad en la Teoría de las Relaciones Internacionales. *Revista CIDOB d'afers internacionals*

---

1. Académico del Departamento de Historia. Universidad de Playa Ancha, Valparaíso, Chile.  Magister en Relaciones Internacionales (PUCV) Doctorando en Historia (USACH) Correo: hugo.castro@upla.cl

2. Director Departamento de Historia. Universidad de Playa Ancha. Magister en Historia de Chile y América. (UV) Doctor© en historia (UNCuyo). Correo: amontev@upla.cl

3. Realizada en dos fases: la primera en Ginebra en diciembre de 2003, y la segunda en Túnez en noviembre de 2005.

4. Infraestructuras críticas se definen como: "*Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas*". Esta definición fue establecida por la Directiva europea: 2008/114/CE del 8 de diciembre de 2008, subrayando sobre la importancia de "*la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección"*. Disponible en: https://manuelsanchez.com/2011/07/06/infraestructuras-criticas-y-Ciberseguridad/

5. Un Equipo de Respuesta frente a Incidencias de Seguridad Informática (CSIRT) es un grupo de profesionales que recibe los informes sobre incidentes de Ciberseguridad, analiza las situaciones y responde a las amenazas.

6. Proyecto de Ley 84/99 que fue aprobado el 7 de noviembre de 2012, fue impulsado por el diputado Eduardo Azeredo, lo que género que la ley obtuviera la denominación de Ley Azeredo.

7. Los datos acerca de la vigilancia mundial son una serie de revelaciones sacadas a la luz por la prensa internacional entre 2013 y 2015, que demuestran la vigilancia que principalmente las agencias de inteligencia de Estados Unidos, en colaboración con otros países aliados, han estado ejerciendo de manera masiva sobre la población mundial. Los documentos que reveló Snowden se publicaron simultáneamente en The Washington Post y en The Guardian.

8. Consejo de Europa. Convenio para la protección de las personas en relación con tratamiento automático de datos personales. ETS 108, en el artículo 5.

9. La seguridad cibernética es una de las prioridades identificadas en el proceso decenal de examen de los resultados de la Cumbre Mundial sobre la Sociedad de la Información (CMSI). La Visión CMSI + 10 hizo énfasis en la complementariedad entre la seguridad y la privacidad y definió que "la construcción de la confianza y seguridad en la utilización de las TIC, especialmente en temas como la protección de datos personales, la privacidad, la seguridad y la solidez de las redes", debe ser una de las prioridades más allá de 2015. En diciembre de 2013, la Asamblea General de las Naciones Unidas aprobó la resolución 68/167, que expresa su profunda preocupación por el impacto negativo que la vigilancia e interceptación de las comunicaciones pueden tener en los derechos humanos. La Resolución 69/166, aprobada en 2014, se basa en la anterior, pidiendo el acceso a un recurso efectivo para las personas cuyo derecho a la privacidad ha sido violado. El 26 de marzo de 2015, el Consejo de Derechos Humanos creó el mandato de un Relator Especial sobre el Derecho a la Privacidad. Sin embargo, la cooperación intergubernamental en materia de Ciberseguridad sigue fragmentada a través de diferentes organismos y foros en las Naciones Unidas. En paralelo, una Conferencia Mundial sobre el Espacio Cibernético (GCCS) anual, conocida como el "Proceso de Londres" ha reunido a los gobiernos y otras partes interesadas para discutir temas en una amplia gama de asuntos relacionados con la seguridad cibernética.

Revista ESPACIOS. ISSN 0798 1015
Vol. 39 (Nº 39) Año 2018

[Índice]