Cuestiones Jurídicas
Revista de Ciencias Jurídicas
de la Universidad Rafael Urdaneta
Vol. X, N° 1 Enero - Junio 2016
ISSN 2343 - 6352

Ciberseguridad realidad y tendencias en Venezuela[1][2]

Gladys Stella Rodríguez[3]

Resumen

La ciberseguridad implica problemas complejos y su resolución exige una voluntad política de diseño e implementación de un plan de desarrollo de infraestructuras y servicios digitales que comprenda una estrategia multidisciplinaria, coherente, eficaz y controlable de la ciberseguridad El objetivo es describir a la ciberseguridad en Venezuela y las tendencias en la materia, a través de una investigación exploratoria-descriptiva con base a la consulta documental. Venezuela, de acuerdo a los ítems del Índice de evaluación sobre ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT), presenta mejor posicionamiento en el aspecto técnico, capacitación y de cooperación, quedando por desarrollar más el aspecto legal y organizativo.

Palabras Claves: Ciberseguridad, Servicios Digitales, Venezuela, Realidad, Tendencias

[1]Recibido: 16/10/2015 Aceptado: 15/04/2016

[2]Este artículo es un avance del Proyecto de investigación intitulado "Regulación de la ciberseguridad de la información en el Estado venezolano: Avances y Desafíos en las redes sociales virtuales. Financiado por el Consejo de Desarrollo Científico y Humanístico (CONDES) No. CH-0541-14.

[3]Abogada, Magister en Planificación y Gerencia de Ciencias y Tecnología, Doctora en Derecho, Postdoctora en Gerencia en las Organizaciones. Docente e Investigadora de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia. Coordinadora del Programa de Estudios sobre Derechos Humanos, Nivel Postdoctorado. Universidad del Zulia. Maracaibo, Venezuela. Contacto de correspondencia: gr1970ve@gmail.com

Cyber security reality and trends in Venezuela

Abstract

Cybersecurity involves complex issues and their resolution requires a political will to Cybersecurity implies complex problems and their resolution requires the political will to design and implement a plan for the development of infrastructure and digital services that include a multidisciplinary, coherent, effective and manageable cybersecurity strategy. The objective is to describe cybersecurity in Venezuela and trends in the field, through an exploratory-descriptive research based on documentary consultation. Venezuela, according to the Cybersecurity Assessment Index of the International Telecommunication Union (ITU), has better positioning in the technical, training and cooperation aspects, lagging to further develop the legal and organizational aspect.

Key Words: Cybersecurity, Digital Services, Venezuela, Reality, Trends

Introducción

En la actualidad se ha venido conformando una aldea global interconectada donde confluyen ciberciudadanos con la información que se traslada en tiempo real desde lugares remotos. Ello ha significado el surgimiento de algunos términos como ciberespacio y ciberseguridad, que ya gozan de un uso generalizado por amplios sectores de la sociedad.

Vale indicar que, antes de abordar un análisis del estatus de la ciberseguridad en Venezuela y, de describir su realidad y las tendencias en la materia, es imprescindible presentar qué es y cómo el ciberespacio interactúa y afecta a todos los individuos. Es importante ser conscientes de sus implicaciones: *Sociale*s, es decir, la sociedad actual se caracteriza porque sus individuos están conectados entre sí y se puede conocer de primera mano los acontecimientos que se producen sin importar dimensiones como lugar y tiempo a través de los distintos instrumentos de comunicación (correo, mensajería, redes sociales, telefonía, video y audio), pero también es relevante desde el punto de vista de la sociedad, el fenómeno de la exclusión a servicios o bienes por el solo hecho de no poseer una conexión a la red de redes; *Económicas,* en este sentido, no cabe

duda que la compra y venta, la banca y el mercado global son influenciados por estas herramientas tecnológicas, se pueden hacer operaciones en línea sin tener que trasladarse al sitio físico, pero de igual forma, hay grandes fraudes electrónicos y violaciones a los datos que se suministran en estas dependencias bancarias; Jurídicas, la ciudadanía exige marcos regulatorios de seguridad y defensa frente al desarrollo tecnológico, de esta manera, ha surgido a nivel mundial algunos instrumentos legales y organismos de tutela y de empoderamiento tecnológico, sin embargo, hay mucha tarea por realizar sobre todo frente a la impunidad o elevada burocracia; *Políticas*, la administración pública ha venido incorporando sitios web a fin de brindar consulta, transparencia, atención y participación al administrado, no obstante, los procedimientos siguen siendo en su mayoría no inmediatos, costosos y, poco transparentes; finalmente, *Culturales*, es posible participar en eventos de otras latitudes sólo con un clic, entrar a museos del mundo, apreciar la riqueza artística y literaria de cualquier nación desde la comodidad que ofrece un computador, móvil o cualquier dispositivo de conexión a la red, pero la conexión a internet es lenta y mucho más cuando involucra archivos de multimedia.

Otro tema sumamente de interés es lo atinente a privacidad y la intimidad. Derechos que en los últimos años, son objeto de frecuente vulnerabilidad producto del desarrollo tecnológico. En años recientes algunos órganos judiciales como es el caso del Tribunal Europeo de Justicia, dictó una sentencia de fecha 13 de mayo del año 2014[4], por la cual los residentes europeos tienen derecho a pedir a los motores de búsqueda en Internet que eliminen los resultados en los que aparezca su nombre en el caso de que estuvieran desfasados, fueran irrelevantes o tuvieran contenido incendiario; el denominado "derecho al olvido". Y por otra parte, se contrapone a estos derechos fundamentales consagrados en Tratados sobre Derechos Humanos y en la mayoría de las Constituciones del mundo, la potestad de conocer por parte de los entes de gobierno, la información contenida en un móvil, archivo o cualquier dispositivo en

[4]Tribunal de Justicia de Unión Europea, Gran Sala , Sentencia ECLI:EU:C:2014:317 Asunto C-131/12 Google contra la Agencia Española de Protección de Datos (AEPD) de fecha 13 de mayo de 2014 La cuestión prejudicial planteada tenía como objetivo esclarecer (i) el ámbito de aplicación territorial de la Directiva 95/46/CE relativa a la protección de las personas físicas, (ii) la determinación del alcance de la responsabilidad de los buscadores de internet como proveedores de contenidos en relación con la Directiva 95/46/CE y (iii) el alcance del derecho de cancelación y oposición en relación con el derecho al olvido.

defensa de ciberataques o ciberdelitos. No obstante, vale aclarar que el tema de la privacidad y su rivalidad con la ciberseguridad no será objeto de tratamiento por este trabajo.

En consecuencia, los objetivos a abordar responden a exponer cuáles son las posibles amenazas a la ciberseguridad, se plantea la propuesta de la Unión Internacional de Telecomunicaciones (UIT en adelante) en materia de ciberseguridad y, particularmente el resultado del Índice Mundial de Ciberseguridad, destacando la situación de Venezuela. La presente investigación es de tipo explorativa-descriptiva-explicativa toda vez que indaga la situación real del Estado venezolano, analiza los indicadores del índice Mundial de Ciberseguridad y explica sus consecuencias para el Estado venezolano, arrojando como conclusiones un panorama sobre las tendencias que sobre la materia se encuentran presentes en Venezuela.

1.- Algunos conceptos básicos

Ciberespacio es un término que se emplea dentro de la comunidad de las Tecnologías de Información y Comunicación (TICs en adelante) y se refiere al conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos (Fojón y Sanz, 2010: 9). Para alcanzar una definición de ciberespacio que permita comprender las implicaciones referidas *ut supra*, será útil recurrir al concepto de servicio, entendido como la prestación que recibe un usuario o consumidor por parte de un proveedor. Por su parte gobiernos como el español a través de un Documento emitido por la Presidencia[5] coinciden también en señalar que el ciberespacio, es el nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información – incluida Internet–, las redes y los sistemas de información y de telecomunicaciones, que han venido a difuminar fronteras, haciendo partícipes a sus usuarios de una globalización sin

[5]Presidencia del Gobierno de España. Estrategia de Ciberseguridad Nacional jueves 5 de diciembre de 2013. La Estrategia de Ciberseguridad Nacionales el documento estratégico que sirve de fundamento al Gobierno de España para desarrollar las previsiones de la Estrategia de Seguridad Nacional en materia de protección del ciberespacio con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas.

precedentes que propicia nuevas oportunidades, a la vez que comporta nuevos retos, riesgos y amenazas (Presidencia del Gobierno de España, 2013).

Las definiciones apuntadas permiten comprender de inmediato que el ciberespacio es ya parte esencial de las sociedades, economías e, incluso, puede llegar a ser factor determinante de la evolución de las culturas, o quizás de su convergencia. De ahí la importancia de proteger el ciberespacio. Anteriormente, la ciberseguridad obedecía a un enfoque de protección de la información *Information Security* donde solamente se trataba de proteger la información a accesos, usos, revelaciones, interrupciones, modificaciones o destrucciones no permitidas.

En la actualidad, este enfoque está evolucionando hacia la gestión de riesgos del ciberespacio *Information Assurance* donde la ciberseguridad consiste en la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados basándose en los estándares internacionalmente aceptados (Fojón y Sanz, 2010).

Una de las razones para este nuevo enfoque es la caracterización del ciberespacio de una determinada entidad como un sistema de TICs que proporcione servicios, de manera que la seguridad del sistema se consigue cuando éste se encuentra en un estado de riesgo conocido y controlado. Realmente, ambos enfoques, *information security e information assurance,* son diferentes pero complementarios, y con mucha frecuencia son utilizados indistintamente de manera errónea.

2.- Riesgos y amenazas a la ciberseguridad en el ciberespacio.

Existen riesgos en el ciberespacio, como el temor a las catastróficas consecuencias de un hipotético "ciber-Katrina" o a un "ciber-11de Septiembre" que ha provocado que países no sólo como EEUU, Francia, el Reino Unido, España, Israel y Corea del Sur, sino también los países de América Latina a través de la misma Organización de Estados Americanos (OEA) al igual que la Organización de las Naciones Unidas (ONU) y la Organización del Tratado del Atlántico del Norte (OTAN), estén tomado conciencia de la importancia y necesidad de un ciberespacio seguro, y están desarrollando marcos normativos, planes y estrategias específicos para la defensa del ciberespacio, como el caso citado

de España y, en el caso de América Latina también hay un informe de la OEA[6], que toma como base una encuesta a 575 organismos públicos y privados de América latina, relacionados con las comunicaciones, la banca, la manufactura y los sectores de energía y seguridad, y en el que el 60%de los participantes aceptó haber sufrido intentos de robos de datos, principalmente a través del llamado *phising*[7].El estudio también revela que se están popularizando otras variedades más inquietantes, el 40% de la población encuestada afirman que se han encontrado intentos de inutilizar las computadoras, 44% ha visto intentos de borrado de archivos y el 54 % ataques para manipular sus sistemas.

Las amenazas sobre el ciberespacio se concretan en ciberataques que pueden ser clasificados, según varios criterios, por ejemplo: los objetivos del ataque (gobierno, sector privado y ciudadanos), las amenazas relacionadas con el ciberespacio (contra la información y contra la infraestructura de las TICs) y, los autores de los ciberataques. Se ha escogido este último criterio por ser el que identifica quienes realizan estos actos y ser más amplia la categorización. Para ello, se sigue a (Fojón, *et al*, 2012: 17-19) y las principales categorías de este criterio de autoría son:

> **1. Ataques patrocinados por Estados.** Los conflictos del mundo físico o real tienen su continuación en el mundo virtual del ciberespacio. En los últimos años se han detectado ciber-ataques contra las infraestructuras críticas de países o contra objetivos muy concretos, pero igualmente estratégicos. Algunos ejemplos, son el ataque a parte del ciberespacio de Estonia en 2007, que supuso la inutilización temporal de muchas de las infraestructuras críticas del país báltico o los ciber-ataques sufridos por las redes clasificadas del gobierno estadounidense a manos de atacantes con base en territorio chino….

[6]Trend Micro Incorporated, la Organización de los Estados Americanos (OEA) y su Secretaría de Seguridad Multidimensional (SMS). 2013. Informe para ilustrar las tendencias en seguridad y delincuencia cibernética en América Latina y el Caribe. La información que aquí se presenta se recabó a través métodos tanto cuantitativos como cualitativos, a partir de datos extraídos de una encuesta entre los gobiernos de los Estados miembros de la OEA, así como de un análisis minucioso de inteligencia de las amenazas mundiales de honeypots y datos aportados por clientes y recogidos por Trend Micro. Disponible en: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-tendencias-en-la-seguridad-cibernetica-en-america-latina-y-el-caribe-y-respuestas-de-los-gobiernos.pdf, consultado 24 de abril de 2015.

[7]Es un engaño para que la víctima permita el acceso de software maligno a su equipo, que suele ser reconocido por falsos emails de bancos.

> **2. Terrorismo, extremismo político e ideológico.** Los terroristas y grupos extremistas utilizan el ciberespacio para planificar sus acciones, publicitarlas y reclutar adeptos para ejecutarlas. Estos grupos ya han reconocido la importancia estratégica y táctica del ciberespacio para sus intereses….
>
> **3. Ataques del crimen organizado.** Las bandas del crimen organizado (ciber-gangs) han comenzado a trasladar sus acciones al ciberespacio, explotando las posibilidades de anonimato que éste ofrece. Este tipo de bandas tienen como objetivo la obtención de información sensible para su posterior uso fraudulento y conseguir grandes beneficios económicos[8].
>
> **4. Ataques de perfil bajo.** Este tipo de ataques son ejecutados, normalmente, por personas con conocimientos en TIC que les permiten llevar a cabo ciber-ataques de naturaleza muy heterogénea y por motivación, fundamentalmente, personal.

Una reflexión rápida de los tipos de amenazas e impactos sobre los activos del ciberespacio y de los servicios que dependen de él evidencia que las TICs, al mismo tiempo que permiten disfrutar de más y mejores servicios en muchos ámbitos de la sociedad, también aumentan el riesgo de sufrir ataques sobre tales servicios, con el agravante de que la extensión y popularización de las TICs difuminan las líneas de defensa del bien a proteger. Con la misma facilidad que un ciudadano accede al ciberespacio para gestionar desde su hogar sus cuentas bancarias, otro individuo puede acceder a información "en red" sobre cómo romper la seguridad de ese servicio y sustraer las claves privadas de aquél y suplantar su identidad.

Estos ciberataques han impulsado desde el año 2011, una estrategia por parte de la UIT[9], la cual consiste en lograr la mayor colaboración entre los gobiernos y las empresas del sector privado para asegurarse de que la policía y el poder judicial dispongan de las herramientas apropiadas

[8]Según datos del FBI en 2009, el impacto del cibercrimen por la acción de bandas organizadas ocasionó pérdidas, tanto a empresas como a particulares estadounidenses, por un valor superior a 560 millones de dólares

[9]La UIT, con sede en Ginebra (Suiza), es la principal organización internacional del sistema de las Naciones Unidas en la cual los gobiernos y el sector privado coordinan los servicios y redes mundiales de telecomunicaciones. Internamente, la UIT está organizada por "sectores", que son áreas administrativas coordinadas desde una oficina, la cual no tiene posición de jerarquía respecto de los diferentes comités, grupos y demás que conforman el sector, sino que únicamente colabora con ellos para la operación armónica en interés de la comunidad internacional y de la UIT

para proteger al público contra las actividades delictivas, pero siempre protegiendo los derechos humanos fundamentales y la vida privada de las personas.

3.- Índice Mundial de Ciberseguridad de la UIT

Partiendo del compromiso antes referido por la UIT y en el marco del Foro[10], se presentó el Índice Mundial de Ciberseguridad (GCI en sus siglas en inglés, y IMC en español usado en adelante), iniciativa formulada por la UIT y ABI *Research*[11] para evaluar los niveles de ciberseguridad en los diferentes países.

Esta iniciativa, responde al compromiso de la UIT de reforzar la ciberseguridad y reducir las disparidades en todo el mundo, fomentando al mismo tiempo las capacidades a escala nacional, especialmente en los países en desarrollo.

El objetivo a largo plazo es impulsar nuevas iniciativas encaminadas a la adopción e integración de la ciberseguridad a escala mundial. Una comparación de las estrategias nacionales en materia de ciberseguridad revelará cuáles son los países que han logrado las clasificaciones más altas en ámbitos específicos[12] y, por consiguiente, se pondrán de relieve las estrategias de ciberseguridad menos conocidas pero que han obtenido buenos resultados.

Por su parte, el objetivo a corto plazo del Índice Mundial de Ciberseguridad (IMC en adelante) es contribuir a fomentar una cultura mundial de la ciberseguridad y su integración como elemento central de

[10]Foro Measuring Countries' Readiness and Build Capacityon Cybersecurity (Medición de la preparación y creación de capacidades de los países en materia de ciberseguridad) celebrado en la Conferencia de la UIT, que se inauguró en Dubai (Emiratos Árabes) del 30 de marzo hasta el 10 de abril de 2015.

[11]Es una compañía asesora de tecnología de inteligencia de mercado, con un historial probado por 25 años que se centra en poner la información en manos de los ejecutivos con el fin de que puedan tomar las decisiones correctas en materia de tecnología y la inversión de mercado en el momento adecuado. ABI Research cuantifica los mercados importantes de la actualidad, define las tecnologías estratégicas del mañana, y da una idea de cómo se adoptó la tecnología en mercados verticales.

[12]En este Ranking aparecen los diez primeros países, pero Venezuela no aparece entre los destacados

las TICs. "Los países deben ser conscientes de su grado de capacidad actual en materia de ciberseguridad y, al mismo tiempo, identificar las esferas en que debe incrementarse", indicó Sanou[13].

Una primera etapa para poner remedio a la situación consiste en comparar las capacidades de los países en materia de ciberseguridad y publicar la clasificación correspondiente.

El Grupo de Expertos de Alto Nivel sobre Ciberseguridad (GEANC en adelante) de la UIT es el principal facilitador en lo que respecta a la Línea de Acción C5[14] de la CMSI (Cumbre Mundial sobre la Sociedad de la Información), en la cual se alienta a las partes interesadas a crear confianza y seguridad en cuanto a la utilización de las TICs a escala nacional, regional e internacional. Esta Línea de Acción se centra en la Agenda sobre Ciberseguridad Global de la UIT, que se lanzó en mayo de 2007 y comprende cinco pilares estratégicos: medidas legales, medidas técnicas y de procedimiento, estructuras institucionales, creación de capacidades y cooperación internacional, que se explicará más adelante.

Los Miembros de la UIT, reunidos en la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT[15]- Año 2012) en Dubai, han revisado y adoptado una Resolución acordada por primera vez en la AMNT de 2008 en Johannesburgo, la Resolución 69, referida al **Acceso y utilización no discriminatorios de los recursos de Internet**, la misma propone "creación de equipos nacionales de intervención en caso de incidente informático, especialmente para los países en desarro-

[13]BrahimaSanou Director de la Oficina de Desarrollo de las Telecomunicaciones de la UIT

[14]Esta línea se refiere a la "Creación de confianza y seguridad en la utilización de las TIC", determinada por la Cumbre Mundial sobre la Sociedad de la Información. Varios participantes presentaron iniciativas al respecto, y se trató de identificar metas y posibilidades de medir los resultados. En total 125 participantes de los sectores público y privado, organizaciones internacionales, el sector docente y la sociedad civil asistieron a la reunión en Ginebra los días 22 y 23 de mayo de 2008.

[15]La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT), que a su vez producen Recomendaciones sobre dichos temas. El UIT-T, es un órgano permanente de la UIT, que estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial. (Unión Internacional de Telecomunicaciones. Sector de Normalización de las Telecomunicaciones de la UIT. Asamblea Mundial de Normalización de las Telecomunicaciones. Dubai, 20-29 de 2012. Resolución 69 Acceso y utilización no discriminatorios de los recursos de Internet)

llo, y cooperación entre los mismos" adoptada por la quinta Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT- Año 2010), y en la Resolución 130 (Guadalajara, 2010) sobre el "Fortalecimiento del papel de la UIT en la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación". A ese respecto, el Secretario General de la UIT lanzó la Agenda sobre Ciberseguridad Global (GCA en sus siglas en inglés), el mecanismo se focaliza en los cinco ámbitos de trabajo siguientes[16]:

a. Medidas Legales, lo que significa evaluar legislación criminal; regulación y cumplimiento.

b. Medidas Técnicas, involucra apreciar si posee un sistema de respuesta a incidentes a nivel nacional; si existe un estándar de seguridad verificado por una agencia especializada; y si existe un sistema de certificación de agencias públicas que cumplan con estándares internacionales

c. Medidas Organizativas, en este elemento se aprecian campañas de concienciación, certificación de profesionales especializados.

d. Creación de Capacidades, está referida al cumplimiento de la exigencia de crear capacidades en recursos financieros, técnicos y humanos específicos, consiste por parte de la UIT en organizar foros regionales sobre ciberseguridad para proporcionar información y facilitar el intercambio de prácticas idóneas y estudios de casos prácticos. La UIT debe trabajar sobre planteamientos integrados de ciberseguridad nacional para coordinar los esfuerzos nacionales

e. Finalmente, Cooperación con otros países, en organizaciones internacionales, y entre el sector público y privado del propio país.

De la evaluación realizada por la UIT, donde se indica las posiciones alcanzadas por los primeros países en el *ranking*, Venezuela no aparece. Por ello, resulta oportuno señalar los aspectos legales, técnicos, organizacionales, de capacitación y de cooperación con los que cuentan el país en materia de ciberseguridad y que posiblemente podrían definir la razón por la que no aparece en el *ranking de destacados*.

[16]Ver Documento ABI Research y UIT. Global Cybersecurity Index. Y:\APP\PDF_SERVER\ALL-USER\IN\BDT\KUSHTUEV\S_GCI_CONCEPTUAL FRAMEWORK.DOCX (361935) 15-05-2014

4. Ciberseguridad en Venezuela: Revisión de los Aspectos Legales-Técnicos-Organizacionales-Capacitación-Cooperación

4.1. Aspectos Legales

Las TICs desde sus inicios en el siglo XIX, han generado cambios que han sido notorios en el ámbito social, económico, político y cultural de la sociedad. Estos cambios se presentaron de manera aislada, desordenada, sin un marco legal, que regulara sus escenarios y acciones.

No fue sino hasta la década de los setenta cuando se difundió las bondades de la tecnología de punta basadas en la microeléctrica, las computadoras con la creación del primer software y las telecomunicaciones para dar respuesta a este cambio paradigmático, la Constitución Nacional de 1999 y la creación del Ministerio de Ciencia y Tecnología el mismo año, expone claramente, por primera vez en el país, la intención política del Estado venezolano de valorar y utilizar la ciencia y la tecnología e innovación como pilar fundamental para el desarrollo. Sin olvidar que conjuntamente con la Ley Orgánica de Telecomunicaciones publicada el 12 de junio de 2000, en la Gaceta Oficial de la República Bolivariana de Venezuela No. 36.970, se crea un marco legal moderno y favorable para la protección de los usuarios y operadores de servicios de telecomunicaciones en un régimen de libre competencia, así como para el desarrollo de un sector prometedor de la economía venezolana. Esta promulgación constituye el logro de una aspiración largamente anhelada por el país. En efecto, la nueva regulación está llamada a sustituir una legislación anacrónica constituida fundamentalmente por la Ley de Telecomunicaciones de 1940 y otras disposiciones legales dictadas con posterioridad a dicha

fecha, con las que se pretendió resolver asuntos puntuales, resultando un instrumento inadecuado a las realidades que el nuevo desarrollo tecnológico había planteado a lo largo de las últimas dos décadas.

Por su parte, recientemente la Asamblea Nacional ha aprobado el Plan de la Patria[17]. Este documento fue presentado ante el órgano representativo, legislativo y de control por el Presidente de la República, Nicolás Maduro, invocando el artículo 237, numeral 18, de la Constitución de la República Bolivariana de Venezuela, el cual lo faculta para "formular el Plan Nacional de Desarrollo y dirigir su ejecución previa aprobación de la Asamblea Nacional"[18].

Este Plan presenta varios ejes centrales, a los fines de la investigación interesa el **IV Eje**, este eje hace referencia al desarrollo de una nueva geopolítica internacional en la cual se conforme el mundo multicentrico y pluripolar, que permita lograr el equilibrio del universo y garantizar la paz planetaria. En concordancia con los Objetivos Nacionales del referido Plan son de interés: los ***Objetivos 4.3 y 4.4.*** En el caso del primer objetivo se pretende continuar impulsando el desarrollo de un mundo multicéntrico y pluripolar sin dominación imperial y con respeto a la autodeterminación de los pueblos. Y el ***Objetivo 4.4.*** busca desmontar el sistema neocolonial de dominación imperial. A este último Objetivo Nacional se le ha asignado unos Objetivos Estratégicos y Objetivos Generales a saber: **4.4.2.4, Llevar a niveles no vitales** la conexión de Venezuela a las redes de comunicación e información dominadas por las potencias neocoloniales. ***4.4.2.5 Eliminar la dependencia de sectores estratégicos para el desarrollo nacional de redes de comunicación e***

[17]Proyecto Nacional Simón Bolívar, Segundo Plan Socialista de Desarrollo Económico y Social de la Nación, 2013-2019. Debe señalarse que el documento pretende trazar un marco valorativo y principista alternativo al de la Constitución, la cual resulta en buena medida ignorada o adulterada. Por otro lado, el llamado Plan de la Patria, que según su propia formulación se presentó ante la Asamblea Nacional para ser sancionado mediante "ley aprobatoria", fue finalmente aprobado por medio de un acuerdo, tiene la ambición de ser "de obligatorio cumplimiento en todo el territorio de la República Bolivariana de Venezuela"

[18]La Asamblea Nacional tiene a su vez la atribución de "aprobar las líneas generales del plan de desarrollo económico y social de la Nación, que serán presentadas por el Ejecutivo Nacional en el transcurso del tercer trimestre del primer año de cada período constitucional" (art. 187, num. 8, de la Constitución)

información controladas por las potencias neocoloniales. Y 4.4.2.6 Llevar a niveles no vitales la participación tecnológica de las potencias imperiales en proyectos de desarrollo nacional

Se desprende de lo planteado que hay una norma en materia de telecomunicaciones que sirve de marco legal así como políticas de Estado, en la materia, sentando así las bases de una acción de gobierno que podría desarrollarse ampliamente en la actualidad, partiendo de una capacitación y cooperación entre Estado-Sociedad Civil – Sector Privado. No es el propósito de la evaluación por parte de la UIT, considerar si estas normas y políticas abordan las necesidades del sector, sólo se limita a verificar que existan normas y políticas en la materia. Por ello, no se hace este tipo de consideración en esta investigación, resultaría infructuoso determinar si la norma es efectiva o si la política ha resultado eficaz.

De esta manera se destacan dentro del marco legal, las siguientes normas.

De acuerdo a lo previsto en el artículo 326 de la Constitución Nacional de 1999, la Seguridad de la Nación se fundamenta en la corresponsabilidad entre el Estado y la sociedad civil, para dar cumplimiento a los principios de independencia, democracia, igualdad, paz, libertad, justicia, solidaridad, promoción y conservación ambiental y afirmación de los derechos humanos, así como en la satisfacción progresiva de las necesidades individuales y colectivas de los venezolanos y venezolanas, sobre las bases de un desarrollo sustentable y productivo de plena cobertura para la comunidad nacional. El principio de corresponsabilidad se ejerce sobre los ámbitos económico, social, político, cultural, geográfico, ambiental y militar.

Concatenado con esta disposición constitucional, el artículo 2 de la Ley Orgánica de Seguridad de la Nación de fecha 18 de diciembre de 2002, en su artículo 2 establece que la seguridad nacional debe estar fundamentada en el desarrollo integral, y es el estado quien garantiza el goce y ejercicio de los derechos y garantías en los ámbitos económico, social, político, cultural, geográfico, ambiental y militar de los principios y valores constitucionales por parte de la población, las instituciones y cada una de las personas que conforman el Estado y la sociedad, con

proyección generacional, dentro de un sistema democrático, participativo y protagónico, libre de amenazas a su sobrevivencia, su soberanía y a la integridad de su territorio y demás espacios geográficos.

Por su parte la ley antes referida también señala en su artículo 3, que la defensa integral de la Nación comprende el conjunto de sistemas, métodos, medidas y acciones de defensa, cualesquiera sean su naturaleza e intensidad, que en forma activa formule, coordine y ejecute el Estado con la participación de las instituciones públicas y privadas, y las personas naturales y jurídicas, nacionales o extranjeras, con el objeto de salvaguardar la independencia, la libertad, la democracia , la soberanía, la integridad territorial y el desarrollo integral de la nación.

En esta misma orientación se promulga en fecha 30 de abril de 2012, una nueva Ley Orgánica contra la delincuencia organizada y financiamiento al terrorismo (LOCDOFT), que derogó a la Ley Orgánica contra la Delincuencia Organizada de fecha 26 de octubre de 2005. La LOCDOFT tiene por objeto prevenir, investigar, perseguir, tipificar y sancionar los delitos relacionados con la delincuencia organizada y el financiamiento al terrorismo de conformidad con lo dispuesto en la Constitución de la República y los tratados internacionales relacionados con la materia, suscritos y ratificados por la República Bolivariana de Venezuela.

Ahora bien, el Estado venezolano también ha venido promulgando una serie de normativas que en consonancia con la Constitución de 1999, específicamente en su art. 108 , establece que es parte de la formación ciudadana el empleo de los medios de comunicación social públicos o privados, garantizando servicios públicos de radio, televisión y redes de bibliotecas y de informática, permitiendo el acceso universal a la información, coloca en un nuevo paradigma el uso de las TICs, como parte del empoderamiento de la ciudadanía. Ello genera junto con el art. 48 de la misma carta fundamental, referido al secreto e inviolabilidad en las comunicaciones, toda una revolución.

En perfecta armonía con lo planteado por la máxima norma constitucional, se inicia un trabajo legislativo con base a los arts. 2 y 3 de

la Constitución Nacional[19], pero a cargo del poder ejecutivo, delegación muy cuestionada, especialmente a partir de la Ley Habilitante del año 2001[20]. Bajo esta potestad se dictaron varios Decretos en la materia de TICs en el país, como es el caso del Decreto No. 825 de fecha 22 de mayo del 2000, en el cual el Gobierno declara el acceso y el uso del Internet como política prioritaria para el desarrollo cultural, económico, social y político de la República, en concordancia con lo establecido en la Constitución de 1999. De igual manera, el Decreto con Fuerza de Ley Mensajes de Datos y Firmas Electrónicas, N°1.204 de fecha 10 de febrero de 2001 y publicado en Gaceta Oficial N°37.148 del 28 de febrero del 2001, con competencia en materia de gestión de incidentes telemático. También destacan en el marco de la ley habilitante, el Decreto con Fuerza de Ley de Registro Público y Notariado, de fecha 04 de mayo de 2006, la cual consagra en la parte final del art. 2 que para el cumplimiento de las funciones registrales y notariales, de las formalidades y solemnidades de los actos o negocios jurídicos, se aplicarán los mecanismos y la utilización de los medios electrónicos consagrados en la Ley.

De igual manera con base a las potestades contenidas en la ley habilitante del año 2001, el Presidente de la República dictó, el Decreto-Ley Orgánica de Ciencia, Tecnología e Innovación, publicado en fecha 30 de agosto de 2.001, el mismo tiene como fin reestructurar y organizar todo el Sistema Nacional de Ciencia, Tecnología e Innovación, que venía

[19]Art. 2 "Venezuela se constituye en un Estado democrático y social de Derecho y de Justicia, que propugna como valores superiores de su ordenamiento jurídico y de su actuación, la vida, la libertad, la justicia, la igualdad, la solidaridad, la democracia, la responsabilidad social y en general, a preeminencia de los derechos humanos, la ética y el pluralismo político". Art. 3 "El Estado tiene como fines esenciales la defensa y el desarrollo de la persona y el respeto a su dignidad, el ejercicio democrático de la voluntad popular, a construcción de una sociedad justa y amante de la paz, la promoción de la prosperidad y bienestar del pueblo y la garantía de cumplimiento de los principios, derechos y deberes consagrados en esta Constitución…"

[20]Actualmente la previsión constitucional que consagra la Ley Habilitante, no depende de que si el interés público requiere o no que se dicten medidas económicas y financieras, sino que exista un consenso político por medio del cual se acuerde autorizar al Presidente para dictar Decretos Leyes sobre ciertas materias. Lo trascendente en este cambio Constitucional es la ausencia de limitación constitucional en cuanto a la materia a delegar, pareciera que de las normas que consagran la autorización legislativa o la Ley Habilitante permiten que se autorice al Presidente para legislar en cualquier materia, sin embargo, esto debe verse con mucho cuidado y atado a los antecedentes constitucionales que la Ley Habilitante se ha ganado en nuestro país. No sólo es inexistente la materia a delegar en el texto constitucional, que repetimos debe hacerse el análisis del caso, sino que a su vez está ausente algún motivo o ratio para despojar temporalmente al Poder Legislativo de sus funciones primigenias para delegárselas al Presidente

manejándose por el Consejo Nacional de Investigaciones Científicas y Tecnológicas (CONICIT), y que de ahora en adelante se denominará Fondo Nacional de Ciencia, Tecnología e Innovación (FONACIT), el cual es un Instituto Autónomo, con personalidad jurídica y patrimonio propio e independiente del Fisco Nacional, que se encuentra adscrito al Ministerio del Poder Popular para Ciencia, Tecnología e Innovación. De esta manera, se pretende redefinir los ejes de acción y planes para promover y estimular todas aquellas actividades relacionadas con el desarrollo científico y tecnológico en el país.

A este respecto se fue creando un marco legal que por una parte impulsaría las TICs en el país y, por la otra, frente a ese desarrollo de las TICs, se garantizara un uso adecuado de las mismas, sobre todo en pro de la defensa de la soberanía nacional y frente a ello la Ley Orgánica de la Seguridad de la Nación antes referida, también consagra la institución de los Riesgos Tecnológicos y Científicos y, señala

> El conocimiento, la ciencia y la tecnología son recursos estratégicos para lograr el desarrollo sustentable, productivo y sostenible de nuestras generaciones, pero agrega, el Estado tiene la obligación de vigilar que las actividades tecnológicas y científicas que se realicen en el país no representen riesgo para la seguridad de la Nación.

También consagra varias zonas de seguridad y, aunque no establece al ciberespacio como parte de esas zonas, señala en su art. 48 numeral 7.Cualquier otra zona de Seguridad que se considere necesaria para la seguridad y defensa de la Nación, donde podría estar incluido el ciberespacio.

Por su parte también la Constitución de la República Bolivariana de Venezuela en su artículo 156, numeral 28 ha otorgado al Poder Nacional la competencia sobre "el régimen del servicio de correo y de las telecomunicaciones, así como el régimen y la administración del espectro electromagnético". Es por ello que la Ley Orgánica de Telecomunicaciones (LOTEL), (Reformada en fecha 07 de febrero de 2011), ha desarrollado el precepto constitucional citado estableciendo un marco general que permite la regulación de las telecomunicaciones, y en particular el régimen de concesiones para el uso del espectro radioeléctrico, como bien del dominio público. El mencionado instrumento legal ha otorgado la competencia para la regulación del sector a la Comisión Nacional de Telecomunicaciones (CONATEL), inicialmente creada mediante el Decreto Nº1826 del 5 de septiembre de 1991 y a la cual la (LOTEL)

ha convertido en un instituto autónomo, con personalidad jurídica, patrimonio propio e independiente del Fisco Nacional y autonomía técnica, financiera, organizaba, normativa y administrativa

De igual manera, la Ley de Responsabilidad social en Radio, Televisión y Medios Electrónicos (Reformada en fecha 07 de febrero de 2011), incorpora el art. 27 que señala lo siguiente:

> En los servicios de radio, televisión y medios electrónicos, no está permitida la difusión de los mensajes que:
>
> 1. Inciten o promuevan el odio y la intolerancia por razones religiosas, políticas por diferencia de género, por racismo o xenofobia
>
> 2. Inciten o promuevan y/o hagan apología al delito
>
> 3. Constituyan propaganda de Guerra
>
> 4. Fomenten zozobra en la ciudadanía o alteren el orden público.
>
> 5. Desconozcan a las autoridades legítimamente constituidas.
>
> 6. Induzcan al homicidio.
>
> 7. Inciten o promuevan el incumplimiento del ordenamiento jurídico vigente.
>
> Los proveedores de medios electrónicos deberán establecer mecanismos que permitan restringir, sin dilaciones, la difusión de mensajes divulgados que se subsuman en las prohibiciones contenidas en el presente artículo…Los proveedores de medios electrónicos serán responsables por la información y contenidos prohibidos a que hace referencia el presente artículo...

Por su parte, otra disposición legal a considerar es la Ley especial contra los Delitos Informáticos de fecha 30 de octubre de 2001, con competencia en materia de seguridad de información al consagrar pena doble (pecuniaria y privativa de libertad) a quienes cometan delitos contra los sistemas que utilizan tecnologías de información.

Finalmente, a criterio particular del autor debe observarse con atención dos disposiciones legales recientes.

Una en materia de Registro Civil, la recién reforma de la Ley Orgánica de Registro Civil venezolana, de fecha 15 de septiembre de 2009, favorece este ámbito con los certificados electrónicos, pues todas las actas emitidas por el Registro Civil digitalizadas con certificados electrónicos,

tendrán la misma eficacia probatoria de los documentos públicos. Se establece una cadena de confianza a fin de constituir las bases confiables para una eficaz identificación por medios electrónicos.

La ley de Infogobierno de fecha 17 de octubre de 2013 tiene por objetivo no copiar los programas privativos, sino desarrollar aplicaciones informáticas en tecnologías libres que soporten los procesos que requieran los servicios públicos para una interacción ágil y eficiente con la ciudadanía, mediante operaciones automatizadas y auditables. La Superintendencia de servicios de certificación electrónica (SUSCERTE) ha expresado: "La migración a software libre es una garantía importante, porque nos asegura el acceso al código, y **permite verificar que este no tenga 'puertas traseras'**. Usar software libre es 'blindarnos' de los ataques cibernéticos contra el Poder Público, que mantienen una tendencia creciente (Noticias 24, 2015).

4.2. Aspectos Técnicos

La **Dirección Conjunta de Seguridad Informática de la Fuerza Armada Nacional Bolivariana (FANB)**, en el 2014 se convirtió en la **Dirección Conjunta de Ciberdefensa**. Esta unidad tiene un doble propósito: 1. unificar la estrategia comunicacional de la FANB y, 2. proteger la plataforma informática de la institución castrense que incluye hardware, software y telecomunicaciones de los sistemas de armas.

El Consejo Nacional de Uso de las Tecnologías de Información tiene como función principal promover el adecuado uso y aprovechamiento de las tecnologías de información en el Poder Público y en el Poder Popular, estableciendo lineamientos, políticas y estrategias para el acceso, uso, promoción, adquisición y desarrollo de las tecnologías de información libres.

Comisión Nacional de las Tecnologías de Información se encargará de administrar el repositorio de programas informáticos libres y de programas informáticos utilizados por el Poder Público y por el Poder Popular, así como la información asociada a éstos y, otorgar, suspender y revocar la certificación de los programas informáticos, equipos y servicios en materia de tecnologías de información, a ser desarrollados, adquiridos, implementados y usados por parte del Poder Público y del Poder Popular

El Centro Nacional de Tecnologías de Información, ente encargado de apoyar a la Comisión Nacional de las Tecnologías de Información,

al proponer las líneas de investigación para el desarrollo de programas y equipos informáticos que apoyen la solución de problemas en el Poder Público y en el Poder Popular, y contribuir con la formación y difusión para la apropiación social del conocimiento en tecnologías de información libres en el país

Ven **CERT** es el Sistema Nacional de Gestión de Incidentes Telemáticos de la República Bolivariana de Venezuela. Su principal objetivo, como **CERT** gubernamental es la prevención, detección y gestión de los incidentes telemáticos generados en los sistemas de información de la Administración Pública Nacional y los Entes Públicos a cargo de la gestión de Infraestructuras críticas de la Nación[21]. También emite avisos de seguridad, noticias, alertas, boletines en materia de seguridad de la información y estadísticas. Dicta cursos presenciales, talleres y eventos de seguridad de la información, donde se otorga material de sensibilización en materia de seguridad. De igual modo, ofrece Sistemas de monitorización y alerta temprana (SMAT). Red de *Honey pots*[22]. Recomendación de herramientas de seguridad evaluadas previamente por el VenCERT para la protección de aplicaciones web y, finalmente realiza análisis básico y avanzado de vulnerabilidades, y evaluación de los niveles de seguridad de los sistemas y aplicaciones de los organismos adheridos al VenCERT.

La Superintendencia de Servicios de Certificación Electrónica (**SUSCERTE**)[23], es un servicio desconcentrado sin personalidad jurídica. Es el organismo encargado de coordinar e implementar el modelo jerárquico de la infraestructura Nacional de Certificación Electrónica, también acredita, supervisa y controla a los Proveedores de Servicios de Certificación (PSC) y es el ente responsable de la Autoridad de Certificación Raíz del Estado Venezolano. Así mismo tiene como

[21]Ministerio del Poder Popular para las Telecomunicaciones e Informática. Resolución N°063de fecha 11 de noviembre de 2008

[22]En computación, un honeypot es una trampa para detectar, desviar o contrarrestar de alguna manera, los intentos de uso no autorizado de los sistemas de información. Utilizada para recoger información sobre los atacantes y sus técnicas Diccionario de Informática y Tecnología. http://www.alegsa.com.ar/Dic/honeypot.php#sthash.PPppfySH.dpuf (consultado 28 de mayo de 2015)

[23]Creada mediante el Decreto- Ley N° 1.204 de fecha 10 de febrero de 2001, sobre Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.148 del 28 de febrero de 2001

alcance proveer estándares y herramientas para implementar una tecnología de información óptima en las empresas del sector público, a fin de obtener un mejor funcionamiento y proporcionar niveles de seguridad confiables

El **Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL)** es un organismo adscrito al Ministerio del Poder Popular para la Ciencia, Tecnología e Industrias Intermedias; y surge como una iniciativa para impulsar los procesos necesarios que permitan transitar el camino hacia el verdadero rol que deben cumplir la Ciencia, la Tecnología y la Innovación para alcanzar el desarrollo económico, social y político de la Nación. En tal sentido este Centro busca promover la investigación, desarrollo y apropiación de Tecnologías Libres. Para lograr tales propósitos CENDITEL tiene como misión Promover la reflexión, investigación, desarrollo y apropiación de Tecnologías Libres pertinentes, acordes con la Sociedad Democrática, Participativa y Protagónica de la Nación. Para la realización de proyectos se debe organizar y administrar recursos de manera tal que se pueda culminar todo el trabajo requerido dentro del alcance, el tiempo, y costos definidos.

4.3 Aspectos Organizativos

Otro de los indicadores que sirven como base de la medición por parte de la UIT, es el aspecto organizacional, el cual se pudiese considerar cumplido por parte de Venezuela, a través de dos entes que están adscritos al Ministerio del Poder Popular para Educación Universitaria, Ciencia y Tecnología y han celebrado un convenio conjunto. Se trata de SUSCERTE Y CENDITEL quienes han firmado electrónicamente un Convenio donde se establece el intercambio de formación entre ambos entes en materia de criptografía e informática forense. Asimismo, impulsarán en conjunto la construcción de un marco nacional de ciberseguridad y ciberdefensa para el Estado venezolano, que será sometido para la discusión al más alto nivel y con todos los entes implicados en la materia. Desarrollarán líneas de investigación en protocolos seguros para el anonimato en redes y para la homologación de dispositivos criptográficos. Impulsarán la inclusión de contenidos curriculares en ciberseguridad y criptografía en las carreras de computación y matemática, respectivamente, de las universidades más importantes del país. Revisarán el marco legal vigente en materia de

ciberseguridad. Seguirán fortaleciendo el uso de tecnologías libres como garantía de mayor seguridad y de impulso a una concepción libertaria y liberadora en el acceso al conocimiento tecnológico.

Adicionalmente, CENDITEL alojará en sus instalaciones el centro de datos de respaldo del AC[24] Raíz de certificación electrónica que administra SUSCERTE, y este último formará personal de CENDITEL en la administración de estos servicios.

4.4. Aspecto sobre Creación de Capacitación.

La capacitación forma parte integrante de las tres primeras medidas (legal, técnica y orgánica). La capacitación se puede medir en función de la existencia del número de programas de investigación y desarrollo (I&D), enseñanza y capacitación, y de profesionales y organismos del sector público certificados. En este sentido, se desarrollaron en el Estado Mérida la I Jornada de Seguridad Informática, auspiciada por el Ministerio para Educación Universitaria, Ciencia y Tecnología para la exposición de desarrollos nacionales en certificados, firmas, cifrado y validación electrónica. Participaron estudiantes, integrantes de la comunidad científica regional, abogados, jueces y servidores públicos de instituciones gubernamentales. Este tipo de jornada busca concienciar a la ciudadanía en general y a los trabajadores sobre la ciberseguridad, para expandir el debate hacia la comprensión jurídica, social y forense. En estas Jornadas se propicia la educación sobre el usos seguro de las TICs . Sin embargo, se reconocieron algunos vacíos legales en la actualidad. "A pesar de las iniciativas impulsadas en los últimos 15 años, es necesario apuntar a la coherencia y generar instrumentos legales adicionales, como una ley de protección de datos personales y de comercio electrónico", Explicó que el contexto gubernamental de la seguridad informática gira alrededor del concepto y estrategia nacional de ciberseguridad y ciberdefensa (Agencia Venezolana de Noticas, 2015).

En este mismo orden de ideas, otra iniciativa ahora desde el ámbito privado en Venezuela está a cargo de la Red Venezolana de Derecho Informático, su ubicación electrónica es reveredin.blogspo.com. Tienen una alianza estratégica con el Instituto Venezolano de Investigación Criminal para desarrollar talleres, cursos y seminarios sobre ciberataques y ciberdelitos.

[24]Autoridad de Certificación Raíz

4.5. Aspectos de Cooperación

El tema de la ciberseguridad o ciberdefensa entraría directamente en la región latinoamericana a partir del año 2002 por medio de la petición[25] que el gobierno de los Estados Unidos de {America hace a la Comisión de Seguridad Hemisférica de la OEA, para que autorice a un funcionario del Departamento de Estado a presentar una iniciativa diplomática de ciberseguridad a los países miembros de la OEA. Esta exposición daría como resultado que un año después los Estados Miembros de la OEA reconocerían formalmente la necesidad de generar y aplicar una estrategia interamericana para combatir las amenazas a la seguridad cibernética[26].

De igual manera, se han establecido redes internacionales para el desarrollo de contenidos como es el caso: Latinoamérica y el Caribe, Tecnologías de Información y Comunicación, (LACTIC). Este programa incluye a todos los países de la región en el desarrollo de contenidos educativos de primaria, y red internacional virtual en educación (RIVED), la cual agrupa a Venezuela, Colombia, Brasil y Argentina, y desarrolla contenidos científicos en la educación secundaria.

En este mismo orden, una delegación de la Comisión Nacional de Telecomunicaciones (Conatel) participó el pasado 14 de agosto de 2014, en el Comité Consultivo Permanente I de la Comisión Interamericana de Telecomunicaciones, CITEL, encuentro en el que se abordaron tópicos como la Calidad de Servicio de Telecomunicaciones y de Roaming, Ciberseguridad, Banda Ancha para el Acceso Universal y la inclusión social. Venezuela informó su reciente ingreso al Comité Asesor Gubernamental de la Corporación de Internet para la Asignación de Nombres y Números (ICANN, por su sigla en inglés).

Por su parte, como medida interna el Ministerio del Poder Popular para Ciencia, Tecnología e Innovación venezolano, aspira involucrar en sus procesos a todos los sectores, desde el mundo de los investigadores

[25]Consejo Permanente de la OEA/Ser.G Organización de los Estados Americanos, presentación sobre ciberespacio, (presentado por la delegación de los Estados Unidos). OEA/Ser.G. CP/CSH/INF.15/02. 7 noviembre 2002

[26]OEA, desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética, resolución aprobada en la cuarta sesión plenaria, celebrada el 10 de junio de 2003 http://www.oas.org/juridico/spanish/agres_1939.pdf. consultado el 20 de julio de 2014.

y tecnólogos, reconocidos por la comunidad científica, hasta aquel conocimiento derivado de las comunidades o de las vocaciones productivas regionales.

En total armonía con lo planteado se debe subrayar la necesidad de conformar un sistema de defensa y seguridad cibernética en el cual concurran tanto el sector estatal como la sociedad civil, entendida como lo no público, esto es, el sector empresarial privado, los ciudadanos, y la academia. Adicionalmente hemos de sugerir que un sistema así conformado debe integrar la seguridad con la defensa, como dos partes indisolubles.

Conclusiones

En cuanto a los aspectos legales en materia de ciberseguridad en Venezuela el resultado o grado de desarrollo de este indicador es parcial, se concluye esto porque en las diferentes normas se hace una simple inserción de oraciones relacionadas con la informática, pero las mismas deben ser revisadas, pues vulneran algunos derechos fundamentales como la libertad de expresión, tal es el caso de las ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos, así en materia de certificaciones electrónicas por parte del Registro Civil, ello sólo en la norma, pues en la práctica, las certificaciones no son obtenidos digitalmente aún y, por su parte, la ley penal especial existente, tendría que ser objeto de una interpretación amplia para poder extender su aplicación al ciberespacio, por ejemplo, en los casos del fraude o la falsificación, así como el acceso indebido, sabotaje y el robo. En definitiva se muestra una normativa que no está relacionada específica o exclusivamente con la ciberseguridad.

Actualmente en lo atinente al aspecto organizativo se han creado varias entidades, resaltando una entidad nacional VenCERT, que es el Sistema Nacional de Gestión de Incidentes Telemáticos, de acuerdo a los indicadores del IMC un EIII (equipo de intervención en caso de incidentes informáticos), en el ámbito nacional. Sin embargo, no se pude definir los marcos nacionales (y sectoriales) nacionales aprobados para la aplicación de normas de ciberseguridad internacionalmente reconocidas.

En cuanto al aspecto organizativo, no se observa claramente una estrategia nacional, modelo de gobernanza y organismo supervisor, por lo que los esfuerzos de los distintos sectores e industrias acaban siendo dispares e incoherentes y frustran los esfuerzos por armonizar a escala

nacional el desarrollo de las capacidades de ciberseguridad. Es necesario crear estructuras efectivas para promover la ciberseguridad, combatir el ciberdelito y promover la importancia de la vigilancia, el aviso y la respuesta ante incidentes para garantizar la coordinación de iniciativas nuevas y existentes dentro de los organismos, entre los sectores y a través de las fronteras.

Finalmente el aspecto de cooperación en Venezuela se logra pero de manera más acentuada en el caso de cooperación intra-organismos públicos, poca entre sectores público y privado, una relación que debería ser bidireccional: las empresas necesitan crear valor alrededor del negocio de la ciberseguridad y el Estado precisa de tecnología que le permita disponer de una capacidad solvente y vanguardista de ciberseguridad, que en otras regiones en el escenario internacional es más avanzada.

Referencias bibliográficas

ABI RESEARCH Y LA UNIÓN INTERNACIONAL DE TELECOMUNICACIONES.2014. Global CybersecurityIndex.Y:\APP\PDF_SERVER\ALLUSER\IN\BDT\KUSHTUEV\S_GCI_CONCEPTUAL FRAMEWORK.DOCX (361935) 15-05-2014.

ASAMBLEA NACIONAL CONSTITUYENTE. Constitución. G.O. 36.860 de fecha 30 de diciembre de 1999.

ASAMBLEA NACIONAL.Ley de Infogobierno Gaceta Oficial No. 40.274 de fecha 17 de octubre de 2013.

ASAMBLEA NACIONAL.Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos (Reformada Gaceta oficial 39.610 de fecha 07 de febrero de 2011).

ASAMBLEA NACIONAL. Ley especial contra los Delitos Informáticos. Gaceta Oficial No. 37.313 de fecha 30 de octubre de 2001.

ASAMBLEA NACIONAL.Ley Orgánica de Registro Civil. Gaceta Oficial No. 39.264 de fecha 15 de septiembre de 2009.

ASAMBLEA NACIONAL.Ley Orgánica de Seguridad de la Nación. Gaceta Oficial Número: 37.594 de fecha 18 de diciembre de 2002.

ASAMBLEA NACIONAL.Ley Orgánica de Telecomunicaciones (LOTEL), (Reformada en Gaceta Oficial No. 39.610 de fecha 07 de febrero de 2011.

ASAMBLEA NACIONAL. Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo. Gaceta Oficial Nº 39.912 del 30 de abril de 2012.

BRAHIMA SANOU Director de la Oficina de Desarrollo de las Telecomunicaciones de la UIT.

CHÁVEZ, Hugo Proyecto Nacional Simón Bolívar, Segundo Plan Socialista de Desarrollo Económico y Social de la Nación, 2013-2019.

CONSEJO PERMANENTE DE LA OEA/Ser.G Organización de los Estados Americanos, presentación sobre ciberespacio, (presentado por la delegación de los Estados Unidos). OEA/Ser.G. CP/CSH/INF.15/02. 7 noviembre 2002.

FOJÓN, Enrique, COZ, José, MIRALLES, Ramón y LINARES, Samuel. 2012. "Estado de riesgo del ciberespacio". En REGO, Miguel (Coord). D`ANTONIO, Gianluca y REY, Nathaly (Eds) La Ciberseguridad Nacional, un compromiso de todos. La necesidad de evolucionar de una cultura reactiva a una de prevención y resiliencia. Spanih Ciber Security Institute – ISMS Forum Spain. Madrid.

FOJÓN, Enrique y SANZ, Angel. "Ciberseguridad en España: una propuesta para su gestión". En: Revista ARI.2010, No. 77, Real Instituto Elcano. Madrid. p.9-12.

FORO MEASURING COUNTRIES' READINESS AND BUILD CAPACITY ON CYBERSECURITY (Medición de la preparación y creación de capacidades de los países en materia de ciberseguridad) celebrado en la Conferencia de la UIT, que se inauguró en Dubai (Emiratos Árabes) del 30 de marzo hasta el 10 de abril de 2015.

MINISTERIO DEL PODER POPULAR PARA LAS TELECOMUNICACIONES E INFORMÁTICA.Resolución N°063de fecha 11 de noviembre de 2008.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA). Desarrollo de una estrategia interamericana para combatir las amenazas a la seguridad cibernética, resolución aprobada en la cuarta sesión plenaria,

celebrada el 10 de junio de 2003. En http://www.oas.org/juridico/spanish/agres_1939.pdf. Fecha de consulta 20 de julio de 2014.

PRESIDENCIA DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA.Decreto- Ley N° 1.204 de fecha 10 de febrero de 2001, sobre Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.148 del 28 de febrero de 2001.

PRESIDENCIA DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA. Decreto No. 825 de fecha 22 de mayo del 2000, publicado en Gaceta Oficial N°36.955.

PRESIDENCIA DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA.Decreto-Ley Orgánica de Ciencia, Tecnología e Innovación. Gaceta Oficial del Decreto N° 1.290, en fecha 30 de agosto de 2001.

PRESIDENCIA DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA.Decreto con Fuerza de Ley de Registro Público y Notariado, de fecha 04 de mayo de 2006.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT). Guía de ciberseguridad para los países en vías de desarrollo. Edición 2007.

AGENCIA VENEZOLANA DE NOTICIAS, Gestión Social. 2015. En Mérida exponen desarrollos venezolanos en ciberseguridad. En http://www.avn.info.ve/contenido/m%C3%A9rida-exponen-desarrollos-venezolanos-ciberseguridad. Fecha de consulta el 30-08-2015.

NOTICIAS 24. 2015. Ley de Infogorbierno busca lograr la independencia tecnológica en Venezuela. En http://www.noticias24.com/venezuela/noticia/276521/ley-de-infogobierno-busca-lograr-la-independencia-tecnologica-en-venezuela/. Fecha de consulta 29 de mayo de 2015

PRESIDENCIA DEL GOBIERNO DE ESPAÑA. 2013. Estrategia de Ciberseguridad Nacional. 2013. En http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf. Fecha de consulta 11de febrero de 2014.

TRIBUNAL DE JUSTICIA DE UNIÓN EUROPEA, Gran Sala. 2014. Sentencia ECLI: EU: C: 2014:317 Asunto C-131/12. Google contra la Agencia Española de Protección de Datos (AEPD) de fecha 13 de mayo de 2014 En. http://curia.europa.eu/juris/liste.jsf?td=ALL&language=es&jur=C,T,F&num=C-131/12&dates=%2524type%253Dpro%2524mode%

DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA. En: http://www.alegsa.com.ar/Dic/honeypot.php#sthash.PPppfySH.dpuf. Fecha de consulta 28 de mayo de 2015.

BUREAU OF JUSTICE ASSISTANCE. 2009 Internet Crime Report. En: http://www.ic3.gov/media/annualreport/2009_ic3report.pdf. Fecha de consulta 22 de abril de 2015.