Gobernanza de Internet en Ecuador: Infraestructura y acceso

Encuentro Nacional de Gobernanza de Internet en Ecuador, 2014

J. Andrés Delgado

Cómo citar este documento

Delgado, J. A. (2014, noviembre). *Gobernanza de Internet en Ecuador: Infraestructura y acceso.* Artículo presentado en el Encuentro Nacional de Gobernanza de Internet, Quito, Ecuador. Obtenido de http://delgado.ec/research/es/Gobernanza_Internet_Ecuador_2014.pdf

Contenidos

Prefacio

Cuando se decidió realizar el Primer Encuentro Nacional de Gobernanza de Internet en Ecuador, se estableció claramente la necesidad de contar con un insumo que permitiese a cualquier persona conocer el desarrollo de los procesos de gobernanza que se hubieren dado hasta la fecha en el país. Originalmente esta fue la intención del presente texto y, como tal, se dividió en función de las áreas usadas por Fundación Diplo (infraestructura y estandarización, marco legal, economía, desarrollo, sociedad y cultura).

Habiendo sido poco el tiempo para la preparación de este documento, se decidió reducir el espectro de temas tratados en pos de conservar la calidad del producto. El uso de documentos adicionales, similares al reporte de Freedom of Net publicado el año pasado, serán imprescindibles si se quiere tener una discusión seria del tema de gobernanza en el país. Este primer acercamiento incluye las siguientes temáticas:

- Infraestructura en telecomunicaciones
- TCP/IP
- DNS
- Neutralidad de la red
- Nube informática
- Ciberseguridad
- Cifrado
- Propiedad Intelectual

El estudio de cada una de las áreas se realizó mediante una revisión de las publicaciones académicas, tanto de fuentes internacionales como de aquellas ubicadas en los repositorios nacionales. Se incluyeron, además artículos noticiosos relevantes de fuentes gubernamentales, privadas o independientes y, cuando fue pertinente, se acudió a grupos de trabajo específicos. Esto fue importante para los temas que actualmente se encuentran en evolución activa, lo cual es muy común cuando se trata de Internet.

Las fuentes, en su mayoría, cuentan con un enlace web que permitirá su revisión por parte del lector. Asimismo, el presente texto será puesto a disposición del público en una o varias páginas web. Esperamos que futuros trabajos en el tema de gobernanza de Internet en Ecuador consideren prácticas similares a fin de contar con herramientas de fácil acceso para la investigación y toma de decisiones por parte de los actores que hacemos parte del proceso.

Introducción

Nunca se pensó que Internet tendría el impacto mundial que generó décadas después de su creación. De hecho, en un inicio casi no se podía percibir intervención de tipo estatal y menos aún mercantil en la gobernanza de la red. Esto no fue accidental puesto que los creadores de Internet consideraban que eso garantiza algunas de sus características centrales: apertura, neutralidad, descentralización. Sin embargo, con el paso del tiempo, Internet atrajo la atención de varios sectores lo que ha hecho que tanto el sector privado como los gobiernos quieran influir en *cómo se manejan* los asuntos vinculados a Internet. Esto se da especialmente por la convergencia de Internet, telecomunicaciones y el manejo de contenidos,[1] y debido al gran protagonismo que la red empezó a tener en la geopolítica global.

Este proceso de intervención ha sido paulatino y, gracias a ello, no tenemos un *gobierno* de Internet dirigido por Estados, sino un proceso de *gobernanza* donde intervienen varios sectores y actores. Y a pesar de que son finalmente las resoluciones, acuerdos, políticas, leyes y reglamentos los instrumentos (emitidos por Estados) que guían esta gobernanza, estos en su mayoría adoptan resoluciones previas de reuniones con varios actores, en lo que se denomina un modelo multisectorial (*multistakeholder,* en inglés*)*.

Existen varios antecedentes importantes que llevaron a la adopción de este modelo. Por ejemplo, entre 1994 y 1998 surgió un gran conflicto cuando la Fundación Nacional de Ciencia de los Estados Unidos quiso subcontratar a una compañía privada para gestionar el sistema de dominios. La resolución final del conflicto, donde intervinieron Estados y organizaciones internacionales, fue el establecimiento de la Corporación de Internet para la Asignación de Nombres y Números (ICANN).

En 2003 y 2005, se desarrollaron las dos fases de la Cumbre Mundial sobre la Sociedad de la Información, con la presencia de 19000 participantes de 174 países. El objetivo era reducir la brecha digital en el acceso a las tecnologías de la información, especialmente El objetivo de la primera fase era redactar y propiciar una clara declaración de voluntad política, y tomar medidas concretas para preparar los fundamentos de la Sociedad de la Información para todos, que tenga en cuenta los distintos intereses en juego. El objetivo de la segunda fase fue poner en marcha el Plan de Acción de Ginebra y hallar soluciones y alcanzar acuerdos en los campos de gobierno de Internet, mecanismos de financiación y el seguimiento y la aplicación de los documentos de Ginebra y Túnez. En esta cumbre se definió que

> La gobernanza de Internet es el desarrollo y aplicación por parte de gobiernos, sector privado y sociedad civil, en sus roles respectivos, de principios, normas, reglas, procedimientos de toma de decisiones y programas que den forma a la evolución y uso de Internet.[2]

---

[1] Además de la Web y los protocolos originales para transmisión de archivos y mensajes, Internet permite la transmisión de contenido y comunicación multimedia, telefonía (VoIP), televisión (IPTV), el uso de juegos en línea, entre otros.

[2] Definición emitida por la **Cumbre Mundial sobre la Sociedad de la Información** (**CMSI**) avalada por la Resolución 56/183 de la Asamblea General de la ONU.

Posteriormente, el primer Foro de Gobernanza de Internet (IGF, por sus siglas en inglés) fue anunciado oficialmente por el Secretario General de las Naciones Unidas en julio de 2006 y ha celebrado una reunión anual desde entonces.

Los países en vías de desarrollo tienen ciertas limitaciones en cuanto a conocimientos, recursos humanos y financieros para participar sostenidamente en los debates sobre gobernanza de Internet en un entorno altamente descentralizado y multi-institucional, seguir los pronunciamientos de instituciones relevantes o asistir a las principales conferencias con una postura desarrollada e informada en un entorno de múltiples variables. .

Adicionalmente, la búsqueda de la desestructuración del poder hegemónico de Estados Unidos en Internet, ha impulsado a países como Rusia o China a abogar por un modelo intergubernamental, donde los Estados puedan tomar control de la red de una forma más directa (considerando además que muchos de los actores privados más poderosos están basados en suelo estadounidense).

En lo relativo a la discusión en América Latina sobre la gobernanza de Internet, en 2007 el gobierno de Brasil alojó la segunda reunión de Foro de Gobernanza de Internet, lo que marcó incidió en que los actores de la región se vinculen a dicha problemática, sin que ello haya significado que se la abordó desde una perspectiva regional (ONG Derechos Digitales, 2014). El debate regional empezó a constituirse en el 2008 cuando un grupo de actores propuso la creación de un espacio multisectorial para el diálogo político sobre la gobernanza de Internet. Desde ese entonces, la reunión regional sobre gobernanza de Internet se ha realiza anualmente en distintos países de América Latina.

En el 2010, la reunión regional se efectuó en Quito, Ecuador, lo que contribuyóa despertar el interés de los actores locales en los temas de la gobernanza de Internet.

En octubre del 2013, Paquistán planteó a nombre del Ecuador y otros países la creación de un mecanismo intergubernamental de gobernanza de Internet en la reunión No. 24 del Consejo de Derechos Humanos. El mismo mes, el presidente de la ICANN, Fadi Chehadi y Dilma Rousseff, presidenta de Brasil, iniciaron el proceso NETmundial, el cual contó con la presencia de representantes del sector público, privado y sociedad civil de Ecuador.

Conviene avanzar en la definición de una agenda de gobernanza de Internet de Ecuador.

Infraestructura y estandarización

A pesar de todos los matices mediante los que Internet se ha manifestado, éste es en su forma más básica un conjunto de estándares, protocolos, cables y estructuras. Sin la presencia de sus componentes técnicos, Internet no podría existir. En años recientes ha entrado en debate el tema de ciberseguridad dentro de la capa básica de Internet. Estos son temas que son difíciles de desarrollar exclusivamente a nivel local debido a la naturaleza global de Internet.

Infraestructura en telecomunicaciones

La regulación de las telecomunicaciones es un asunto complejo, puesto que involucra diversos medios como telefonía, ondas de radio, fibra óptica, entre otros. Cada una de estas herramientas tiene una regulación distinta. A nivel internacional, esta regulación es llevada a cabo por la Unión Internacional de Telecomunicaciones. En Ecuador, es ejercida por la Superintendencia de Telecomunicaciones (SUPERTEL) y su reglamentación es emitida por el Consejo Nacional de Telecomunicaciones (CONATEL). Esta institucionalidad actualmente se encuentra en debate.[3]

La liberalización del mercado de telecomunicaciones

Un número considerable de países han liberalizado sus mercados de telecomunicaciones con el objetivo de impulsar el desarrollo de nuevos servicios de comunicación al permitir el acceso a la infraestructura (de propiedad estatal) existente. En Ecuador, sin embargo, existen restricciones que dificultan este tipo de prácticas. El artículo 316 de la Constitución de la República del Ecuador (2008), por ejemplo, indica que “el Estado podrá delegar la participación en los sectores estratégicos (que incluye al sector de las telecomunicaciones) y servicios públicos a empresas mixtas en las cuales tenga mayoría accionaria”, limitando la participación del sector privado.

Incluso en el escenario de un tratado de libre comercio, las telecomunicaciones deben ser tratadas como un sector estratégico (Estévez, 2012). Un estudio realizado por CEPAL (2014) revela que la Empresa Nacional de Telecomunicaciones (CNT) estaría incluida en el escenario de un acuerdo comercial con la Unión Europea. , Esto es importante puesto que es precisamente en el sector de las telecomunicaciones donde las empresas del viejo continente tienen a uno de sus sectores más fuertes (Maldonado & Torres, 2013:148).

Recientemente la Corte Constitucional aprobó que se trate como enmienda constitucional la modificación a la carta magna. La enmienda propone que se defina a a "la comunicación como un servicio público[4] [que] se prestará a través de medios públicos, privados y comunitarios", con lo cual existe una alta probabilidad de que dicha enmienda se haga efectiva. Algunos

[3] Al momento de redactar este documento, la Asamblea Nacional (2014) ha aprobado el informe para primer debate de la nueva ley orgánica de telecomunicaciones, según la cual la SUPERTEL sería absorbida por el Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL), que mediante su Agencia de Regulación y Control, se convertiría en el ente rector, operador, administrador, regulador y de control del sector (“El control total a las telecomunicaciones”, 2014), esto supondría una contradicción con la Constitución actual y con el artículo 143 del acuerdo comercial firmado con la Unión Europea (aunque el mismo aún no entra en vigor), por lo que habrá que esperar a la decisión final antes de emitir un criterio al respecto.

grupos han interpretado esta reforma de la comunicación como servicio público y su inclusión dentro de la Ley Orgánica de Comunicación, como una forma adicional de regulación ("La comunicación, ¿un derecho constitucional o servicio público?", 2014). Esto podría o no suponer un desincentivo para la inversión. Actualmente, las relaciones entre las operadoras y el Estado siguen siendo ásperas ("Claro: 'Negociaciones para espectro 4G están estancadas'", 2014).

La última milla

El 90% del tráfico internacional en Ecuador se realiza mediante dos cables de fibra óptica: el submarino Panamericano o *Pan-Am* y el submarino Emergia o *Sam-1* (Cabrera et Col, 2014:3). En ambos[5] casos, Ecuador solicitó "la entrega de una determinada capacidad internacional con acceso Internet, para uso de desarrollo social y educativo en la estación terminal de cable submarino" a ser administrada por el Fondo de Desarrollo de las Telecomunicaciones (FODETEL). Esta capacidad correspondió al 1% y 2% respectivamente. En marzo de 2015 entraría en operaciones un tercer cable, el Pacific Caribbean Cable Systems o *PCCS*, que le permitiría al país tener un ancho de banda de hasta 100 Gbps ("Ancho de banda de Ecuador será igual que países desarrollados", 2014).

Ya en el territorio, existen 20.000 kms de fibra óptica troncal, es decir la red central de distribución y 15.000 kms adicionales en última milla, es decir la conexión directa con el cliente. Este recurso llega al 67% de los cantones del territorio nacional. El número de hogares conectados a Internet de banda ancha en 2013 es 891.000 (7.7%),[6] el porcentaje conectado a Internet de alta velocidad es 0.89%.

---

[4] La Ley Orgánica de Comunicación, en su artículo 79, señala que "la comunicación social que se realiza a través de los medios de comunicación es un *servicio público* que deberá ser prestado con responsabilidad y calidad, respetando los derechos de la comunicación establecidos en la Constitución, los instrumentos internacionales y contribuyendo al buen vivir de las personas(...)".

[5] Véase resoluciones 392-21-CONATEL-2007 y 067-04-CONATEL-2010.

[6] Según reportes de MINTEL, el precio de Internet es asequible sólo para los 4 deciles más adinerados de la población. Si se contabiliza el acceso a Internet en general, el porcentaje asciende a 28,3%, según cifras del INEC (2013).

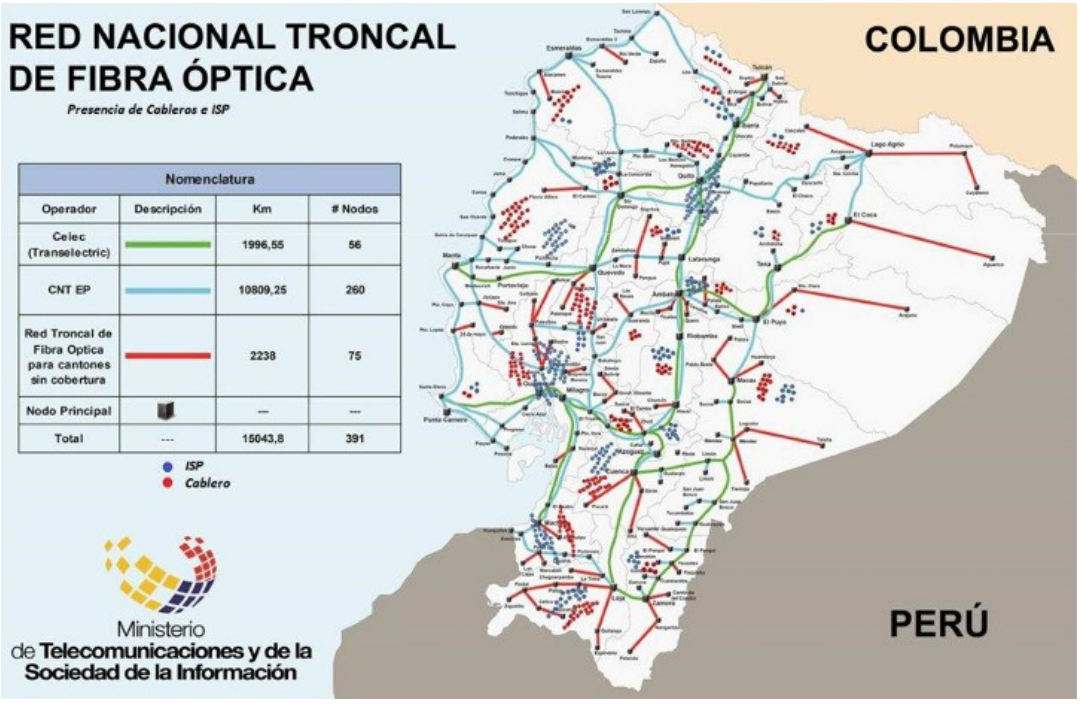

Figura 1. Red Nacional Troncal de Fibra Óptica. Fuente: MINTEL

Por otro lado, el número de líneas activas en el sistema móvil avanzado[7] en 2013 alcanzó los 17 millones, representando al 109% de la población (Armijos, 2013). Del total de parroquias en territorio, solamente 337 no cuentan con cobertura por servicio de datos móviles (3G y 3.5G), lo que representa al 32% del número total pero representa únicamente al 6.43% de la población (674.246 habitantes). La ventaja de la tecnología de Internet móvil es evidente, por sus menores costos de implementación y uso de infraestructura existente. Es previsible que el ensamblaje local de equipos de telefonía, que se incluye dentro de la estrategia de cambio de matriz productiva, o la disminución de aranceles para su importación, fruto de la entrada en vigor del acuerdo comercial con la Unión Europea, incrementen el uso de Internet móvil (Valarezo et col., 2014).

Dentro de este escenario donde prevalece la telefonía móvil,[8] es importante considerar las implicaciones que este tipo de infraestructura de acceso suponen en el tema de gobernanza de Internet, específicamente aquellas relacionadas con la protección de la privacidad. , La tecnología móvil maneja estándares cerrados, su firmware no es accesible (Bini, 2014) y en el país existe registro obligatorio de todos los dispositivos móviles. La vigilancia tiene el potencial de producir no sólo violaciones directas a la privacidad y la libertad de expresión, sino también otros daños como ataques remotos, sanciones legales, exposición a ataques de terceros y, en general, es perjudicial para el ejercicio de los derechos humanos (Torres, 2014), como veremos

[7] Los operadores dominantes son Claro con 68% y Movistar con el 30%, dejando el 2% para la empresa pública, CNT

[8] Según proyecciones del Ministerio de Telecomunicaciones y Sociedad de la Información (2013), en 2017 habrá un incremento de la penetración de conexiones a Internet fijo de 16 puntos porcentuales, mientras que el incremento en la penetración de la telefonía móvil sería de 43 puntos porcentuales.

más adelante. Esta tendencia no es exclusiva de Ecuador, sino que se da a nivel mundial (Tejada et col., 2014).

La implementación de redes comunitarias, garantizada en la constitución (Alvear, 2011), sería una opción adicional en sectores rurales donde la penetración es baja. A pesar de haber sido sugerido previamente (Torres, 2014), se desconocen esfuerzos sistemáticos de parte del Estado para su implementación.

El espectro radioeléctrico

El artículo 408 de la Constitución de Montecristi (2008) manifiesta que:

> Son de propiedad inalienable, imprescriptible e inembargable del Estado los recursos naturales no renovables y, en general, los productos del subsuelo, yacimientos minerales y de hidrocarburos, sustancias cuya naturaleza sea distinta de la del suelo, incluso los que se encuentren en las áreas cubiertas por las aguas del mar territorial y las zonas marítimas; así como la biodiversidad y su patrimonio genético y el espectro radioeléctrico [respecto a los cuales] el Estado participará en los beneficios del aprovechamiento de estos recursos, en un monto que no será inferior a los de la empresa que los explota.

Tras un reclamo de emisoras, canales de televisión y empresas de telecomunicaciones, y por solicitud del desaparecido Consejo Nacional de Radio y Televisión, la Corte Constitucional dictaminó que el espectro radioeléctrico “no se inserta dentro de la categoría de recursos naturales no renovables, no obstante, con el fin de evitar congestiones en el uso de las telecomunicaciones (...) se trata de un recurso limitado”. Asimismo señaló que se trata de un recurso estratégico[9] (“Espectro no es recurso no renovable, interpreta la Corte Constitucional”, 2009). Quien entonces presidiera la Asamblea Nacional, Fernando Cordero, declaró previamente que de darse esta aclaración, se interpretaría que su uso “no tiene que pagar el 50% de las utilidades” (“En video, asambleístas constituyentes de PAIS hablan sobre espectro radioeléctrico”, 2014).

Pese a esto, en 2014 se generó malestar social tras el anuncio gubernamental de la repartición de las utilidades fruto del uso de dicho espectro, que suponía que el 80% de las utilidades que hasta el momento perciben los empleados de las empresas de telecomunicaciones ,(alrededor de 4500 familias), serían reasignados directamente al Estado (“Utilidades de las empresas de telefónia [SIC] celular se reinvertirán [SIC] en proyectos de inversión social”, 2014).

Esto aparentemente se resolverá con la aprobación de la nueva normativa de la Ley Orgánica de Comunicación, con la que se busca eliminar problemas de interpretación y se mantienen las utilidades de los empleados de empresas privadas, percibidas por uso del espectro radioeléctrico (“Concluyó el primer debate en proyecto de ley de telecomunicaciones”, 2014).

[9] Lo que significa que el Estado se reserva el derecho de administrar, regular, controlar y gestionar dicho recurso.

Por su parte, el MINTEL está implementando[10] un plan maestro de migración a televisión digital terrestre para liberar el espectro radioeléctrico y ha previsto el inicio del apagón tecnológico para fines de 2016[11] ("Ecuatorianos deben adquirir televisores con estándar ISDBT-TB", 2014). Otra consecuencia de la migración es que la televisión pasa de ser un medio unilateral a ser un medio de comunicación bidireccional, ya que necesita de un canal de retorno para implementar la interactividad. Este proceso estaría finalizado en diciembre de 2018 (Martínez, 2014).

TCP/IP

Una vez establecida la capa física para el funcionamiento de Internet, se necesitó de estándares que aseguren la robustez de una interconexión global. Así fue que se llegó a la implementación del protocolo TCP/IP, que se basa en tres principios básicos:

1. *conmutación de paquetes*: es la fragmentación de un paquete de datos en partes más pequeñas para facilitar su transmisión. Estos paquetes son reorganizados en el destino final.
2. *robustez*: o disciplina estática. En palabras de Jon Postel es "ser conservador en lo que haces, ser liberal en lo que se acepta de los demás". , Este principio aparentemente contradictorio intenta mantener estándares estrictos y funcionales pero al mismo tiempo estar dispuesto a aceptar modificaciones en función de las necesidades de los usuarios.
3. *formación de redes punto a punto* (*end-to-end*): es aquella donde el canal de datos (la red) se utiliza para comunicar dos puntos únicamente, sin tener que ser forzosamente analizados por un intermediario.

Existen dos temas de gobernanza vinculados al protocolo TCP/IP, la introducción de nuevos **estándares** y la transición de IPv4 a **IPv6**, producto del agotamiento del primero. Cualquier modificación a los estándares existentes suponen riesgos enormes para Internet y, por este motivo, el responsable de dicha labor, el Grupo de Trabajo de Ingeniería de Internet (IETF por sus siglas en inglés) es muy cuidadoso al respecto (Kurbalija, 2014).

Cuando se planificó la cuarta versión del protocolo de Internet (1981), el primero en ser implementado a gran escala, no se consideró que habría tantos dispositivos conectados a la red. 4300 millones de identificadores parecían suficientes, pero dado que cada equipo que se conecta a Internet necesita una IP, éstas se agotan rápidamente. En Ecuador, quedaban menos de un 5% de direcciones a mediados de 2012 ("El congreso de Internet se inauguró hoy en Quito", 2012). El 10 de junio del presente año, LACNIC envió un comunicado en el cual indicó que "la región ingresó definitivamente en la fase de agotamiento de la vieja tecnología de Internet (IPv4)".

A pesar de que muchos proveedores de servicios de Internet (ISP, por sus siglas en inglés) locales ya están preparados o preparándose para desplegar IPv6 y de que varias instituciones

[10] Mediante Resolución RTV- 681-24-CONATEL-2012 se emitió el mencionado plan. El 23 de diciembre de 2013, se emitió el Reglamento Técnico RTE 83 para Televisores, fecha a partir de la que todos los televisores, que se importen, fabriquen, ensamblen o comercialicen en el Ecuador deben ser aptos para el estándar ISDB-Tb.

[11] En el 2016 iniciará en: Quito, Guayaquil, Cuenca. Posteriormente, en el 2017 se realizará el apagón analógico en varias capitales de provincia y, finalmente, en el 2018, todo el territorio nacional tendrá únicamente señales de televisión digital.

gubernamentales y académicas ya funcionan con ambos protocolos (Pérez, 2014), al día de hoy, la mayoría de usuarios se conectan a Internet dentro de sub-redes administradas por los proveedores de servicio, mediante soluciones “parche” como los mecanismos NAT y CIDR. Eso quiere decir que nuestro equipo tiene acceso a Internet público pero Internet no tiene acceso a nuestro equipo, al menos no directamente. Esto compromete el principio de extremo a extremo y podría comprometer la integridad de la información. Estas soluciones, a pesar de no ser las ideales, son de fácil aplicación y representan menores costos, incluso podrían existir ganancias indirectas al mantener el viejo esquema, mediante la capitalización del uso de información (Kleiner, 2014) y la especulación de las restantes direcciones IP, en su versión más antigua.

Para proveer de una solución definitiva a este problema se creó la versión seis del protocolo de Internet o IPv6 (Coellar & Cedeño, 2013), la cual cuenta con un número virtualmente infinito de identificadores, lo que permitiría contar una vez más con una red simétrica que restablece el principio de extremo a extremo. Sin embargo, este nuevo protocolo no es, en principio, compatible con el antiguo, lo que ocasiona que ambos protocolos deban coexistir hasta que se de un “apagón” del IPv4.

La migración a IPv6 comprende aspectos de política pública, economía, operativos y, aún más importante, técnicos y de ingeniería que requieren del compromiso y cooperación de todos los sectores involucrados, entre ellos las instituciones de gobierno, industria y academia (Tejada et col., 2014). Frente a esto, el MINTEL impulsó la incorporación de IPv6 como requisito en compras públicas de productos y servicios de Tecnologías de la Información y Comunicaciones y estableció lineamientos generales para la implementación y creación de un Plan Maestro de Transición de IPv4 a IPv6 (“Se agotan dominios IPV4 , pero en Ecuador se fortalece protocolo IPV6”, 2014).

Además del MINTEL, representantes de la industria (proveedores de Internet, desarrolladores de software), el sector educativo (universidades e institutos de investigación) y usuarios en general, han formado un grupo participativo abierto para ayudar a la transición. La IPv6 Task Force de Ecuador trabaja desde 1999 coordinando y comunicando en actividades relacionadas a la migración. A pesar de estos esfuerzos, al momento no existe un entendimiento cabal de la importancia de la implementación del IPv6 (Tejada et col., 2014; LACNIC, 2014) y habría un promedio de uso de 0.08%[12] entre los usuarios de todos los proveedores, excepto CNT (Aizprua, 2014).

DNS

El sistema para nombres de dominio (DNS por sus siglas en inglés) es el responsable del enrutamiento de una página web desde una dirección conocida fácilmente legible hacia una dirección IP. El sistema utiliza servidores raíz,[13] dominios de primer nivel (TLD por sus siglas en

[12] Esta estadística refleja sólo el tráfico hacia Google, sin embargo se trata de un buen indicador por ser el buscador más utilizado en el país.

[13] Ecuador maneja dos servidores raíz en su territorio, el servidor F fue instalado en 2007 y es administrado por la Asociación Ecuatoriana de Proveedores de Internet - AEPROVI, esto implica que la primera búsqueda de dominios teóricamente no saldría del país, sin embargo no se ha podido indagar al nivel necesario para sustentar esta afirmación. La infraestructura, por ejemplo, fue provista por una empresa privada que según las últimas revelaciones de Snowden sería “socio” de la Agencia Nacional de Seguridad estadounidense.

inglés) y servidores DNS (Kurbalija, 2014). Este sistema está estandarizado a nivel internacional y, por tanto, una discusión sobre su aplicación local es poco pertinente en este texto.[14] Sin embargo, una clase específica de dominio es el de nivel superior *geográfico* (ccTLD por sus siglas en inglés), el cual es usado y reservado para un país específicamente.

En el caso de Ecuador el ccTLD asignado es **.ec**[15] cuya administración es concedida por IANA a inicios de la década de 1990 a **Intercom-Ecuanex**, el primer ISP del Ecuador, ahora desaparecido. Sin embargo, por su limitada capacidad técnica y porque no disponía de un enlace dedicado a Internet, esa administración fue asumida *de facto*[16] por **EcuaNet - Corporación Ecuatoriana de Información**, en ese entonces del Banco del Pacífico (Roggiero, 2008). Luego de la crisis bancaria de finales de los 90, el NIC.ec (**NICEC S. A.)** y desde entonces es el administrador (IANA, 2014). EcuaNet fue una entidad privada[17] sin fines de lucro que facilitó la primera red de conexión a Internet satelital en Ecuador con nodos ubicados en Guayaquil, Quito, Cuenca, Ambato, Machala, Manta y Galápagos (Corporación Ecuatoriana de Información, 198?). Ecuanex, por su parte, fue el primer nodo de correo electrónico a operar en el país.

Eventualmente podría existir la intención de nacionalizar el manejo del sistema de dominios, considerando que la constitución de Montecristi (2008) designa a las telecomunicaciones como sector estratégico. Este no se trataría de un caso aislado, dado que ya se han dado casos de disputa similares en otros países. En el caso eventual de que esta situación se desarrolle, el Comité Asesor Gubernamental[18] de la ICANN adoptó los *principios para la delegación y administración de ccTLD* (2000a) y estableció los *lineamientos de Las Mejores Prácticas para Administradores de ccTLD* (2000b), los cuales especifican procedimientos y políticas para el efecto.

Para resolver disputas provenientes de terceras personas con registradores de dominios, NIC.EC ha adoptado la Política Uniforme de Resolución de Disputas (UDRP por sus siglas en inglés) de la ICANN, un proceso de arbitraje obligatorio administrativo para resolver disputas de nombres de dominio entre registradores de dominios y terceras personas. Sin embargo, hay caso como el chileno en el que un comité multisectorial se encarga de la política de administración del ccTLD.

---

[14] Ecuador ha protagonizado un sólo incidente respecto a los dominios de nivel superior genérico (gTLD por sus siglas en inglés), cuando apoyó la iniciativa de Brasil y Perú, de incluir en el sistema de alerta temprana la solicitud de registro del gTLD **.amazon** llevado a cabo por la empresa de ventas en línea del mismo nombre.

[15] El código se asigna siguiendo el código ISO 3166-1

[16] El dominio **.ec** fue registrado por Intercom-Nodo Ecuanex y estuvo a su nombre hasta 1999. Se traspasó a Ecuanet cuando este pasó a manos del gobierno como parte de la incautación del Banco del Pacífico. En ese momento, el gobierno manifestó su interés por manejar el dominio.

[17] EcuaNet se constituye en 1990, por iniciativa del Banco del Pacífico, contó además con el apoyo financiero y de infraestructura de Almacenera del Agro, IBM del Ecuador, L.E.A.S.I.N.G. del Pacífico, MasterCard, Pacific National Bank y Seguros Sucre.

[18] Ecuador no se encuentra listado dentro de los miembros de este comité ("GAC Members", 2014), sin embargo se encontró registro (Acuerdo Ministerial N° 017-2012) de la participación de Mario Ortega, asesor de despacho de MINTEL, en su reunión de 2012.

Neutralidad de la red

La neutralidad de la red es el trato isonómico que se le da a cualquier paquete de datos, sin distinción por contenido, origen y destino, servicio, terminal o aplicación. En palabras más sencillas “significa que los cables sean únicamente cables, sin que puedan tener ningún tipo de capacidad de decisión sobre lo que circula por ellos” (Dans, 2010).

Desde sus inicios, el flujo de todo el contenido de Internet fue tratado sin discriminación, sin importar si se tratase de empresas emergentes o multinacionales. No se necesitaba permiso o poder de mercado para innovar en Internet y esta ha sido reconocida como una de sus principales fortalezas (Kurbalija, 2014). El Consejo de Derechos Humanos de las Naciones Unidas reconoció la naturaleza abierta y global del Internet como una fuerza que impulsa el progreso hacia el desarrollo en sus varias formas (ONU, 2014).

En Ecuador, ll principio de neutralidad de la red es mencionado en 2006 sin mayor descripción o análisis del tema, pero ya en ese entonces se sugirió desde la academia una legislación que protegiera este principio (Richero & Cerbino, 2006). Quizás el precedente de acción civil más importante en Ecuador fue la “campaña por la inclusión del principio de neutralidad de la red en la ley de comunicación” (León, 2011) iniciada el 30 de julio de 2011, por parte del diario digital GkillCity.com. Esto, debido a que como resultado de la convergencia en Internet de servicios de voz, audio, multimedia, video, broadcasting (que incluye transmisión en vivo de audio y video), entre otros, existen muchos intereses económicos que buscan un servicio diferenciado en Internet, similar al que se da en la televisión por cable (Betancourt, 2011).

Desde hace unos pocos años, el principio de neutralidad de la red ha sido visto como uno de los temas más críticos y polémicos, junto con el de privacidad, libertad de expresión y el derecho de copia (Regattieri et al., 2014). Así, a pesar de que Dilma Rousseff señalara la importancia de la neutralidad de la red dentro del Marco Civil de Brasil, NETmundial, una iniciativa conjunta del Comité Gestor de Internet en Brasil (CGI.br) y /1Net que reúne a múltiples partes interesadas sobre el futuro de la gobernanza de Internet a nivel global, no recogió este principio dentro de sus declaraciones finales (La República, 2014). Ecuador tampoco realizó declaración alguna al respecto (Correa, 2014).

En el 2012, a través del organismo del Consejo Nacional de Telecomunicaciones, expide su reglamento, que en el Artículo 15 numeral 6 señala:

> Los prestadores de los servicios no deberán distinguir ni priorizar de modo arbitrario contenido, servicios, aplicaciones u otros, basándose en criterios de propiedad, marca, fuente de origen o preferencia. Los prestadores de los servicios pueden implementar las acciones técnicas que consideren necesarias para la adecuada administración de la red de servicios, lo cual incluye también la gestión de tráfico en el exclusivo ámbito de las actividades que le fueron concesionadas o autorizadas para efectos de garantizar el servicio.

El reglamento emitido por CONATEL, al tiempo que protege en principio la neutralidad de la red, pone también en riesgo la misma al permitir a los proveedores de servicio de Internet administrar la red bajo su propio criterio (Kelly et al., 2013; Correa, 2014). En el pasado, se han dado prácticas atentatorias al principio de neutralidad en la red mediante la compartición de

servicio[19], donde no se le otorga al cliente la velocidad contratada, reduciendo su capacidad de acceder a los contenidos que este desee (Andrade, 2011). Existe, además, falta información y transparencia en cuanto a la forma en cómo se gestiona y garantiza técnicamente el servicio (Merchán & Carrillo, 2009).

Estos incidentes y otros que permiten la comercialización de un servicio con ventaja competitiva sobre otro, han generado pronunciamientos por parte de los usuarios para que se evite la comercialización de Internet solo para servicios determinados, así como reclamos por un compromiso más serio por parte de la Superintendencia de Telecomunicaciones para el control de calidad del servicio de las empresas prestadoras (La Revista, 2014). Por su parte, la Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación, dentro de su propuesta de ley Código Orgánico de la Economía Social de los Conocimientos y la Innovación (COESCI), ha incluido en su artículo N° 36:[20]

> El Estado generará las condiciones necesarias para garantizar progresivamente la universalización del acceso a las tecnologías de la información y comunicación, priorizando el uso de tecnologías libres, bajo los principios de: soberanía tecnológica, seguridad, **neutralidad de la red,** acceso libre y sin restricciones a la información y precautelando la privacidad. Estas condiciones serán respetadas sin perjuicio del proveedor del servicio. Los organismos de control competentes vigilarán que se cumplan con estas condiciones.

Se estima que este proyecto de ley sea enviado a la Asamblea Nacional a fines de 2014. Se apruebe o no esta ley, no se ha emitido normativa alguna que permita la adecuada penalización en el caso de incumplimiento por parte de los proveedores de servicio. Los procesos y procedimientos de evaluación y regulación del servicio deben ser más proactivos y de aplicación sistemática, basados en plan de corto y largo plazo, y en donde todos los ISP mejoren su nivel de competencia (Merchán & Carrillo, 2009).

El gobierno de Ecuador, por medio de su canciller Ricardo Patiño, ha señalado la importancia de “un régimen normativo internacional vinculante que acompañe los procesos de la gobernanza de la red global, con decisiones fuertes sobre cuestiones sensibles, como la protección de la privacidad, la promoción de la ciberpaz y la erradicación de la ciberguerra, la *neutralidad de la red* y la protección inequívoca de su naturaleza abierta y distribuida” ("Ecuador debe proteger a Assange y a quienes sacrifican su libertad para informar", 2014). La importancia de un tratado de ciberpaz también ha sido señalado desde la sociedad civil (Burch, 2014[a]).

---

[19] El proveedor de servicio de Internet configura su servidor a fin de que cierta cantidad de usuarios, compartan una misma línea en sus servidores, a fin de que este, pueda tener una mayor cantidad de abonados y sus servidores no colapsen por una excesiva demanda de parte de los usuarios. Por ejemplo: si el proveedor de servicio de Internet, determina que la línea de conexión será 10:1, 10 usuarios se agruparán automáticamente a nivel del servidor para que consuman una misma conexión de datos limitada a una velocidad asignada por el proveedor de servicio de Internet, una vez llenada esta línea por 10 usuarios, otra línea se abre para agrupar 10 usuarios más.

[20] Texto disponible en: http://coesc.educacionsuperior.gob.ec/

Nube informática

La nube informática es un modelo para permitir, desde cualquier lugar y a través de la red, el acceso a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) con un esfuerzo mínimo de gestión así como una mínima interacción con el proveedor del servicio.

Existen tres modelos de servicio que un proveedor de nube informática podría ofertar (Morocho, 2013):

1. Software como servicio (Saas), permite usar aplicaciones previamente instaladas.
2. Plataforma como servicio (PaaS), permite la creación de aplicaciones con herramientas e idiomas previamente definidos por el proveedor.
3. Infraestructura como servicio (IaaS), permite la instalación de cualquier tipo de software en un hardware remoto, también se lo conoce como máquina virtual.

El surgimiento del modelo de software como servicio es una tendencia a nivel mundial por considerarse una solución flexible, escalable, de bajo costo y fácil adopción (Jara, 2012; Zuñiga, 2014:62). Ecuador no es la excepción. En el sector de la pequeña y mediana empresa, por ejemplo, cerca del 40% hace uso de la nube informática (Armijos, 2013) y las páginas más visitadas por los usuarios finales, como Facebook, usualmente incorporan este tipo de servicios.

Este modelo de negocio ha despertado la preocupación de organizaciones comprometidas con la privacidad, ya que los operadores de las nubes podrían usar información privada de sus clientes sin su consentimiento (Kurbalija, 2014). Adicionalmente, un potencial atacante no tendría que infiltrarse en varios computadores para obtener la información de un grupo de personas, sino sólo en unas pocas (Ramos, 2014). La tendencia al monopolio en el mercado (Burch, 2014b) podría incrementar el número de posibles víctimas de estos ataques, como se ha evidenciado en casos recientes.

Según el fundador de la Free Software Foundation, el SaaS “equivale a ejecutar software que contiene código espía y una puerta trasera universal. Otorga al administrador del servidor un poder injusto sobre los usuarios” (Stallman, 2010). No obstante, es el segundo modelo de negocio más utilizado en el sector del software libre en Ecuador (Delgado, 2014). Esto puede ser un claro indicador de la preponderancia de este modelo de negocio, considerando que entre los desarrolladores de software libre se tiene una mayor conciencia sobre los temas de privacidad (Appelbaum, 2014a) y, a pesar de ello, este modelo persiste como uno de los más importantes.

La adopción masiva de servicios en nube podría suponer que al haber una pérdida de conexión se comprometan una mayor cantidad de servicios, como redacción de texto o incluso cálculo simplificado (Kurbalija, 2014). La problemática de interoperabilidad entre nubes se volverá crítica y podría ser necesaria la creación de un nuevo estándar para mantener una correcta funcionalidad, así como para un mayor nivel de seguridad (Kurbalija, 2014; Fox et col., 2009).

Las revelaciones de Snowden han mitigado la migración a servicios en la nube entre aquellas empresas que todavía no han adoptado este servicio (NTT Communications, 2014).La razón es que no existe suficiente confianza sobre la privacidad de los usuarios y la seguridad de la información. Esta es también la principal preocupación en Ecuador (Infantino, 2014). Según el ex-analista de la CIA, una forma en que los proveedores podrían recuperar a sus clientes es ofrecer sistemas en los cuales estos no puedan obtener acceso alguno a la información (Meyer, 2014). Este tipo de servicio se daría en una nube privada (Iaas).

A fin de aumentar el nivel de seguridad en la nube se debería también asegurar el cifrado en la transmisión de datos (Ramos, 2014; Morocho, 2013). La ubicación de los servidores también es una característica importante para los usuarios. En el sector privado, apenas un 5% de quienes toman las decisiones sobre TIC piensa que la ubicación de los servidores es intrascendente. De hecho entre el 92 - 97% refiere preferir que estos se encuentren en su propia región (NTT Communications, 2014). Esto también es cierto para los gobiernos, dado que la mayoría de granjas de servidores se encuentran en Estados Unidos (Kurbalija, 2014).

En noviembre de 2013, el en ese entonces Secretario Nacional de la Administración Pública, Cristian Castillo, declaró que “la premisa detrás de la política pública [ecuatoriana] siempre ha sido garantizar la soberanía tecnológica” (“Una Minga por la Libertad Tecnológica”, 2013). El reglamento emitido por la misma institución prohíbe a los servidores públicos el uso de nubes ubicadas fuera del territorio nacional.[21]

Si bien es cierto que la seguridad informática es la principal preocupación, también debe considerarse la importancia de otras áreas como la gestión de la identidad, la gestión del control de acceso, la seguridad forense, la virtualización, la computación distribuida, entre otras (Salazar, 2013).

El 16 de marzo de 2010, se presentó ante la Asamblea Nacional el proyecto de “Ley de Protección a la Intimidad y a los Datos personales”. El Legislativo resolvió su archivo por considerar que varias de las normas propuestas ya constan en la Constitución y en la legislación secundaria existente (Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, Ley de Transparencia y Acceso a la Información Pública), a pesar de que la propia constitución señala que debe existir una ley de protección a datos privados en registros públicos (“Asamblea Nacional archiva el proyecto de Ley de Protección a la Intimidad y a los Datos Personales”, 2010).

Debido a la falta de una regulación específica para la Nube, los contratos o acuerdos de Nivel de Servicio representan el principal elemento de cumplimiento. Salazar (2013:108) propone una serie de principios para ser incluidos en un nuevo marco regulatorio específico para Ecuador, que abarque la protección de datos en la Nube:

[21] Se prohíbe expresamente a las entidades de la Administración Pública la contratación, acceso y uso de servicios de correo electrónico en la Internet (Nube), para uso institucional o de servidores públicos, con empresas privadas o públicas cuyos centros de datos, redes (salvo la Internet), equipos, software base y de gestión de correo electrónico y cualquier elemento tecnológico necesario, se encuentren fuera del territorio nacional; y adicionalmente, si las condiciones de los servicios que tales empresas prestaren no se someten a la Constitución y Leyes Ecuatorianas.

Aprobación: Considerar si el tratamiento de datos necesita el consentimiento del titular, responsable de los datos, interesado de los datos, etc.
Delimitación de responsabilidades: Esclarecer cuáles son las responsabilidades específicas de las partes en un servicio de Cloud Computing.
Finalidad: Cual será la finalidad determinada para utilizar la plataforma de Cloud Computing, y si debe o no extenderse hacia otra finalidad.
Seguridad: Qué medidas técnicas y organizativas deben adoptarse para el tratamiento de datos en un entorno de Cloud. Si es posible establecerlo como un requisito para los proveedores de la Nube.
Transferencias Internacionales: Cómo debería realizarse el flujo transfronterizo de los datos personales y los niveles de protección que deben presentar los involucrados. Qué se reconoce por un adecuado nivel de protección.
Intervención de terceras partes que afecten el tratamiento de los datos: Qué requisitos deben cumplir las terceras partes cuando intervengan en un ambiente de Nube. Comunicación al cliente de quienes intervienen en el tratamiento de datos en la Nube.
Comunicación: Comunicación a los clientes acerca de todos los cambios y modificaciones importantes que se den en la plataforma de la Nube, que afecten el servicio, siendo claros y transparentes.
Indemnizaciones, garantías y sanciones: Cómo retribuyen los proveedores de servicios de la Nube al cliente en el caso de provocarle daños irreparables en el tratamiento de los datos.
Propiedad intelectual: Cómo se interpreta la propiedad intelectual de los datos colocados en una infraestructura de Nube. Qué sanciones se colocarían al mal uso o abuso de contenido con derechos de autor.

La responsabilidad de desarrollar este marco regulatorio, según la normativa actual, recaería sobre la Dirección de Regulación, Integración y Control de la Subsecretaría de Informática de la Secretaría Nacional de Administración Pública.[22]

Ciberseguridad

La ciberseguridad es “el cuerpo de tecnologías, procesos y prácticas destinadas a proteger a las redes, ordenadores, programas y datos de ataques, daño o acceso no autorizado” (Khan, 2013). Los objetivos generales de seguridad comprenden disponibilidad, integridad y confidencialidad de la información. En este documento nos centraremos principalmente en la ciberseguridad del Estado, dado que otros en documentos se abordará el tema de cibercrimen, la protección de datos ciudadanos y la privacidad.

Ecuador, al ser un país en desarrollo, no se había preocupado de desarrollar una infraestructura segura en el ámbito de telecomunicaciones, exceptuando tal vez parte de su infraestructura militar. En 2011, el investigador de seguridad informática Dmitry Bestuzhev, declaraba:

[22] Según acuerdo ministerial número 119, publicado en registro oficial el 1 de agosto de 2007, dentro de sus atribuciones y responsabilidades está “Preparar proyectos de leyes y reglamentos para la regulación, control, evaluación y seguimiento de los proyectos informáticos; así como para el acceso a al [SIC] información”.

> A pesar de que se han hecho esfuerzos, [en Ecuador] todavía no se trabaja en seguridad de manera sistemática con políticas definidas. El Gobierno no tiene un plan de acciones para todas las entidades del país. Muchas veces es el propietario o el administrador del sitio web el que decide qué hacer para que este sea seguro, por ello Ecuador llega a ser un blanco fácil de los atacantes (“Ecuador es un blanco fácil para ataques de hackers”, 2011).

Años después, Bestuzhev, denunció la existencia de una campaña de ciberespionaje en Latinoamérica que buscaba información *militar, diplomática y gubernamental* desde 2010, habiendo afectado en Ecuador a 280 personas (“Denuncian ciberespionaje en Ecuador”, 2014). En 2013, se produce la filtración de documentos de inteligencia de Estados Unidos que revelan vulneraciones a la privacidad de los ciudadanose intromisión en empresas estatales públicas y privadas, en los centros de investigación y desarrollo; y espionaje a las misiones diplomáticas (Greenwald, 2014; Reyes 2014). Se evidencian centros de inteligencia en diferentes territorios que típicamente usan a embajadas como sedes y a inicios de 2014, se revela una posible presencia de equipos de inteligencia de señales en la embajada de Estados Unidos en Quito (Appelbaum, 2014b). El Presidente de la República, Rafael Correa, denunció intentos de extracción de información de la presidencia y de las Fuerzas Armadas y posteriormente señaló que el país debe estar preparado para la “guerra cibernética” (“Ecuador denuncia ataques cibernéticos desde Colombia para extraer datos”, 2014).

En los últimos tres años, hemos evidenciado un esfuerzo por adaptarse a las nuevas amenazas que supone el entorno digital por parte del Estado. Hace poco el Ministerio Nacional de Defensa indicó que considera al espacio cibernético como “vital” para la seguridad del Estado y sus ciudadanos, por lo que anunció el desarrollo de capacidades operativas pertinentes y políticas específicas (“Agenda Política de la Defensa”, 2014). En mayo de 2014, se anunció la inclusión de ciberdefensa dentro del pensum académico (“Formación militar prevé ciberdefensa”, 2014) y en septiembre del mismo año se anunció que en 2015 se pondría en funcionamiento el Comando de Operaciones de Ciberdefensa (“Comando de Operaciones de Ciberdefensa para el 2015, anuncian Fuerzas Armadas de Ecuador”, 2014), el que contaría con un presupuesto inicial de 8 millones de dólares y se dedicaría principalmente a la protección de infraestructura crítica para las operaciones del Estado.

El jefe del Comando Conjunto indicó que

> existen países que tienen un gran potencial económico y bélico que han sido afectados por esta amenaza del ciberataque, ciberguerra, el espionaje. Estos pueden ser susceptibles de ser afectados desde cualquier parte del mundo, por ejemplo al control del tráfico aéreo (Garzón, 2014).

Declaraciones similares han sido efectuadas anteriormente por miembros del gabinete, como ya se mencionó previamente (“Una minga por la libertad tecnológica”, 2013), esta misma secretaría, mediante su Dirección de Arquitectura Tecnológica y Seguridad de la Información, supervisa la gestión de la seguridad de la información mediante la promulgación de disposiciones, decretos y acuerdos a nivel ministerial.

La SNAP, conjuntamente con el Ministerio de Telecomunicaciones y de la Sociedad de la Información y la Secretaría Nacional de Inteligencia, conformaron en 2011 la Comisión para la Seguridad Informática. Dicha comisión tiene dentro de sus atribuciones “establecer

lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional", como tal estableció el Esquema Gubernamental de Seguridad de la Información que deberá ser implementado en su totalidad en febrero de 2015 en todas las instituciones públicas (Acuerdo Ministerial N° 166).

En julio de 2013, probablemente como reacción a las revelaciones de Edward Snowden sobre espionaje masivo, Homero Arellano, que en ese entonces presidía el Ministerio Coordinador de Seguridad, anunció la implementación de procesos de ciberseguridad para combatir el espionaje a altos funcionarios del Estado. Arellano señaló que los procesos de cifrado eran aplicados en las Fuerzas Armadas en épocas de conflicto bélico pero que esta experiencia "podría ser llevada al sector público" ("Estado inicia planes reservados para asegurar comunicaciones entre altos funcionarios y evitar espionaje", 2013).

Adicionalmente se están empezando a implementar centros de respuesta a incidentes informáticos (Hidalgo, 2011) tanto en instituciones privadas como públicas. La Superintendencia de Telecomunicaciones ha creado el EcuCERT (OEA, 2014) como un servicio centralizado para todos los sectores, pero especialmente para el sector público.

Como ya se mencionó previamente, Ricardo Patiño, cabeza del Ministerio de Relaciones Exteriores, ha declarado el interés de Ecuador sobre "un régimen normativo internacional [para] la promoción de la ciberpaz y la erradicación de la ciberguerra ("Ecuador debe proteger a Assange y a quienes sacrifican su libertad para informar", 2014). Es importante considerar que Ecuador estaría considerando adherirse al convenio de Budapest (Stel, 2014), que es el primer instrumento internacional que busca combatir el cibercrimen mediante la armonización de leyes nacionales, la cooperación entre países y la mejoría de técnicas de investigación.

Las intenciones del gobierno incluyen una expansión regional. Siguiendo recomendaciones provistas por varias organizaciones de Sociedad Civil (Burch, 2014c), el Ministerio de Defensa ha anunciado que fortalecerá el trabajo del Centro de Estudios Estratégicos de Defensa, de la Escuela Sudamericana de Defensa del Consejo de Defensa Suramericano de UNASUR, para generar una visión compartida en defensa regional y proyectos de defensa cibernética ("Agenda Política de la Defensa", 2014). A pesar del interés de las naciones del sur global de crear condiciones para evitar que el ciberespacio sea utilizado como un arma de guerra, estas nociones no fueron mencionadas en el documento final de NetMundial (Burch, 2014b).

Existen muchos matices a considerar cuando se trata de la seguridad del Estado. En la Asamblea General de la ONU en 1946, los Estados miembros acordaron que "la libertad de información es un derecho humano fundamental y (...) la piedra angular de todas las libertades a las cuales están consagradas las Naciones Unidas". Sin embargo, en virtud de los instrumentos internacionales de Derechos Humanos, los Estados pueden restringir el acceso a la información bajo ciertas excepciones. Por ejemplo, respetar los derechos o la reputación de los demás, proteger la seguridad nacional y el orden público, y proteger la salud o la moral públicas. Sin embargo, cuando apliquen estas excepciones, los gobiernos deben sopesar el daño al interés público (Aaronson, 2014), ya que algunos derechos y libertades podrían verse afectados por las prácticas implementadas por los Estados para, por ejemplo, combatir el

ciberterrorismo, a pesar de que no exista un caso que, en estricto rigor, pueda ser calificado como tal (Reyes, 2014). También es importante considerar que la protección de las comunicaciones de funcionarios públicos debe asegurar al mismo tiempo la transparencia de sus funciones y que los Estados deben ser transparentes sobre el uso y alcance de las leyes y prácticas de vigilancia de las comunicaciones, tal como lo sugieren los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la vigilancia de las Comunicaciones (Necessary and Proportionate, 2014).

En diciembre de 2012, la compañía de tecnología rusa Speech Technology Center reveló que había sido contratada para proveer a Ecuador el servicio de "plataforma de identificación biométrica", capaz de reconocimiento facial y de voz (Kelly et col, 2013). Posteriormente se han realizado denuncias de adquisición de equipos para intercepción de tecnología GSM (Grey, 2013). Aunque las autoridades gubernamentales han declarado que esta tecnología se utilizaría para luchar contra delincuentes, existen denuncias de espionaje a organizaciones ciudadanas durante el ejercicio de sus derechos por parte de la Policía Nacional que no han sido desmentidas hasta la fecha (Ser Publicos Agencia de Comunicacion, 2013).

El 10 de agosto de 2014, entró en vigencia el nuevo Código Orgánico Integral Penal (COIP), que establece como delito la publicación de información reservada (5 a 7 años de prisión), el espionaje, la destrucción de registros (ambos con 7 a 10 años de prisión) y establece mecanismos legales para la interceptación de comunicaciones. Y actualmente se debaten dos leyes que podrían influenciar de una u otra manera el estado de la ciberseguridad:, el propuesto Código Orgánico de la Economía Social de los Conocimientos y la Innovación, que incluye cláusulas de uso obligatorio de software libre en todo el sector público y la Ley Orgánica de Telecomunicaciones.

Cifrado

En lo que respecta al cifrado, o la codificación de los documentos electrónicos y la comunicación en un formato ilegible que pueden ser leídos sólo por las partes interesadas y no por un tercero, mediante el uso de software de cifrado. Existen dos escenarios importantes. El primero son los aspectos *internacionales* sobre políticas de cifrado, puesto que la regulación de cifrado debe ser global, o al menos, involucrar a los países capaces de producir herramientas de cifrado (Kurbalija, 2014). En este escenario es importante señalar que Ecuador no ha firmado el tratado Wassenaar que limita el uso de criptografía. El segundo aspecto es la implementación de obligaciones legales locales para el cifrado de datos, lo cual hemos visto en los últimos años en Estados Unidos, Europa, Asia y Australia (Room, 2014).

El Código Orgánico Integral Penal (2013), en su artículo 190, sanciona el “descubrimiento o descifrado de claves secretas o encriptadas [y la] violación de seguridades electrónicas, informáticas u otras semejantes” con uno a tres años de prisión, pero también establece salvaguardas para el desciframiento por peritos, en caso de que un juez así lo disponga, en su artículo 145.

Marco Legal

Cada uno de los aspectos de Internet supone una dimensión legal, y en los últimos años hemos visto una constante adaptación a las nuevas tecnologías sea mediante una legislación especial (ciberlegislación) o mediante la adaptación de los principios de la ley existente a las nuevas realidades permitidas por la existencia de Internet, este último enfoque ha sido el que ha ganado más espacio en los últimos años (Kurbalija, 2014).

Existen muchísimos aspectos a ser analizados en el marco legal, pero el presente documento sólo explorará el tema de derechos de propiedad intelectual.

Derechos de propiedad intelectual

La herramienta de propiedad intelectual tiene dos objetivos principales.El primero es la protección del autor de una obra dada y el segundo es asegurar la difusión de la obra para beneficio del interés público. Es la lucha por encontrar un equilibrio entre estas dos tendencias lo que nos ayudan a comprender la coyuntura actual sobre derechos de propiedad intelectual en Internet.

Los países en vías de desarrollo se benefician mucho de las limitaciones y excepciones que permiten los acuerdos internacionales de propiedad intelectual,[23] puesto que el Internet se constituye como una herramienta de intercambio científico, de crecimiento económico y de expansión cultural. Es por eso que Ecuador ha impulsado, incluso en escenarios internacionales, la utilización del conocimiento como un bien público (Ramírez, 2012). No obstante, la ley de propiedad intelectual que existe en el Ecuador cuenta con estándares superiores a los mínimos exigidos por los tratados internacionales, y se la ha señalado como “hiperproteccionista” (Golinelli et col., 2014).

La ley de propiedad intelectual vigente, en su artículo 292, indica que la violación de los derechos de autor no es sólo responsabilidad de quien comete el acto sino que también es responsabilidad del “operador o cualquier otra persona natural o jurídica que tenga el control de un sistema informático interconectado a dicha red (...) siempre que tenga conocimiento o haya sido advertido de la posible infracción, o no haya podido ignorarla sin negligencia grave de su parte”.

Si bien se indica que dicha notificación debe estar “debidamente fundamentada”, el sistema actual ha demostrado ser muy peligroso e ineficiente. Muchos casos de *takedown*[24] han sido usados de forma inadecuada para censura, dando espacio a abusos de la industria del entretenimiento, y realizados sin el debido proceso (Freedom of Net, 2013).

Recientemente existen dos procesos en desarrollo que podrían modificar la forma en que la propiedad intelectual afecta a Internet. Por un lado la firma del acuerdo comercial con la Unión Europea (UE), el cual aún no ha sido ratificado por la Asamblea Nacional y que, por tanto, aún

[23] El término “Fair use” se usa mucho en este contexto.
[24] Takedown se refiere a retirar el acceso o el contenido de Internet.

no entra en vigor y, por otro lado, la propuesta de ley Código Orgánico de Economía Social de los Conocimientos y la Innovación.

Los tratados internacionales, por regla general, tienden a reducir el acceso al conocimiento (Aaronson, 2014) y en el caso específico del convenio suscrito con la UE existen problemas con sus artículos 251, 252 y 253 que, al igual que la ley actual, abren la puerta para mecanismos de bloqueo que no son judiciales. Al incluir a la "autoridad administrativa" como un mediador legítimo, los supuestamente afectados pueden recurrir a los prestadores de servicio de Internet para que bajen contenidos sin orden judicial y dichos prestadores, para evitar responsabilidad, los den de baja sin consultar con el que proveyó los contenidos.

Adicionalmente se indica que los ISP están libres de responsabilidad siempre y cuando "no interfiera[n] en la utilización lícita de tecnología ampliamente reconocida y utilizada *por la industria*, para obtener datos sobre la utilización de la información, legalizando la acumulación de datos y facilitando el espionaje masivo del cual ya son víctimas los ciudadanos (Greenwald, 2014). Si bien esto no es algo negativo *per se*, esto evitaría acuerdos entre los usuarios y los proveedores en el caso de que los primeros prefieran un mayor nivel de privacidad.

Otra consecuencia que puede ser atribuida a la firma del acuerdo comercial son las reformas[25] al Código Orgánico Integral Penal, las cuales imponen una multa de 500 a 500.000 dólares a los falsificadores de las marcas de fábrica o de comercio y una multa de 500 a 200.000 dólares para la piratería a escala comercial. Si bien se alude a los acuerdos previamente suscritos con la Organización Mundial de Comercio como el motivante principal de estas reformas ("Alexis Mera dice que reforma al COIP responde a tratados", 2014), lo cierto es que esas reformas, junto con muchas otras que incluyen reformas constitucionales, se dan en un marco de tiempo que sugiere una posible relación entre las mismas y el acuerdo (Profitas, 2014 & "Reforma al COIP pretende cumplir con la OMC", 2014).

Al tiempo que se realizan estas acciones que facilitan la restricción de acceso a contenidos y castigan de una forma más severa a la infracción en materia de derecho de autor, el proyecto de ley COESCI (2014), en su artículo número 36 declara que "el acceso universal, libre y seguro al conocimiento en entornos digitales se constituye como un derecho de los y las ciudadanas". Sin embargo, no se establecen mecanismos claros que permitan la consecución de este objetivo.

[25] Véase Memorando PAN-GR-2014-0247 de la Asamblea Nacional remitido por su presidenta Gabriela Rivadeneira a Libia Rivas, Secretaria General.

Bibliografía

Aaronson, S. A. (2014). Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security. *Human Rights and National Security*. Artículo en elaboración, citado con permiso de su autora.

Acs, A. (2014). Reshaping the Organizing Vision of Cloud Computing. *The Information Systems Student Journal*, 18. Obtenido de http://www.lse.ac.uk/management/documents/ISCHANNEL--9.1.pdf#page=19

Aizprua, J. (2014). *[Foro-IPv6] Resumen de Foro, Vol 30, Envío 2*. [correo electrónico] Mensaje a foro@ipv6tf.ec. Enviado el 13 de agosto de 2014.

Albornoz, M. B. (2008). Cibercultura y las nuevas nociones de privacidad.*Nómadas*, *28*, 44-50.

Albornoz, M. B., & Agüero, A. (2011). *El estado de la banda ancha en el Ecuador*. Disponible en: http://dirsi.net/sites/default/files/El%20estado%20de%20la%20Banda%20Ancha%20en%20Ecuador.pdf

Alvear, M. N. (2011). *Espectro abierto para el desarrollo Estudio de caso: Ecuador*. Obtenido de http://www5.apc.org/es/system/files/countries/Espectro_Ecuador.pdf

ANDES. (2012, octubre 4). *Asamblea Nacional archiva el proyecto de Ley de Protección a la Intimidad y a los Datos Personales*". Obtenido de http://www.andes.info.ec/

Andrade Aguilar, D. A. (2011). *La neutralidad en la red y su marco legal en Ecuador* (Doctoral dissertation, Universidad Internacional SEK). Disponible en: http://repositorio.uisek.edu.ec/jspui/bitstream/123456789/491/1/La%20neutralidad%20en%20la%20red%20y%20su%20marco%20legal%20en%20Ecuador

Appelbaum, J. (2014a, Marzo). *Free software for freedom. Surveillance and you.* Discurso presentado en LibrePlanet 2014. Cambridge, MA. Obtenido de http://media.libreplanet.org/u/zakkai/m/free-software-for-freedom-surveillance-and-you/

Appelbaum, J. (2014b, Enero 30). *Art as evidence.* Discurso presentado en Transmediale. Berlín, Alemania. Obtenido de https://www.youtube.com/watch?v=ndx0eox0Lkg

Armijos, A. (2013, Noviembre). *Tecnologías de la Información y de la Comunicación y el Desarrollo Productivo*. Conferencia presentada en el 3er. Foro Estrategia Ecuador Digital 2.0. Inclusión Digital. Obtenido de http://infocentros.gob.ec/infocentros/images/Alistamiento/Exposiciones/alvaroarmijos.pdf

Asamblea Constituyente, A. (2008). Constitución de la República del Ecuador. *Ciudad Alfaro*.

Asamblea Nacional. (2013). Código Orgánico Integral Penal.

Asamblea Nacional. (2014, Octubre 29). *Se aprueba informe para primer debate de la ley orgánica de telecomunicaciones.* Obtenido de http://www.asambleanacional.gob.ec/

Asamblea Nacional. (2014, noviembre 11). *Concluyó el primer debate en proyecto de ley de telecomunicaciones.* Obtenido de http://www.asambleanacional.gob.ec/

Asamblea Nacional. (2014, julio 17). Memorando PAN-GR-2014-0247. Obtenido de http://www.araujoasociados.net/blog/wp-content/uploads/2014/07/Proyecto-de-Ley-Reformatoria-del-C%C3%B3digo-Org%C3%A1nico-Integral-Penal-1.pdf

Betancourt, V. (2011). Ciberactivismo: ¿Utopía o posibilidad de resistencia y transformación en la era de la sociedad desinformada de la información?. *Chasqui* 116. 18 Ensayos. Disponible en: http://186.5.95.155:8080/handle/123456789/383

Bini, Ola. (2014, septiembre 20). *Encrypt everything!*. Discurso presentado en Campus Party Quito 2014. Obtenido de http://new.livestream.com/Gamatv-Vivo/CampusPartyQuito4-MainStage/videos/62585971

Brasil. Marco Civil da Internet, Lei 12.965 (2014). Disponible en: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm

Burch, S., sburch@alainet.org (2014a). *[Internetlibre] Apuntes sobre la necesidad de un tratado de ciberpaz.* [correo electrónico] Mensaje a Internetlibre@listas.asle.ec. Enviado el 13 de junio de 2014.

Burch, S. (2014b, Agosto). *Retos de la era digital para América Latina y el Caribe.* Discurso presentado en el conversatorio: "Geopolítica de la Comunicación e Integración: retos y perspectivas", organizado por CIESPAL, ALAI y el Foro de Comunicación para la Integración de NuestrAmérica. Quito. Obtenido de http://www.alainet.org/active/76641

Burch, S., sburch@alainet.org (2014c). *[Internetlibre] Recomendaciones para Unasur.* [correo electrónico] Mensaje a Internetlibre@listas.asle.ec. Enviado el 25 de mayo de 2014.

Cabrera, J. J., Tello, D. A., & Villao, F. (2014). *Estudio para determinar la necesidad del aterrizaje de un nuevo cable submarino de fibra óptica en el Ecuador.* Obtenido de http://www.dspace.espol.edu.ec/bitstream/123456789/25445/1/Resumen%20de%20tesis%20JCabrera,%20Dtello,%20director%20de%20tesis%20Ph.D.%20Freddy%20Villao%20Q.%2020%20feb%202014.pdf

Cavalli, O. (2009). Gobernanza de Internet: el debate en Latinoamérica. *Telos: Cuadernos de comunicación e innovación*, (80), 106-109.

CEPAL. (2014). *Evaluación de los posibles impactos de un acuerdo comercial entre el Ecuador y la Unión Europea.* Santiago de Chile.

Coellar Solórzano, J., & Cedeño Mendoza, J. (2013). *Propuesta para la transición de IPv4 a IPv6 en el Ecuador a través de la Supertel* (Doctoral dissertation). Disponible en: http://repositorio.ucsg.edu.ec:8080/bitstream/123456789/498/1/T-UCSG-POS-MTEL-5.pdf

Consejo de Regulación y Desarrollo de la Información y Comunicación. (2014, septiembre 17). *Comunicado-Corte Constitucional del Ecuador ratifica la voluntad popular y refuerza la libertad de expresión y el respeto a los Derechos Humanos.* Obtenido de http://www.cordicom.gob.ec/comunicado-corte-constitucional-del-ecuador-ratifica-la-voluntad-popular

Corporación Ecuatoriana de Información. (198?). *Ecuanet - Una red de comunicaciones e investigación científica para construir el futuro del país*. Obtenido de https://www.flacso.org.ec/biblio/catalog/resGet.php?resId=18779

Correa, C. (2014). La Neutralidad de la red, principio indispensable*. IT Ahora Nº5.* Obtenido de http://calu.me/bitacora/files/2014/09/IT_Ahora_Neutralidad.pdf

Dans, Enrique. (2010). *El caso Comcast vs. FCC y la neutralidad de la red*. Obtenido de http://www.enriquedans.com/2010/04/el-caso-comcast-vs-fcc-y-la-neutralidad-de-la-red.html

Delgado, J. A. (2014). Modelos de Negocio de Software Libre en Ecuador, *SENESCYT*. Obtenido de http://repositorio.educacionsuperior.gob.ec//handle/28000/1267

Ecuador Inmediato. (2013, julio 29). *Estado inicia planes reservados para asegurar comunicaciones entre altos funcionarios y evitar espionaje.* Obtenido de http://ecuadorinmediato.com/

Ecuavisa. (2014, septiembre 5). *Reforma al COIP pretende cumplir con la OMC*. Obtenido de http://www.ecuavisa.com/articulo/noticias/actualidad/79004-reforma-al-coip-pretende-cumplir-omc

El Comercio. (2012, mayo 7). *El congreso de Internet se inauguró hoy en Quito*

El Comercio. (2014, octubre 16). *Ecuador denuncia ataques cibernéticos desde Colombia para extraer datos*. Obtenido de http://www.elcomercio.com/

El Comercio. (2014, noviembre 11). *'Ancho de banda de Ecuador será igual que países desarrollados'.* Obtenido de http://www.elcomercio.com/

El Comercio. (2014, noviembre 5). *Claro: 'Negociaciones para espectro 4G están estancadas'*. Obtenido de http://www.elcomercio.com/

El Telégrafo. (2013, junio 27). *Ecuador gives up on ATPDEA exemptions, offers U.S. a $23 million grant to get some human rights education*. Obtenido de http://www.telegrafo.com.ec/

El Telégrafo. (2014, septiembre 9). *FF.AA. analizan crear un Comando Operacional de Ciberdefensa.* Obtenido de http://www.telegrafo.com.ec/

El Universo (2009, octubre 7). *Espectro no es recurso no renovable, interpreta la Corte Constitucional*. Obtenido de http://www.eluniverso.com/

El Universo (2014, mayo 21).*Formación militar prevé ciberdefensa.* Obtenido de http://www.eluniverso.com/

El Universo. (2014, septiembre 4). *Alexis Mera dice que reforma al COIP responde a tratados*. Obtenido de http://www.eluniverso.com/noticias/2014/09/04/nota/3693691/mera-dice-que-reforma-coip-responde-tratados

El Universo. (2014, septiembre 9). *Comando de Operaciones de Ciberdefensa para el 2015, anuncian Fuerzas Armadas de Ecuador.* Obtenido de http://www.eluniverso.com

El Universo. (2014, octubre 5). *La comunicación, ¿un derecho constitucional o servicio público?*. Obtenido de http://www.eluniverso.com/

El Universo. (2014, agosto 4). *En video, asambleístas constituyentes de PAIS hablan sobre espectro radioeléctrico.* Obtenido de http://www.eluniverso.com

Erique, E. (2014). *Necesidad de agregar un inciso en el art. 31 del reglamento de radiocomunicaciones ecuatoriano, para la implementación de equipos con tecnología digital, con el fin de proteger el uso de el espectro radioeléctrico* (Doctoral dissertation). Obtenido de http://dspace.unl.edu.ec/jspui/bitstream/123456789/6548/1/Erika%20Estefan%C3%ADa%20Erique%20Camposano.pdf

ESPE - Escuela Superior Politécnica del Ejército. (2014, junio 2). *Ciberdefensa: Un desafío emergente para Ecuador.* Obtenido de http://blogs.espe.edu.ec/

Estévez, I. (2012). ¿Hacia dónde va la política comercial ecuatoriana? Nuevos elementos normativos en el ámbito comercial y sus implicaciones para el Acuerdo Comercial Multipartes con la Unión Europea.

Cuadernos de política pública, (1). Obtenido de http://iaen.edu.ec/wp-content/uploads/2012/08/PolicePaper_digital.pdf

European Commision. (2014, septiembre 23). *EU and Ecuador publish text of trade agreement*. Obtenido de http://trade.ec.europa.eu/doclib/press/index.cfm?id=1156

Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., ... & Stoica, I. (2009). Above the clouds: A Berkeley view of cloud computing. *Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS*, *28*, 13.

Gagliardo G. (2011). [Carta a los organizadores del cuarto Foro Parlamentario sobre la Configuración de la Sociedad de la Información]. Archivo de *The Global Centre for Information and Communication Technologies in Parliament*. Obtenido de http://www.ictparliament.org/sites/default/files/pf2011_ecuador.pdf

Garzón, L. (2014, septiembre 9). *Discurso de apertura*. Discurso presentado en el Seminario Internacional de Ciberdefensa. Quito, Ecuador.

Golinelli, S., Vega-Villa, K. & VillaRomero, J. F. (2014). *Biodiversidad*. Obtenido de http://es.wiki.floksociety.org/w/Biodiversidad

Governmental Advisory Commit - ICANN. (2014). *GAC Members.* Obtenido el 19 de noviembre de 2014 de https://gacweb.icann.org/display/gacweb/GAC+Members

Gray, R. (2013, junio 25). *Exclusive: Documents Illuminate Ecuador's Spying Practices.* Obtenido de http://www.buzzfeed.com/

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. Metropolitan Books.

Herrera Tamariz, H. A. (2010). *El impacto de la tecnología digital y los nuevos mecanismo de protección de fonogramas controversia y soluciones en la normativa nacional.* Disponible en: http://dspace.udla.edu.ec/jspui/bitstream/33000/1314/1/UDLA-EC-TAB-2010-29.pdf

Hidalgo, J. (2011). *Implementación del CERT en Campus Party.* Conferencia presentada en Campus Party Quito 2011. Obtenido de http://es.slideshare.net/juka1978/presentacin-csirt-campus-21-oct-2011

IANA - Internet Assigned Numbers Authority. (2014). *Delegation Record for .EC*. Obtenido el 19 de noviembre de 2014 de: https://www.iana.org/domains/root/db/ec.html

ICANN. (2000a, febrero 23). *Principles for the Delegation and Administration of Country Code Top-Level Domains*. Obtenido de http://archive.icann.org/en/committees/gac/gac-cctldprinciples-23feb00.htm

ICANN. (2000b, junio 12). *Lineamientos de Las Mejores Prácticas para Administradores de ccTLD*. Obtenido de http://www.wwtld.org/ongoing/bestpractices/spanish/bp.12jun00.es.html

Infantino, M. (2014). *¿Cómo está el mercado del Cloud Computing para el canal IT de Ecuador?* [Infografía]. Obtenido el 27 de octubre de 2014 de https://licenciasonline.com

Instituto Nacional de Estadísticas y Censos. (2013). *Tecnologías de la Información y Comunicación (TIC's) 2013.* Obtenido de http://www.observatoriotic.mintel.gob.ec/images/varios/Noticias/Reportes/Resultados_principales_12_09_2014.pdf

Jara, J. (2012). *Guía para el análisis de factibilidad en la implantación de tecnologías de Cloud Computing en empresas del Ecuador*(Doctoral dissertation, QUITO/EPN/2012). Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/4649/1/CD-4281.pdf

Katz, R., & Kallorda, F. (2013). *Economic impact of broadband deployment in Ecuador*. Lima: International Development Research Center. Obtenido de http://dirsi.net/web/web/en/publicaciones/detalle/economic-impact-of-broadband-deployment-in-ecuador

Kelly, S., Truong, M., Earp, M., Reed, L., Shahbaz, A., Greco-Stoner, A.. (2013). *Freedom of Net. 29 de septiembre de 2014*, de Freedom House Sitio web: http://www.freedomhouse.org/report/freedom-net/2013/ecuador

Khan, M. F. (2013). *End user awareness of cybersecurity challenges*. Obtenido de http://www.theseus.fi/bitstream/handle/10024/61606/Khan_Muhammad%20Faheem.pdf

Kleiner, D. (2014, julio 30). *Querida #NETMundial, la Gobernanza es genial y todo, pero necesitamos EXIGIR el IPv6 ¡AHORA!* (J. A. Delgado, Trans.) Obtenido de http://www.aperturaradical.org/ (publicación original 2014, abril 28).

Kurbalija, J.. (2014). *An Introduction to Internet Governance.* Suiza: DiploFoundation.

La Hora. (2011, agosto 22). '*Ecuador es un blanco fácil para ataque de hackers'*. Obtenido de http://www.lahora.com.ec

La República. (2014, Abril 23). *Brasil aprueba ley de privacidad en Internet.* Obtenido de http://www.larepublica.ec

La República. (2014, agosto 19). *Denuncian ciberespionaje en Ecuador.* Obtenido de http://www.larepublica.ec

La Revista, El Universo. (2014, Julio 6). *4G en Ecuador*. Obtenido de http://www.larevista.ec/

LACNIC - La Casa de Internet de Latinoamérica y el Caribe. (2014, junio 10). *No hay más direcciones IPv4 en América Latina y Caribe.* Obtenido de http://www.lacnic.net/

León, J. M. (2011, Julio 29). *Inacción y Neutralidad en la Red*. Obtenido de http://gkillcity.com/

Maldonado Olivo, M. G., & Torres Ramos, J. A. (2013). *Análisis de los temas sensibles de negociación del acuerdo comercial de desarrollo entre el Ecuador y la Unión Europea, Caso Específico: Compras Públicas* (Doctoral dissertation). Obtenido de http://dspace.internacional.edu.ec:8080/jspui/bitstream/123456789/42/1/AN%C3%81LISIS%20DE%20LOS%20TEMAS%20SENSIBLES%20DE%20NEGOCIACI%C3%93N%20%20DEL%20ACUERDO%20COMERCIAL%20%20DE%20DESARROLLO%20ENTRE%20EL%20ECUADOR%20Y%20LA%20UNI%C3%93N%20EUROPEA,%20CASO%20ESPEC%C3%8DFICO%20COMPRAS%20P%C3%9ABLICAS.pdf

Martínez, E. (2014). *Análisis del espectro radioeléctrico, modificación, asignación y optimización durante la transición de televisión analógica a digital terrestre en el Ecuador*. Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/3239/1/98T00041.pdf

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. Obtenido de http://csrc.nist.gov/publications/PubsSPs.html#800-145.

Merchán, V. R., & Carrillo, J. J. (2009). *Regulación de Internet: una propuesta para el mercado ecuatoriano*. Disponible en: http://repositorio.usfq.edu.ec/bitstream/23000/1063/1/95117.pdf

Meyer, D. (2014, Julio 18). *Edward Snowden thinks cloud providers still have a chance to win users' trus*t. Obtenido de https://gigaom.com/

Ministerio Coordinador de Seguridad. (2014, Mayo 13). *Ciberseguridad: Escenarios y recomendaciones.* Nuestra Seguridad. Obtenido de http://www.nuestraseguridad.gob.ec/

Ministerio de Justicia. (2013, abril 9) *Justicia participó en COMJIB realizado en Chile*. Obtenido de http://www.justicia.gob.ec/justicia-participo-en-comjib-realizado-en-chile/

Ministerio de la Defensa Nacional. (2014). *Agenda Política de la Defensa 2014 - 2017.* Obtenido de http://www.defensa.gob.ec/wp-content/uploads/downloads/2014/06/Agenda-Politica-Defensa.pdf

Ministerio de Telecomunicaciones y Sociedad de la Información. (2014, septiembre 30). *Ecuatorianos deben adquirir televisores con estándar ISDBT-TB.* Obtenido de http://www.telecomunicaciones.gob.ec/

Ministerio de Telecomunicaciones y Sociedad de la Información. (2014, junio 12). *Se agotan dominios IPV4 , pero en Ecuador se fortalece protocolo IPV6.* Obtenido de http://www.telecomunicaciones.gob.ec/

Morocho, G. O. (2013). Limitaciones a las Técnicas Tradicionales y Actuales de Encripción Inherentes a los Servicios de la Nube. *ReDiFIS, Systems Engineering, National Polytechnic School, Ecuador*, *2*(1), 31-34. Obtenido de http://redifis.epn.edu.ec/index.php/RediFis/article/download/28/25

Naciones Unidas. 26th General Session of UN Human Rights Council. (2014). *The promotion, protection and enjoyment of human rights on the Internet*. Obtenido de bit.ly/HRonInternet

Necessary and Proportionate. (2014). *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* [aplicación digital]. Obtenido de https://es.necessaryandproportionate.org/text

NIC.EC. (n.d.). *Política de resolución de disputas.* Obtenido el 19 de noviembre de 2014 de http://nic.ec/info/resolucion.htm

NTT Communications. (2014). *NSA After-shocks*. Obtenido de http://nsaaftershocks.com/wp-content/themes/nsa/images/NTTC_Report_WEB.pdf

ONG Derechos Digitales. (2014). *Latin America in a glimpse: Human Rights and the Internet*. Obtenido de https://www.derechosdigitales.org/wp-content/uploads/igf_2014.pdf

Organización de Estados Americanos. (2014). *Tendencias de Seguridad Cibernética en América Latina y el Caribe*. Obtenido de http://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

Pérez, E., ernesto.perez@cedia.org.ec (2014). *[Foro-IPv6] estado*. [correo electrónico] Mensaje a foro@ipv6tf.ec. Enviado el 13 de agosto de 2014.

Plan V. (2014, octubre 12). *"Hay que mantener la neutralidad de la red": Juan Carlos Solines*. Obtenido de http://www.planv.com.ec

Plan V. (2014, octubre 31). *El control total a las telecomunicaciones.* Obtenido de http://www.planv.com.ec

Profitas. (2014, agosto 15). *Efectos Iniciales del Tratado Comercial con la Unión Europea*. Obtenido de http://www.profitas.com/blog/?p=2846

Ramírez, R. (2012). *La vida (buena) como riqueza de los pueblos. Hacia una socioecología política del tiempo*. Obtenido de http://iaen.edu.ec/wp-content/uploads/2013/10/La_vida_buena.pdf

Ramos, M. (2014, Sepiembre 24). *Acerca de la soberanía del Ecuador en el ciberespacio.* Obtenido de http://tercerainformacion.es/spip.php?article74389

Regattieri, L. L., Herkenhoff, G., Malini, F., & Goveia, F. *MarcoCivil: Visualizing the Civil Rights Framework for the Internet in Brazil*. Disponible en: http://ceur-ws.org/Vol-1210/datawiz2014_10.pdf

Reyes Benz, A. B. (2014). *Alcances del "ciber-terrorismo" en la sociedad contemporánea* (Doctoral dissertation, Universidad de Chile). Obtenido de http://tesis.uchile.cl/bitstream/handle/2250/116821/de-reyes_a.pdf?sequence=1

Richero, A & Cerbino, M. (2006). *Gobernanza, políticas públicas y aplicaciones de Internet*. Flacso. Obtenido de https://www.flacso.org.ec/docs/gobernanza.pdf

Roggiero, R., roberto@nuevared.org (2008). *[Asociacion] Dominios .ec.* [correo electrónico] Mensaje a asociacion@listas.asle.ec. Enviado el 12 de mayo de 2008.

Room, S. (2014). *The legal obligations for encryption of personal data*. Obtenido de http://www.xnetworks.es/contents/Vormetric/2014-The-legal-obligations-for-encryption-of-personal-data-in-Europe-Asia-and-Australia.pdf

Russia Today. (2014, Agosto 20). *"Ecuador debe proteger a Assange y a quienes sacrifican su libertad para informar"*. Obtenido de http://actualidad.rt.com

Salazar, C. (2013). *Análisis de los riesgos técnicos y legales de la seguridad en Cloud Computing.* Obtenido de http://repositorio.educacionsuperior.gob.ec/bitstream/28000/1202/1/T-SENESCYT-000333.pdf

Secretaría Nacional de Administración Pública. (2013, Noviembre 26). *Una Minga por la Soberanía Tecnológica.* Obtenido el 27 de octubre de 2014 de http://www.administracionpublica.gob.ec

Secretaría Nacional de Administración Pública. (2013). Acuerdo ministerial N° 166*. Registro Oficial Suplemento 88 de 25-sep-2013.* Obtenido de http://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-Informaci%C3%B3n.pdf

Secretaría Nacional de Administración Pública. *Acuerdo ministerial N° 119.* Obtenido de http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2014/06/siac119.pdf

Ser Publicos Agencia de Comunicacion. (2013, diciembre 23). *Declaracion del Observatorio Ciudadano ante problemas en recoleccion de firmas.* [archivo de video]. Obtenido de https://www.youtube.com/watch?v=-xCELWybBkc

Stel, E. (2014). *Seguridad y Defensa del Ciberespacio*. Editorial Dunken.

Superintendencia de Telecomunicaciones. (2012). *Ciberseguridad: Incremento del conocimiento acerca de atención de seguridad informática.* Revista Institucional SUPERTEL. Ed. 13. Obtenido de http://www.supertel.gob.ec/pdf/publicaciones/supertel13_2012.pdf

Superintendencia de Telecomunicaciones. (2014). *Disminuye la tarifa de Internet residencial. en promedio.* Obtenido de http://www.supertel.gob.ec/index.php/noticias/item/113-disminuye-la-tarifa-de-Internet-residencial

Tejada, C. E., Rodriguez, X. D., & Villao, F. (2014). *Elaborar un plan de acción para la implementación de IPv6 en el Ecuador y fomentar su uso*. Obtenido de https://www.dspace.espol.edu.ec/bitstream/123456789/25473/1/Resumen%20de%20tesis%20CTejada%20y%20XRodr%C3%ADguez,%20director%20de%20tesis%20Ph.D.%20Freddy%20Villao%20Q.%2012%20marzo%202014.pdf

Torres, J. (2014). *Open Technical Infrastructures*. Obtenido de http://floksociety.org/docs/Ingles/4/4.3.pdf

Valarezo, E. G., Zhunio, D. A., & Villao, F. (2014). *Estructuración del entorno regulatorio adecuado del Ecuador para facilitar la implementación de la banda ancha móvil.* Obtenido de https://www.dspace.espol.edu.ec/bitstream/123456789/25091/1/Resumen%20de%20Tesis%20corregida%20%20EValarezo%20-%20DZhunio,%20director%20de%20tesis%20Ph.D.%20FVillao%20%20Version%20Final%2022%20julio%202013.docx