ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ANÁLISIS DE LA GOBERNANZA DE INTERNET EN EL ENTORNO MUNDIAL Y SU IMPACTO EN ECUADOR"

TESINA DE SEMINARIO

Previo a la obtención del título de

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentado por:

FERNANDO FABRICIO JARAMILLO ASAAFF

JORGE ANDRÉS MEDINA MOLINA

GUAYAQUIL – ECUADOR

2014

AGRADECIMIENTO

Primeramente, queremos agradecer a Dios por ser nuestra fuente de sabiduría y perseverancia en nuestros trayectos de estudio.

De la misma manera agradecemos al Dr. Freddy Villao Quezada, Ph.D., por haber confiado en nosotros y elegirnos para formar parte del seminario de graduación; así también como por su guía y su predisposición a ayudarnos en la elaboración de este documento.

DEDICATORIA

Con todo el cariño de mi corazón dedico este trabajo de manera muy especial a mis queridos padres Wilman y Aideé quienes en todo momento de mi vida nunca han dudado en apoyarme y con todo el sacrificio siempre han estado ahí cuando los necesité; a mis hermanos Luis y María Fernanda, y a todos mis familiares quienes siempre han estado presente con una muestra de cariño y apoyo.

Fernando Jaramillo Asaaff

DEDICATORIA

Este trabajo va dedicado de manera muy especial a mis padres, Martha y Jorge, a mi abuela Gloria, a mi hermana Stefanny, y demás familiares que además de ser ejemplos de vida para mí, han estado de una u otra manera apoyándome en todo momento, tanto en mi formación personal como profesional.

Jorge Medina Molina

TRIBUNAL DE SUSTENTACIÓN

PhD. Freddy Villao Quezada

PROFESOR DEL SEMINARIO DE GRADUACIÓN

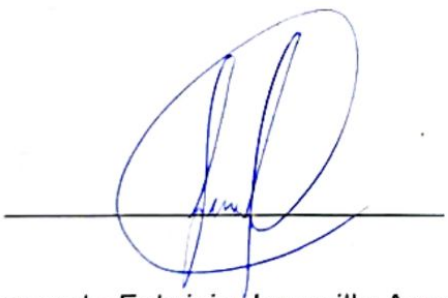
Ing. Washington Medina Moreira

PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA

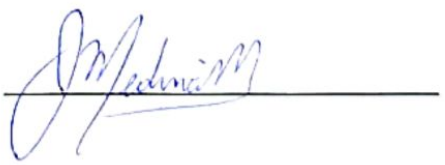
DECLARACIÓN EXPRESA

"La responsabilidad por los hechos, ideas y doctrinas expuestas en esta Tesina corresponden exclusivamente a los autores de este documento, y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL".

(Reglamento de Graduación de la ESPOL)



Fernando Fabricio Jaramillo Asaaff



Jorge Andrés Medina Molina

ABREVIATURAS

3G	Tercera Generación en Tecnología de Telefonía Móvil
4G	Cuarta Generación en Tecnología de Telefonía Móvil
ADpE	Agenda Digital para España.
AEPROVI	Asociación de empresas proveedoras de servicios de Internet, valor agregado, portadores y tecnologías de la información.
AGC	Agenda Global de la Ciberseguridad.
APT-1	Advanced Persistent Threat.
CAFEC	Centro Africano de Intercambio Cultural.
CCD	Corporación Colombia Digital.
ccTLD	Country Code Top-Level Domain.
CdE	Consejo de Europa.
CDMA 450	Code División Múltiple Access (450 Mhz).
CEPAL	Comisión Económica para América Latina y el Caribe.
CERT	Computer Emergency Response Team.
CIDH	Comisión Interamericana de los derechos Humanos.
CIIP	Critical Information Infrastructure Protection.
CMSI	Cumbre Mundial de la Sociedad de la Información.
CNT E.P.	Corporación Nacional de Telecomunicaciones - Empresa Pública.
COIP	Código Orgánico Integral Penal.
ColCERT	Centro de Respuesta de Emergencias Cibernéticas de Colombia.

CONATEL	Consejo Nacional de Telecomunicaciones.
COP	Protección de Niños en Línea.
CRC	Comisión de Regulación de Comunicaciones.
CSIRT	Computer Security Incident Response Team.
DNS	Domain Name System.
EED 2.0	Ecuador Estrategia Digital 2.0.
EEUU	Estados Unidos de Norte América.
EFF	Electronic Frontier Foundation.
eLAC	Plan de acción para América Latina y el Caribe.
ESN	Estrategia de Seguridad Nacional.
ETNO	European Telecommunications Network Operators' Association.
EUCS	Estrategia Europea de Ciberseguridad.
FGI	Foro para la Gobernanza de Internet.
FITL	Fiber in the Loop
FSFE	Free Software Foundation Europe.
FTTH	Fiber to the home.
GTGI	Grupo de Trabajo sobre la Gobernanza de Internet.
gTLD	Generic Top-Level Domain.
IANA	Agencia de Asignación de Números de Internet.
ICANN	Corporación de Internet para la Asignación de Nombres y Números.
IETF	Internet Engineering Task Force.
IMPACT	Alianza Internacional Multilateral contra las ciberamenazas.

INEC	Instituto Nacional de Estadística y Censos.
INTECO	Instituto Nacional de Tecnologías de la Comunicación.
IP	Internet Protocol.
IPv4	Internet Protocol version 4.
IPv6	Internet Protocol version 6.
IPv6TF-EC	Fuerza de Trabajo de IPv6 de Ecuador.
ISP	Internet Service Provider.
IVA	impuesto al valor agregado.
Kbps	Kilobit por Segundo.
LACNIC	Registro de Direcciones de Internet para América Latina y Caribe.
LOC	Ley Orgánica de Comunicación.
Malware	Malicious software.
Mbps	Megabit por Segundo.
Mhz	Megahertz
MINTEL	Ministerio de Telecomunicaciones y de la Sociedad de la Información.
MinTIC	Ministerio de Tecnologías de la Información y las Comunicaciones.
MIPYME	Micro, Pequeña y Mediana Empresa.
NIC.EC	Registro de Dominios – Ecuador.
NIST	Instituto Nacional de Estándares y Tecnología de los Estados Unidos.
OMPI	Organización Mundial de la Propiedad Intelectual.

ONU	Organización de las Naciones unidas.
PIB	Producto Interno Bruto.
PIPA	Protect Intelectual Property Act.
RIR	Registros de Internet regionales.
SENATEL	Secretaría Nacional de Telecomunicaciones.
SMA	Servicio Móvil Avanzado.
SND	Servicio de nombres de dominio.
SOPA	Stop Online Piracy Act.
sTLD	Sponsored Top-Level Domain.
SUPERTEL	Superintendencia de Telecomunicaciones.
TIC	Tecnología de la Información y la Comunicación.
TLD	Top-Level Domain.
UIT	Unión Internacional de Telecomunicaciones.
UIT – D	Sector de Desarrollo de las Telecomunicaciones de la UIT.
UIT – T	Sector de Estandarización de las Telecomunicaciones de la UIT.
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la cultura.

RESUMEN

En este documento analizaremos la Gobernanza de Internet en el mundo y su impacto en nuestro país. Se presentarán los antecedentes que dieron origen al término de Gobernanza de Internet en la Primera y Segunda Cumbre Mundial de la Sociedad de la Información.

De la misma manera, se realizará un estudio de las diferentes ponencias de los Foros para la Gobernanza de Internet (FGI) que han venido realizándose anualmente; destacando como temas de mayor importancia el acceso, la seguridad, la diversidad y el manejo de recursos críticos de la web.

Además, mencionaremos los distintos problemas que han surgido en el mundo debido a los diferentes pensamientos sobre el manejo de Internet en cada país, donde los principales actores han sido los gobiernos y la sociedad civil. Así también analizaremos las medidas tomadas por la Unión Internacional de Telecomunicaciones (UIT), para dar solución a los problemas y brindar seguridad en este ámbito.

Asimismo analizaremos la situación de la Gobernanza de Internet en Ecuador; verificaremos sus políticas públicas: La Constitución, Ley Orgánica de Comunicación y Código Orgánico Integral Penal, constatando que se garanticen los derechos y se impongan sanciones, según acuerdos y recomendaciones de Organismos Internacionales. Por otra parte, estudiaremos los planes y estrategias de gobierno: Plan del Buen Vivir y Ecuador Estrategia Digital 2.0., que pretenden reducir la brecha digital y asegurar el acceso a las Tecnologías de la Información y la Comunicación (TICs) en el Ecuador.

Finalmente, elaboraremos un Plan de Acción que contribuya y garantice la gobernanza de Internet en nuestro país, basándonos en lineamientos y recomendaciones del FGI, y en medidas ejecutadas en otros países que han mostrado resultados positivos en el marco de Gobernanza de Internet.

ÍNDICE GENERAL

ÍNDICE FIGURAS

INTRODUCCIÓN

En los últimos años, Internet se ha convertido en un elemento importante en la vida diaria de las personas debido a las ventajas que ésta brinda para poder acceder a información, generar conocimiento y comunicarnos en tiempo real en cualquier parte del mundo.

Debido al alcance que Internet ha tenido en la sociedad, ha surgido el interés por su control y gestión por parte de los gobiernos, sociedad civil y demás interesados, lo cual ha llevado a lo que se conoce como Gobernanza de Internet.

Luego de definir la Gobernanza de Internet como el desarrollo y aplicación de principios, normas, reglamentos y procedimientos que configuran la evolución de Internet, se empezaron a debatir sobre los mecanismos de manejo y control de la Red en lo que respecta a los recursos críticos de Internet, acceso, seguridad y demás cuestiones de interés público; teniendo como actores a los gobiernos, organismos internacionales, empresas públicas y privadas de Telecomunicaciones, universidades y sociedad civil en general.

Las insuficientes políticas públicas en torno a la Gobernanza de Internet en Ecuador, nos obliga a analizar la situación actual del país y planear estrategias nacionales que permitan gestionar Internet en Ecuador de acuerdo a las recomendaciones hechas en los Foros para la Gobernanza de Internet (FGI).

CAPÍTULO 1:

ORIGEN DE LA GOBERNANZA DE INTERNET.

1.1. Declaración de Principios de la Sociedad de la Información.

La Declaración de Principios de la Sociedad de la Información (2003, WSIS-03/GENEVA/4-S) [1] es el documento elaborado por la Unión Internacional de Telecomunicaciones (UIT) con todas las conclusiones obtenidas luego de la realización de la primera fase de la Cumbre Mundial sobre la Sociedad de la Información (CMSI). Para este evento se reunieron los representantes de los países pertenecientes a la UIT, en Ginebra del 10 al 12 de diciembre de 2003.

Los participantes de la Cumbre Mundial sobre la Sociedad de la Información priorizaron el acceso universal a la información como

garantía para el desarrollo de las personas y los pueblos. Por ello, a través del documento declararon su deseo y compromiso común de:

> *"construir una Sociedad de la Información centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos".*

El Internet se ha convertido en el medio principal que brinda dicho acceso universal a la información de forma inmediata y eficiente; por ser hoy en día la red de telecomunicaciones más grande interconectada alrededor de todo el mundo. Conscientes de lo que Internet ha logrado, los participantes de la CMSI manifestaron en el documento antes mencionado que "*Internet se ha convertido en un recurso global disponible para el público, y su gestión debe ser una de las cuestiones esenciales del programa de la Sociedad de la Información".* Esta manifestación se convirtió en el inicio para lo que hoy es "Gobernanza de Internet"; que básicamente es el "Gobierno Internacional de Internet", donde los Gobiernos, el sector privado, la sociedad civil y las organizaciones internacionales; tienen una participación importante para lograr una "*gestión internacional de Internet multilateral, transparente y democrática".*

Según el Informe de la Declaración de Principios, para lograr una adecuada gestión de Internet se deben abarcar cuestiones técnicas y de política pública, y contar con la participación democrática de todos

los interesados, a fin de garantizar *“la distribución equitativa de recursos, y un funcionamiento estable y seguro de Internet”.* Además, de la inclusión de organizaciones internacionales e intergubernamentales competentes como veedores de dicha gestión.

Por este motivo, en el informe en mención se reconoce que:

a) *“la autoridad de política en materia de política pública relacionada con Internet es un derecho soberano de los Estados. Ellos tienen derechos y responsabilidades en las cuestiones de política pública internacional relacionadas con Internet;*

b) *el sector privado ha desempeñado, y debe seguir desempeñando, un importante papel en el desarrollo de Internet, en los campos técnico y económico;*

c) *la sociedad civil también ha desempeñado, y debe seguir desempeñando, un importante papel en asuntos relacionados con Internet, especialmente a nivel comunitario;*

d) *las organizaciones intergubernamentales han desempeñado, y deben seguir desempeñando, un papel de facilitador en la coordinación de las cuestiones de política pública relacionadas con Internet;*

e) *las organizaciones internacionales han desempeñado, y deben seguir desempeñando, una importante función en la elaboración de normas técnicas y políticas pertinentes relativas a Internet”.*

La Declaración de Principios de la Sociedad de la Información marca la pauta para reuniones futuras sobre el gobierno de Internet. Los participantes solicitaron al Secretario General de las Naciones Unidas que establezca un Grupo de trabajo sobre el gobierno de Internet, a fin de investigar y formular propuestas de acción.

1.2. Plan de Acción de la Sociedad de la Información: Entorno Habilitador.

En la introducción del documento oficial de Plan de Acción (2003, WSIS-03/GENEVA/5-S) [2], se cita que:

> *"la visión común y los principios fundamentales de la Declaración de Principios se traducen en líneas de acción concretas para alcanzar los objetivos de desarrollo acordados a nivel internacional, con la inclusión de los consignados en la Declaración del Milenio; mediante el fomento del uso de productos, redes, servicios y aplicaciones basadas en las tecnologías de la información y las comunicaciones, y para ayudar a los países a superar la brecha digital".*

El Plan de Acción *"constituye una plataforma dinámica para promover la Sociedad de la Información en un nivel nacional, regional e internacional".* Tiene como objetivos *"construir una Sociedad de la Información integradora, poner el potencial del conocimiento y las TIC al servicio del desarrollo; fomentar la utilización de la información y del conocimiento; y hacer frente a los nuevos desafíos que plantea la Sociedad de la Información".*

En lo que respecta a la Línea de Acción C6: Entorno Habilitador, el documento menciona que *"para maximizar los beneficios sociales, económicos y medioambientales de la Sociedad de la Información, los gobiernos deben crear un entorno jurídico, reglamentario y político fiable, transparente y no discriminatorio".*

Mediante este documento se solicitó al Secretario General de las Naciones Unidas que establezca un grupo de trabajo sobre el gobierno de Internet, de la misma manera que se lo solicitó en el documento de la Declaración de Principios. El grupo debía:

- *"Elaborar una definición de trabajo del gobierno de Internet.*
- *Identificar las cuestiones de política pública que sean pertinentes para el gobierno de Internet.*
- *Desarrollar una comprensión común de los respectivos papeles y responsabilidades de los participantes y partes interesadas, así como la preparación de un informe sobre los resultados de esta actividad.*
- *Preparar un Informe sobre los resultados de esta actividad, que se someterá a la consideración de la Segunda Fase de la CMSI que se celebrará en Túnez, para que ésta tome las medidas del caso".*

Asimismo, en este documento se invitó a los gobiernos a "*facilitar la creación de centrales de Internet nacionales y regionales, supervisar o dirigir sus respectivos nombres de dominio de nivel superior de código de país, y promover la sensibilización sobre Internet".*

1.3. Agenda de Túnez para Sociedad de la Información: Definición de la Gobernanza de Internet.

La Agenda de Túnez para la Sociedad de la Información (2005, WSIS-05/TUNIS/DOC/6(Rev.1)-S) [3] se adoptó en la segunda fase de la Cumbre Mundial de la Sociedad de la Información. Esta reunión *"pasa de los principios a la acción, considerando los trabajos que ya se han hecho para aplicar el Plan de Acción de Ginebra e identificando donde se han logrado avances, se están logrando avances o aún no se han logrado avances; y se reafirman los compromisos adquiridos en Ginebra".*

Al comenzar la discusión sobre la Gobernanza de Internet, los participantes reconocieron *que "Internet, elemento capital de la infraestructura de la Sociedad de la Información, ha pasado de ser un recurso de investigación y académico para convertirse en un recurso mundial disponible para el público".* Además que *"la gobernanza de Internet, llevada a cabo con arreglo a los Principios de Ginebra, es un elemento esencial de una Sociedad de la Información centrada en la persona, integradora, orientada al desarrollo y no discriminatoria".*

De acuerdo al informe realizado por el Grupo de Trabajo sobre la Gobernanza de Internet (GTGI), en el documento de la Agenda de Túnez se define por primera vez al *"Trabajo de la Gobernanza de Internet"* como:

> *"desarrollo y aplicación por los gobiernos, el sector privado y la sociedad civil, en el desempeño de sus respectivos papeles, de principios, normas, reglas, procedimientos de toma de decisiones y programas comunes que dan forma a la evolución y a la utilización de Internet.".*

Cabe mencionar que el documento de la Agenda de Túnez hace énfasis en mejorar *"la coordinación de las actividades de las organizaciones internacionales e intergubernamentales, así como de otras instituciones muy interesadas en la gobernanza de Internet"*, facilitando el intercambio de información entre estas entidades. Internet es un *"medio altamente dinámico"* que obliga a todos los interesados en la Gobernanza de Internet a crear estructuras de gestión *"que respondan al crecimiento exponencial y a la rápida evolución de Internet como plataforma común para el desarrollo de aplicaciones múltiples".*

La seguridad y confianza de los usuarios de Internet, fueron los temas más importantes en ser analizados y debatidos por los participantes e interesados en la Gobernanza de Internet. El documento de la Agenda de Túnez destaca la importancia de *"crear confianza de los usuarios y seguridad en la utilización de las TIC, fortaleciendo la necesidad de continuar promoviendo, desarrollando e implementando en colaboración con todas las partes interesadas una cultura mundial de ciberseguridad".* De la misma manera manifiesta la importancia de *"enjuiciar la ciberdelincuencia"*, surgiendo *"la necesidad de concebir instrumentos y mecanismos nacionales e internacionales eficaces y eficientes, para promover la cooperación internacional, entre otros, de los organismos encargados de aplicar la ley en materia de ciberdelincuencia".*

Un fortalecimiento en la ciberseguridad permite que los usuarios tengan mayor protección de información y datos personales, garantizándoles la privacidad que requieren al usar Internet. Con la finalidad de contribuir a dicho fortalecimiento en la ciberseguridad, en el documento se exhorta a los Gobiernos que *"en cooperación con otras partes interesadas, promulguen leyes que hagan posible la investigación y enjuiciamiento*

de la ciberdelincuencia", esta medida permite asegurar la estabilidad y seguridad de Internet, combatiendo la ciberdelincuencia.

Los Gobiernos cumplen un rol importante en la Gobernanza de Internet, ya que son ellos los que deben garantizar el acceso universal de todos los habitantes de sus Naciones. Por este motivo, los participantes de la Agenda de Túnez ven con satisfacción que los Gobiernos utilicen cada vez más las TIC para dar nuevos servicios a los ciudadanos y/o mejorar los existentes. Además, alientan a los países que aún no lo han hecho a que *"elaboren programas nacionales y estrategias para el cibergobierno"*, con la finalidad de mantener el *"compromiso de convertir la brecha digital en una oportunidad digital y asegurar un desarrollo armonioso y equitativo para todos".*

Debido al crecimiento de las actividades de comercio electrónico por parte de los usuarios de Internet se solicita a través del documento de la Agenda de Túnez, *"la elaboración de leyes y prácticas nacionales de protección del consumidor y el establecimiento de mecanismos para su aplicación, cuando sea necesario, a fin de proteger los derechos de dichos consumidores que adquieran mercancías y servicios en línea".* Esta petición es importante porque involucra a los Gobiernos Nacionales en la protección del comercio electrónico y los exhorta a garantizar la confianza de los usuarios de Internet.

Así también, los participantes de la Agenda de Túnez manifestaron su deseo de convertir a Internet en una herramienta importante en el desarrollo social de todas las Naciones del Mundo, por este motivo, alentaron a lograr el desarrollo multilingüismo en Internet que permita fortalecer a las comunidades locales e indígenas, e incluirlas en el crecimiento que tiene Internet, con el fin de disminuir la brecha digital que existe dentro de un mismo país. El documento exhorta a combatir la

“brecha digital lingüística”, para lo cual, según los interesados en la Gobernanza de Internet es importante *“implementar programas que permitan la presencia de nombres de dominio y contenido multilingüe en Internet”*, para que las comunidades locales tengan acceso a las adaptaciones y traducciones de información a contenido local.

Cabe mencionar que en el documento se manifiesta la importancia del desempeño que tiene el sector privado y la sociedad civil como *“motor de innovación e inversión privada”*, ya que su participación es *“esencial tanto para el desarrollo de Internet, como de la Sociedad de la Información”*. La inversión que realiza el sector privado es importante tanto en los países en desarrollo como en los desarrollados, debido a que toda innovación agrega valor a la red y permite la evolución de nuevas aplicaciones y usos de Internet. Como la gobernanza de Internet debe ser *“completa y flexible”*, los participantes se vieron en la obligación de exigir a los Gobiernos que sigan *“promoviendo un entorno propicio para la innovación, la competencia y la inversión”* en un marco político internacional y nacional.

La Agenda de Túnez marcó el inicio de la Gobernanza de Internet; y debido a que los debates fueron exitosos, los participantes solicitaron al Secretario General de las Naciones Unidas que convoque para el segundo trimestre de 2006 una reunión del nuevo *“Foro para la Gobernanza de Internet – FGI”*, con el fin de fomentar el diálogo entre las múltiples partes interesadas, con respecto a temas sobre políticas públicas en la Gestión de Internacional de Internet. En el documento de la Agenda de Túnez se incluyen los objetivos que el FGI debe cumplir, entre los que tenemos:

- *“facilitar el intercambio de información y de mejores prácticas, entre organismos que se ocupan de políticas públicas internacionales transversales y relacionadas con Internet,*
- *aconsejar a todas las partes interesadas, para que Internet esté disponible más rápidamente y esté al alcance de un mayor número de personas en los países en desarrollo;*
- *identificar temas emergentes, exponerlos ante los organismos competentes y público en general, y, formular recomendaciones;*
- *contribuir a la creación de capacidad para la gobernanza de Internet en países en desarrollo,*
- *remover y evaluar permanentemente la materialización de los principios de la CMSI en los procesos de gobernanza de Internet;*
- *debatir temas relativos a los recursos críticos de Internet, entre otras cosas;*
- *ayudar a encontrar soluciones a los problemas que plantea la utilización correcta o incorrecta de Internet”.*

En el documento también se manifiesta que el *“Foro para la Gobernanza de Internet, tanto en su trabajo como en sus funciones, ha de ser multilateral, democrático y transparente y dejar intervenir a las múltiples partes interesadas”.* Además, se recomienda que el FGI debe *“constituirse como una estructura sencilla y descentralizada”,* y reunirse periódicamente, según se requiera, publicando las actas de

compromisos de cada reunión, de tal manera que todos tengan acceso a las estrategias de Gobernanza de Internet.

Al finalizar la Agenda de Túnez, se acordó que la primera reunión del Foro para la Gobernanza de Internet (FGI) se llevaría a cabo en Atenas 2006, debido a que el Gobierno de Grecia se ofreció como anfitrión para esta primera reunión.

CAPÍTULO 2:

FOROS MUNDIALES PARA LA GOBERNANZA DE INTERNET.

2.1. Organismos Internacionales Interesados.

El informe inaugural del Foro para la Gobernanza de Internet (2006, WSIS-2006/1)[4] cita que durante la celebración de la Segunda Fase de la Cumbre Mundial de la Sociedad de la Información, se solicitó al Secretario General de las Naciones Unidas que convocara a un nuevo foro para el diálogo entre los múltiples interesados, denominado el Foro para la Gobernanza de Internet. Entre las partes interesadas podemos mencionar a la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), Unión Internacional de Telecomunicaciones (UIT), Agencia de Asignación de Números de Internet (IANA), Corporación de Internet para la Asignación de Nombres

y Números (ICANN), Registro de Direcciones de Internet para América Latina y Caribe (LACNIC), Consejo de Europa, Organización de Cooperación y Desarrollo Económicos (OCDE), Cámara de Comercio Internacional, Gobierno de Quebec, Federación Empresarial del Japón, Sociedad de Internet, Grupo de Usuarios No Comerciales de la ICANN, Free Software Foundation Europe (FSFE), Electronic Frontier Foundation (EFF), Swiss Internet User Group, Eurolinc, Asociación de Comunicaciones Progresistas (APC), Centro Africano de Intercambio Cultural (CAFEC), Grupo de Expertos Españoles en Gobernanza de la Fundación Telefónica y la Universidad Politécnica de Madrid, Consorcio para la Utilización de los Idiomas Autóctonos en Internet, Proyecto sobre Sociedad de la Información de la Universidad de Yale, Profesor William H. Dutton (Director del Oxford Internet Institute), Vittorio Bertola (Presidente del Comité Consultivo de la ICANN), International Chamber of Commerce/Business Action to Support the Information Society (BASIS), European Telecommunications Network Operators' Association (ETNO), entre otras.

El informe menciona que el Foro *"recibió el mandato de debatir los principales temas de políticas públicas relativos a la gobernanza de Internet con objeto de contribuir a la sostenibilidad, la solidez, la seguridad, la estabilidad y el desarrollo de Internet*." Además, se estableció una Secretaría que apoye al Foro y un Grupo Consultivo que se encargue de la organización del mismo. Asimismo, se llegó a un acuerdo de que se reúna el foro una vez al año con previas rondas de consultas públicas donde intervengan las partes interesadas.

Se han realizado hasta el momento los siguientes foros:

- FGI Atenas, Grecia 2006
- FGI Río de Janeiro, Brasil 2007

- FGI Hyderabad, India 2008
- FGI Sharm El Sheikh, Egipto 2009
- FGI Vilnius, Lituania 2010
- FGI Nairobi, Kenia 2011
- FGI Baku, Azerbaiyán 2012
- FGI Bali, Indonesia 2013
- FGI Estambul, Turquía 2014

2.2. Seguridad y Apertura.

En el foro inaugural de Grecia (2006) se propusieron los temas de seguridad y apertura. Al hablar de que exista apertura o eliminación de restricciones se referían a la existencia de libertad de expresión, la libre circulación de ideas, información y conocimiento. De la misma manera, se propuso el tema de seguridad con la finalidad de generar confianza, mediante la protección del usuario contra el correo basura, virus y adquisición fraudulenta de información confidencial; y por ende se protegía la privacidad.

En diferentes ponencias de este foro se señaló que gracias al Internet muchas personas pudieron comunicarse, intercambiar información e ideas. Concordaron en que millones de personas pudieron educarse a sí mismas y participar democráticamente expresando sus opiniones gracias a que el objetivo del internet radicaba en la eficacia, mas no en el control. Además, se reconoció que el control del Internet estaba a cargo de los propios usuarios y no de un punto central determinado. Gracias a estas ponencias hubo consenso sobre eliminar restricciones en la web.

En el foro del año siguiente (2007, WSIS-2007/1)[5], en Río de Janeiro, se reafirmaron las ponencias hechas anteriormente sobre la eliminación de restricciones, aunque se reconoció que:

> *"la legitimidad de determinados objetivos de las políticas públicas, como la protección del público en general, y los niños en particular, contra los contenidos objetables de Internet y la prohibición del uso de Internet con fines delictivos, así como la difusión de información que pudiera ser perjudicial para la seguridad mundial".*

Tras esto, se recomendó:

> *"una política de autorregulación con un etiquetado facultativo como alternativa a la legislación. En los casos en que la legislación fuera absolutamente necesaria, se recomendó que ésta fuera clara, precisa y se centrara estrictamente en las actividades ilícitas que la justificaban. Además, este tipo de legislación no debía suponer cargas o costos indebidos para las empresas y debía limitar la responsabilidad que se imponía a los proveedores de servicios de Internet."* (2007, WSIS-2007/1)[5].

En el foro de Egipto (2009, WSIS-2009/1)[6], se señaló que debe existir una relación de equilibrio entre apertura y propiedad intelectual, ya que la libre circulación de información estaría limitada en cierto punto a disfrutar los resultados de un trabajo personal, aunque se reconoció que para el caso de propiedad intelectual y derechos de autor se podrían hacer excepciones como en el caso de la educación, un elemento esencial para el desarrollo. Asimismo, se hizo evidente la importancia de la privacidad, ya que ésta contribuye a la seguridad. Se señaló sobre

la importancia de una regulación en lo que respecta al robo de identidad, especialmente en países donde no hay o es muy bajo el nivel de control sobre este tema. Además, se expuso la importancia de la protección de datos personales, que también lo relacionaba a los derechos propios de libertad y seguridad de cada individuo.

En el foro de Kenia (2011,WSIS-2011/1)[7], se discutieron temas como las propuestas de bloqueo de sitios web y aplicación de filtros en redes, así como ciberseguridad, cibercrimen y el impacto que causa la restricción de acceso a Internet a individuos, comunidades e incluso un país, como fue el caso de la Primavera Árabe. También hubo un gran debate sobre quién recaía la responsabilidad al momento de hablar de ciberseguridad, finalmente se llegó a la conclusión de que todos (usuarios, familias, proveedores de servicio de Internet, legisladores, gobiernos, instituciones) están llamados a ser los responsables. De la misma manera, se continuó hablando de estos temas en el Foro del 2012, teniendo siempre como referencia a los derechos humanos. Se mencionó que todos los usuarios de Internet debemos saber los riesgos que implica navegar por la red, y que se mantenga un trato con los demás de igual manera que cuando no estamos conectados en la red.

2.3. Acceso y Diversidad.

En el primer foro (2006, WSIS-2006/1)[4] se consideró que el acceso podía ser el único problema para la mayoría de las personas, particularmente en los países en vías de desarrollo. Se señaló que:

> *“entre los elementos que podían influir en la disponibilidad y el acceso a Internet eran los precios y el costo de la conectividad internacional. Las normas y acuerdos de*

> *interconexión, incluidos los acuerdos de intercambio de tráfico, se consideraban fundamentales para que Internet funcionara de manera satisfactoria y para que su disponibilidad y fiabilidad siguieran siendo integrales y económicas."*

Además, se expuso en este foro que el acceso no sólo implicaba infraestructura, sino que se vinculó la brecha digital y el plurilingüismo con acceso. Se mencionó que:

> *"A menudo los idiomas autóctonos no eran lenguas escritas, de modo que para que los pueblos indígenas obtuvieran acceso a Internet se necesitaban soluciones no convencionales en los niveles de los programas y los equipos informáticos*." (2006, WSIS-2006/1)[4].

Entre las ponencias se sostuvo que:

> *"los problemas relativos a la interconexión de Internet, en especial a la conectividad internacional, podrían solucionarse al liberarse los mercados de telecomunicaciones que, en los últimos años, habían hecho que aumentara el acceso a la red y las innovaciones en ella, y que disminuya drásticamente el precio del acceso a Internet."* (2006, WSIS-2006/1)[4].

En este mismo foro se celebró que existían casi mil millones de usuarios de Internet aunque mucho de éstos no podían leer ni escribir en Inglés. La idea era que todas las personas pudieran usar Internet en su propio idioma, por lo que se propuso que la información circulante por la web estuviera disponible en varios idiomas. Como medida la UIT recibió de la Asamblea Mundial de Normalización de las Telecomunicaciones el mandato de estudiar los nombres de dominio internacionalizados, ya que se consideraba que su aplicación facilitaría

y aumentaría la utilización de Internet en los países en los que los idiomas autóctonos u oficiales no se representaban en caracteres del Alfabeto Internacional de Referencia.

En una ponencia en el foro de Río de Janeiro (2007, WSIS-2007/1)[5], se afirmó que

> *"para lograr el valor de servicio público de Internet era necesario que todas las personas tuvieran un acceso universal y asequible a la infraestructura de las tecnologías de la información y comunicación. Ello requería una estructura jurídica y reglamentaria estable que garantizara a las empresas la seguridad de sus inversiones, a su vez promover la libre competencia, acceso a las infraestructuras y a Internet. Se señaló también que era indispensable mejorar las infraestructuras para colmar la brecha digital, especialmente en zonas rurales. Toda mejora de infraestructura debía ir acompañada de medidas educativas sobre la forma de utilizar Internet."*

En el foro de Sharm El Sheikh (2009, WSIS-2009/1)[6], hubo consenso sobre la importancia de un organismo regulador en cada uno de los distintos países y que los gobiernos tenían la responsabilidad de formular políticas que fomenten el acceso universal; así como también se destacó la necesidad de abrir los mercados para la inversión privada. Además, se mencionó que el acceso no se limitaba solamente a lo que respecta con conectividad, sino también con precios, calidad, disponibilidad y contenido.

Además, en el documento del foro se reconoció que:

> *“era importante la inclusión de personas con discapacidad, el uso de un diseño universal y de tecnologías de apoyo. Se recordó a los representantes que un aspecto importante del apoyo a la diversidad en ese contexto debería ser el idioma hablado que no tenía forma escrita y el lenguaje de signos que no se hablaba y que, al escribirse, utilizaba representaciones icónicas”.* (2009, WSIS-2009/1)[6]

Esto, así como implicaba inclusión, también implicaba independencia económica y social para ellos.

En el foro de Bakú (2012, WSIS-2012/1)[8] se reconoció una Internet plurilingüe, donde ya no sólo dominaba el idioma Inglés, sino también idiomas como el Mandarín y Árabe. Asimismo, se presentaron resultados que indicaban que un aumento del 10 % en ancho de banda, permitía un incremento de 3.2 % en el Producto Interno Bruto de un país. Por consiguiente, un aumento en el ancho de banda de un país se considera de gran importancia en la economía del mismo y en el bienestar de la sociedad.

2.4. Gestión de recursos críticos de Internet.

Se empezó a tratar sobre el tema de los recursos críticos de Internet a partir del Foro de Río de Janeiro (2007, WSIS-2007/1)[5], aunque ya habían sido definidos en el Informe del Grupo de Trabajo sobre la Gobernanza de Internet como:

> *“las cuestiones relacionadas con la infraestructura de las telecomunicaciones, normas técnicas, intercambio de tráfico y la interconexión, administración del sistema de servidores raíz,*

> *administración del sistema de nombres de dominio, direcciones IP y el plurilingüismo".* (2007, WSIS-2007/1)[5].

El gobierno Chino propuso en este foro que debían analizarse la distribución de direcciones electrónicas de tal manera que exista un acceso igualitario de direcciones IPv6 por parte de todos los países; así como promover en el futuro un desarrollo equilibrado de Internet durante la transición de IPv4 a IPv6. También puso a debate el tema sobre la igualdad en adición, supresión y modificación de nombres de dominio de nivel superior genéricos.

En Río de Janeiro, el Consejo de Europa afirmó que:

> *"la gobernanza de los recursos críticos de Internet tenía importantes consecuencias para las políticas públicas. Cuando esos recursos, especialmente los que afectaban a los problemas en materia de políticas públicas de los Estados, eran responsabilidad de organizaciones privadas, como la ICANN, éstas se convertían en agentes del Estado y deberían ser objeto de regulación y supervisión públicas. Se afirmó también que la ICANN, que en esos momentos sólo rendía cuenta a los Estados unidos, debía rendir cuentas a la comunidad internacional en general."* (2007, WSIS-2007/1)[8].

En el foro del año siguiente (2008, WSIS-2008/1)[9] se señaló que según los principios de la CMSI, no podía existir un gobierno predominante en lo que respecta a la gobernanza.

En este foro, se recomendó:

> "*el uso de torres de protocolo dobles IPv4/IPv6 y un mayor énfasis de los países desarrollados en adoptar la*

> *iniciativa de promover el uso de la dirección IPv6, como respuesta a la limitada disponibilidad de direcciones IPv4*." (2008, WSIS-2008/1)[9].

En el foro de Egipto (2009, WSIS-2009/1)[6] se continuó exponiendo sobre el eventual agotamiento de las direcciones IPv4 y se proyectó que para el 2011, éstas ya estarían agotadas. Se consideró que había que enseñar y educar al público, así como impartir capacitación sobre IPv6. También se señaló que la participación del sector público y privado, y la sociedad civil eran necesarias.

En este mismo foro se habló sobre la importancia de nuevos dominios de nivel superior y de los nombres de dominio internacionalizados para el desarrollo. Es que ya estaba planificado para el 2010 la habilitación de nuevos dominios de nivel superior geográfico por parte de la ICANN; y entre los problemas más evidentes estaban la estabilidad y seguridad de Internet con un mayor número de nombres de dominio, derechos de marcas registradas y las funciones de los nombres de dominio internacionalizados, de nivel superior (gTLD) y los de nivel superior geográfico (ccTLD).

Algunos ponentes de los dos últimos foros antes citados venían insistiendo en que el Gobierno de Estados Unidos renuncie a su función de supervisor de nombres de dominio; y con la expiración del acuerdo entre la ICANN y Estados Unidos se sugirió que el mismo no sea renovado, y que sea en el mismo foro donde se analice el tema de los nombres de dominio (2009, WSIS-2009/1)[6].

Para el foro de Lituania (2010, WSIS-2010/1)[10] se trataron sobre las prioridades para la estabilidad a largo plazo de Internet, nuevos gTLD y nombres de dominio internacionalizados, fortalecimiento de los ccTLD

en África y capacidad de recuperación y planificación para casos de emergencia en relación con los nombres de dominio.

Se trataron en el foro de Bakú (2012, WSIS-2012/1)[8] como temas principales del manejo de recursos de Internet, el nuevo programa de gTLD de la ICANN y las recomendaciones acerca del surgimiento de mercados secundarios para las direcciones IP.

Fue muy clara la idea del nuevo programa de la ICANN de introducir un ilimitado número de sufijos como nombres de dominio de nivel superior. Se decidieron ciertas políticas como el manejo de aplicaciones para usar nombres geográficos como TLD, direccionar las peticiones hechas sobre propiedad intelectual, considerar nombres TLD relacionados con industrias, términos religiosos y culturales. También fueron consideradas aplicaciones para nombres de dominio internacionalizados, pero éstos abarcaron sólo un 6% del total de aplicaciones. (2012, WSIS-2012/1)[8].

Debido a que en la transición al nuevo protocolo de direccionamiento, IPv6, no tuvo una buena aceptación, se esperaba que surgieran mercados secundarios para la reventa de direcciones IPv4. Sin embargo, algunos de los ponentes que asistieron a Bakú consideraron que estos mercados secundarios no iban a ser necesarios debido al gran número de dispositivos que se conectaban a Internet mediante un nateo. (2012, WSIS-2012/1)[8].

2.5. Seguridad en el ciberespacio.

Los expertos en Gobernanza de Internet saben que al potenciar una mayor ciberseguridad se mejora considerablemente la confianza de los

usuarios de Internet. Estos temas de ciberseguridad son los más discutidos en las reuniones del FGI debido a su gran importancia, por este motivo, los encargados de la Gobernanza de Internet tuvieron la necesidad de incluir el tema *"Fomento de la seguridad y la confianza en el ciberespacio"* en el debate principal de la reunión del FGI del 2008. (2008, WSIS/2008/1)[9].

Según el informe, los interesados en la ciberseguridad buscaron estrategias que permitan controlar el incremento en las amenazas a la seguridad de la información, y evitar el uso de Internet con el fin de provocar inestabilidad en las seguridades internacionales. Los problemas que afectan a la ciberseguridad tales como; *"las violaciones de los derechos de propiedad intelectual y la privacidad, el envío masivo de mensajes no solicitados y la pornografía infantil"*, obliga a los interesados a juntar esfuerzos internacionales para combatir dicha problemática. Además, en el informe se reafirma que *"una Internet segura y fiable facilitaría una mayor utilización y más confianza en Internet en todo el mundo"*, por este motivo, los participantes del debate se vieron en la necesidad de exigir una mayor *"cooperación mundial entre los sectores público y privado".*

En el informe del FGI se considera que uno de los elementos decisivos para lograr una Internet segura es que *"los usuarios supieran cómo utilizarla"*, por ello, exhortaron a los gobiernos de todas las naciones del mundo a dar mayor atención a la educación para garantizar la seguridad de los usuarios al utilizar Internet.

En los debates correspondientes al acceso abierto a Internet se afirma *"la importancia del acceso abierto a Internet, la libertad de expresión y el acceso a los conocimientos"* como requisito global independientemente de las fronteras. Los interesados en la Gobernanza

de Internet perciben como una necesidad el poder lograr *“un equilibrio entre la reglamentación del gobierno y la autorregulación privada a fin de combatir el contenido pernicioso en Internet al tiempo que se fomente la libertad de expresión”.* Según el informe, los usuarios de internet tienen derecho a recibir un servicio con mínimas restricciones y máxima seguridad.

Finalmente, los participantes del FGI prepararon un proyecto, basándose en los principios y directrices para la gestión de Internet de los cuarenta y siete Estados miembros del Consejo de Europa para los debates en la Gobernanza de Internet.

En este proyecto se incluyeron recomendaciones para:

- *“Aplicar una política penal común encaminada a la protección de la sociedad contra el ciberdelito.*
- *Mejorar la red y la seguridad de la información para que pueda resistir a las acciones que comprometan su estabilidad, disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o trasmitidos.*
- *Proteger los datos personales y la privacidad en Internet.*
- *Luchar contra la piratería en la esfera de los derechos de propiedad intelectual y los derechos de autor.*
- *Promover la participación activa del público en el uso de Internet.*
- *Promover la libertad de comunicación y creación en Internet, independientemente de las fronteras.*
- *Promover la accesibilidad del público a la información vía Internet, para que todos puedan participar en el proceso de gobernanza.*

  En este mismo proyecto se incluyeron también recomendaciones concretas respecto de los siguientes aspectos del problema:

- *“Directrices sobre derechos humanos para los proveedores de servicios de Internet (ISP);*
- *Directrices sobre derechos humanos para los proveedores de juegos en línea;*
- *Protección de la dignidad, la seguridad y la intimidad del niño en Internet;*
- *Tratamiento del problema del ciberdelito;*
- *Represión del uso de Internet con fines terroristas; y*
- *Protección de los consumidores contra medicamentos y accesorios médicos falsificados”.*

2.6. Impacto de las Redes Sociales.

El creciente desarrollo de las Redes Sociales ha provocado que el acceso de nuevos usuarios a Internet aumente considerablemente, y que el uso de la red sea cada vez más prolongado. Las características de entretenimiento que las redes sociales le brindan al usuario, permitió que muchas de estas redes alcancen una considerable popularidad en los últimos años.

Para la segunda reunión del FGI del 2007 ya se examinaban cuestiones correspondientes a la Web 2.0 y sus consecuencias para la gobernanza de Internet; y se comenzaba a considerar a *“los medios sociales como un asunto a tratar desde la perspectiva social, cultural, política y económica”*, debido a que el contenido generado por los usuarios constituía una profunda revolución cultural, impulsando la globalización y la democratización de la información. (2007, WSIS-2007/1)[5].

Esta reunión permitió que los interesados en la Gobernanza de Internet comiencen a estudiar y analizar nuevas medidas que permitan *"la regulación y autorregulación de las redes sociales y las comunidades de la Web 2.0"*, a fin de garantizar siempre *"la legalidad del contenido generado por los usuarios y de las comunidades sociales en línea"*. Además, provocó que surgieran dudas entre los participantes con respecto a si el contenido de la Web 2.0 estaba realmente fomentando *"una sociedad mejor informada, más analítica y solidaria"*. (2007, WSIS-2007/1)[5].

Según, el informe del FGI (2007, WSIS-2007/1)[5], se analizaron diversas cuestiones como *"los distintos comportamientos de los distintos usuarios, y la gestión de la privacidad o la intimidad en redes sociales".* Así también, los participantes discutieron sobre lo que representa el anonimato en las redes sociales, manifestando que en algunos casos *"crea la posibilidad de efectos negativos"* debilitando *"la democracia y planteando riesgos"* para los gobiernos; mientras que en otros casos, dicho anonimato *"protege al usuario de Internet"* y se vuelve fundamental para *"promover democracia en países con restricciones a la libertad de expresión"*.

En el 2009, debido a las importantes contribuciones respecto a los medios sociales aportadas por las anteriores reuniones del FGI, los interesados en la Gobernanza de Internet se vieron en la obligación de incluir como tema de debate primordial al *"Impacto de las Redes Sociales"* en la cuarta reunión del FGI (2009, WSIS-2009/1) [6], con la finalidad de discutir nuevas cuestiones de gobernanza provocadas por la evolución de las Redes Sociales en la sociedad mundial.

El desarrollo de los medios sociales ha sido considerable en los últimos años, y hoy en día ya forman parte del uso ordinario de la Internet,

afectando *“no solo la vida cotidiana de los jóvenes, los primeros en adoptarlos, sino a casi todas las esferas sociales”,* en actividades desde *“el entretenimiento hasta los negocios y los espacios políticos”* (2009, WSIS-2009/1) [6].

Finalmente, este constante desarrollo de los medios sociales requiere la modificación de las normativas tradicionales, y es importante darle otro enfoque a dichas normas, particularmente en temas relacionado con *“la protección de la privacidad y de los datos; al contenido generado por los usuarios y al material protegido por derechos de autor; y la libertad de expresión y contenido ilícito”*.

2.7. Computación en la nube.

En la actualidad, Internet se ha convertido en una herramienta de gran utilidad para todos los sectores en los que se desenvuelve esta nueva sociedad tecnológica; y debido a las nuevas aplicaciones que se desarrollan en internet, le dan mayor importancia a su uso. Además, una de estas aplicaciones permite que los usuarios puedan tener un uso cada vez más personal de Internet, y se encuentren con la necesidad de no solo adquirir información desde el ciberespacio, sino también el poder almacenar gran cantidad de datos en él. Esta necesidad creciente entre los usuarios de Internet, obligó a la estructuración de lo que hoy se conoce como *“computación en nube”.* Esto también generó interés entre los expertos en Gobernanza de Internet, y conscientes de la necesidad de contar con una adecuada gestión que garantice el uso de esta nueva infraestructura, decidieron incluir en la quinta reunión del FGI del 2010 (2010, WSIS-2010/1)[10], al

nuevo concepto de *"Computación en la nube"* como un tema emergente de importante interés a ser debatido.

Este primer debate hizo posible obtener un panorama mucho más amplio de este nuevo concepto en cuestiones de normativa y técnica. Al principio, fue necesario hacer una exploración inicial de las nuevas políticas públicas y reglamentaciones que permitan garantizar la privacidad, integridad y confianza de los usuarios de la computación en nube. Luego de esto, se analizó la infraestructura, equipos y entornos en los que se desarrolla la computación en nube.

En el informe del FGI (2010, WSIS-2010/1)[10], se menciona que El Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST por sus siglas en Inglés) definió la computación en nube como:

> *"un modelo que permite acceder en Internet, cómodamente y según las necesidades individuales, a una serie de distintos recursos informáticos configurables (por ej., redes, servidores, almacenamiento, aplicaciones y servicios), suministrados de forma rápida y listos para ser utilizados con un mínimo de gestión por parte el usuario o de interacción con el proveedor de los servicios".*

El desarrollo de toda nueva aplicación trae consigo tanto ventajas como desventajas, lo cual genera diversos criterios entre los usuarios. Para los interesados en la Gobernanza de Internet, la principal ventaja que la computación en nube brinda a los usuarios es *"la posibilidad de pagar solamente por los recursos informáticos que usan en lugar de tener que mantener ellos mismos todos los recursos e insumos informáticos que necesitan"* (2010, WSIS-2010/1)[10], y la facilidad de tener disponible el acceso a sus datos cuando los requiera y desde cualquier parte del

mundo en que se encuentren; esto sin duda alguna, evita gastos de software y hardware que a veces son difíciles de financiar por los usuarios. Sin embargo, para algunos de los participantes del foro, una desventaja en el uso de la computación en nube es la dependencia de los usuarios con el proveedor del servicio; donde si por alguna razón el servicio falla, los usuarios simplemente no pueden hacer nada para solucionarlo, y estarían expuestos a perder la información almacenada.

Los Interesados en la gestión de internet pretenden establecer reglamentaciones tanto a nivel nacional como internacional que garanticen *"la seguridad y la privacidad de los datos almacenados en dicha nube"* (2010, WSIS-2010/1)[10]. Para los expertos en la Gobernanza de Internet, la seguridad suele expresarse recurriendo a la confianza del usuario; pero este *"modelo de computación en nube se vuelve difícil saber en quién se está depositando la confianza y de acuerdo a qué reglas se opera".*

El debate sobre computación en nube provocó todo tipo de dudas; una de las preocupaciones es que *"la mayor parte de los usuarios no tiene idea de las condiciones en que se almacenan y acceden sus datos".* Los expertos afirmaron que a menudo los usuarios desconocen que sus datos personales ya no se encuentran en su país y que pueden estar disponibles para otros usos y ser vendidos legalmente con fines comerciales. Otra de las inquietudes que se presentó entre los participantes del debate, es que si *"los datos que se encuentran en las plataformas de computación en nube corren riesgos"* y si estos riesgos pueden seguir aumentando con *"la computación en nube transnacional"*; tal y como mencionó uno de los participantes *"con la computación en nube, la información privada de una persona está en el disco rígido de otra y, así, la protección de la privacidad depende de la*

jurisdicción en la que se encuentran esos discos". Por este motivo, es importante debatir las responsabilidades que tienen los distintos agentes que participan en la computación en nube. (2010, WSIS-2010/1)[10].

Finalmente, aunque para algunos de los participantes la computación en nube es *"volver a los antiguos sistemas centralizados de uso en red y que es un híbrido de tecnologías nuevas y antiguas con algunos avances que hacen más eficaces y prácticas las viejas técnicas"* (2010, WSIS-2010/1)[10], resulta ser la nueva forma de almacenamiento de recursos privados y acceso a información personal en Internet, que cada día interesa a más personas. Por ello, es importante que la computación en nube continúe siendo analizada y debatida por los interesados en la Gobernanza de internet para tener una nube sólida, con una gestión apropiada; donde sean los usuarios los principales beneficiados.

CAPÍTULO 3:

PROBLEMÁTICA MUNDIAL.

3.1. Libertad de Expresión e Internet.

Respecto a la libertad de expresión en línea, es oportuno mencionar que el 1 de junio del 2011 se adoptó *"La Declaración Conjunta sobre libertad de expresión e Internet"* (2011)[11]. El relator especial de la Organización de las Naciones Unidas (ONU) junto a los representantes de las organizaciones encargadas de velar por los Derechos Humanos y Libertad de Expresión de todas las regiones del mundo, conscientes del crecimiento y desarrollo que ha alcanzado y sigue alcanzando Internet alrededor de todo el mundo, se reunieron para sentar un precedente que garantice la Libertad de expresión en Internet.

Previamente, los representantes analizaron la importancia fundamental que tiene la libertad de expresión como *“herramienta esencial para la defensa de todos los demás derechos”*, y como elemento fundamental de la democracia. Así también, destacaron el carácter transformador de Internet, siendo hoy en día el medio principal que permite a *“miles de millones de personas en todo el mundo expresar sus opiniones”.* Y aunque celebraron el notable crecimiento del acceso a Internet en casi todos los países y regiones del mundo, enfatizaron que existen también miles de millones de personas que aún no tienen acceso a Internet.

Para la redacción del documento de la Declaración Conjunta sobre Libertad de Expresión e Internet se consideraron *“los mecanismos del enfoque multisectorial del Foro para la Gobernanza de Internet”,* debido a los múltiples actores que participan en la gestión de Internet. Estos actores deben ser los encargados de fomentar medidas educativas como la *"alfabetización digital”,* para concientizar a todas las personas en el uso autónomo, independiente y responsable de Internet.

La Declaración Conjunta sobre Libertad de Expresión e Internet manifiesta que *“la libertad de expresión se aplica a Internet del mismo modo que a todos los medios de comunicación”.* Por este motivo, se debe diseñar la reglamentación específicamente para este medio, atendiendo a sus particularidades, y no utilizando reglamentaciones que ya han sido desarrolladas para otros medios de comunicación.

Los representantes de las organizaciones responsables de garantizar el cumplimiento de los Derechos Humanos y la Libertad de Expresión enfatizaron que las medidas que restringen la libertad de expresión en Internet como:

> *"el bloqueo obligatorio de sitios web enteros, direcciones IP, puertos, protocolos de red o redes sociales constituye una medida extrema que solo podría estar justificada conforme a estándares internacionales, por ejemplo, para proteger a menores del abuso sexual".*

En la Declaración Conjunta sobre Libertad de Expresión e Internet se advierte que:

> *"la interrupción del acceso a Internet, o a parte de este, aplicada a poblaciones enteras o a determinados segmentos del público (cancelación de Internet) no puede estar justificada en ningún caso, ni siquiera por razones de orden público o seguridad nacional. Lo mismo se aplica a las medidas de reducción de la velocidad de navegación de Internet o de partes de este";*

Mientras enfatiza que:

> *"la negación del derecho de acceso a Internet, a modo de sanción, constituye una medida extrema que solo podría estar justificada cuando no existan otras medidas menos restrictivas y siempre que haya sido ordenada por la justicia, teniendo en cuenta su impacto para el ejercicio de los derechos humanos".*

De acuerdo a lo señalado, los representantes denunciaron que algunos gobiernos han actuado en contravención a este derecho internacional, al restringir indebidamente la libertad de expresión en Internet.

Con respecto a la neutralidad de la red, en el documento antes mencionado se enfatiza que:

> *"el tratamiento de los datos y el tráfico de Internet no debe ser objeto de ningún tipo de discriminación en función de factores como dispositivos, contenido, autor, origen y/o destino del material, servicio o aplicación".*

Exigiendo a los intermediarios de Internet que *"sean transparentes respecto de las prácticas que emplean para la gestión del tráfico o la información",* las cuales deben estar a disposición del público con libre acceso. Sin embargo, se exhorta a Los Estados a que no deben exigir a los intermediarios de Internet, el control de los contenidos generados por los usuarios, liberándolos de responsabilidad por dichos contenidos que son difundidos a través de los servicios que éstos ofrecen.

Finalmente, la Declaración Conjunta sobre Libertad de Expresión e Internet recomienda a Los Estados a cumplir con *"la obligación positiva de promover y facilitar el acceso universal a Internet para garantizar el disfrute efectivo del derecho a la libertad de expresión"*. Para ampliar el acceso a Internet, Los Estados deben adoptar *"planes de acción detallados de varios años de duración"*, con medidas especiales que aseguren el *"acceso equitativo para personas con discapacidad y los sectores menos favorecidos";* priorizando la generación de conciencia sobre el uso adecuado de Internet y los beneficios que brinda especialmente entre *"sectores pobres, niños y ancianos, y en las poblaciones rurales aisladas".*

3.2. Espionaje Cibernético.

Los problemas de espionaje cibernético a través de Internet siempre han sido temas de debate en todo el mundo; involucrando Gobiernos, empresas de ciberseguridad, agencias gubernamentales y entidades

internacionales. Ellos están siempre atentos a identificar posibles ataques de espionaje cibernético que afecten sus redes e información valiosa.

Estos ataques a la ciberseguridad generalmente son atribuidos a gobiernos como el de Rusia, Israel, Estados Unidos y China. Estos gobiernos son potencias militarles del mundo, y sus ejércitos siempre están pendientes de las acciones que realizan los otros gobiernos como estrategia para enfrentar posibles guerras y ataques a sus respectivas naciones. En los últimos años, los espionajes y ataques a la ciberseguridad han generado una "Guerra Cibernética" entre los gobiernos mencionados, y podrían crecer de forma considerable si se continúa considerándolos como problemas político.

Reporteros sin Fronteras, organización activa que protege la libertad de expresión en el mundo, viendo la necesidad de vigilar e informar los acontecimientos que pudiera poner en peligro el derecho a la libre expresión en Internet, en el año 2013 realizó un informe, llamándolo *"Enemigos de Internet"* (Reporteros sin Fronteras, 2013) [12]. Este informe se hizo público el día 12 de marzo, considerado como *"el Día Mundial Contra la Censura en Internet"*.

En este informe se revela la primera lista de *"cinco Estados enemigos de Internet"*; los cuales son: "*Siria, China, Irán, Bahréin y Vietnam".* Además se incluye una lista de *"cinco empresas enemigas de Internet",* también llamadas *"mercenarias de la era digital"*; las cuales son: *"Gamma, Trovicor, Hacking Team, Amesys y Blue Coat"; e*stas empresas son consideradas de esa manera debido a que sus *"productos son utilizados por las autoridades de diversos países para cometer violaciones de derechos humanos y de la libertad de información".*

Reporteros sin Fronteras denuncia a través del informe en mención, la grave violación a la libertad de información y los derechos humanos. Describe los peligros a los que se enfrentan los periodistas, blogueros, defensores de los derechos humanos y ciudadanos comunes, debido a la vigilancia en Internet por parte de estados que practican una vigilancia activa e intrusiva en la red. Dichas vigilancias son destinadas a controlar las voces disidentes y la difusión de informaciones sensibles que pudieran desestabilizar sus gobiernos.

La República Popular China, se ha convertido en la nación con mayor controversia en temas de ciberseguridad a lo largo de los últimos años. Se considera que su gobierno es el principal involucrado en espionajes cibernéticos y uno de los mayores represores de la libertad de expresión en todo el mundo.

En el año 2009, el Gobierno Chino fue acusado de actividades de espionaje cibernético y ataques contra redes informáticas de otras naciones. La acusación fue realizada por un grupo de investigadores canadienses del centro “Munk” para Estudios Internacionales de la Universidad de Toronto que descubrió una red de espionaje cibernético china especializada en el control de los sistemas informáticos del líder religioso Dalai Lama, así como de exiliados tibetanos en todo el mundo. (Descubierta una red, 2009)[13].

Los investigadores canadienses descubrieron esta red, a la que bautizaron como *“GhostNet”,* mientras inspeccionaban el ordenador de Dalai Lama para encontrar posibles virus informáticos, por encargo del propio líder tibetano. Los investigadores afirmaron también que en menos de dos años aproximadamente 1.295 ordenadores fueron atacados; y se sustrajeron miles de documentos de ordenadores de los Ministerios de Relaciones Exteriores de 103 países. Sin embargo, El

Gobierno Chino negó las acusaciones y denunció que también es víctima de numerosos ataques procedentes de los Estados Unidos (Descubierta una red, 2009)[13].

En el 2013, el informe "*APT-1: Exposición de una de las unidades de CiberEspionaje de China"*, realizado por la empresa de seguridad digital de los Estados Unidos, "Mandiant"; denuncia que el Ejército de Liberación Popular Chino está detrás de los múltiples ataques que se han venido realizando en todo el mundo durante muchos años. (Mandiant, 2013)[14].

El informe revela que los ataques en su mayoría fueron realizados desde el edificio sede de las operaciones de la unidad 61398 del Ejército de Liberación Popular chino, situado en las afueras de Shanghai. Y que son al menos 141 entidades y organizaciones de todo el mundo, en su mayoría estadounidenses, las que sufrieron ataques de este grupo de piratas informáticos identificado como APT-1 (Por sus siglas en inglés es *Advanced Persistent Threat).* El Grupo APT-1 tiene por objetivo robar información industrial y de defensa. Los ataques son variados y se centran en campos considerados fundamentales para los planes económicos, militares y tecnológicos del Gobierno Chino (Mandiant, 2013)[14].

El informe proporciona una gran variedad de evidencias que aseguran que el APT-1 ha robado centenares de TeraBytes de información principalmente a industrias de habla inglesa claves para la economía. Además, demuestra que este grupo tiene la capacidad de atacar simultáneamente a docenas de organizaciones; y una vez que el grupo establece acceso con la entidad perjudicada, periódicamente la visitan y así por un largo tiempo, de manera que analizan la información que contiene y seleccionan aquella que es de utilidad (Mandiant, 2013)[14].

Según Mandiant, el APT-1 posee una extensa infraestructura de sistemas informáticos a lo largo del mundo, aunque más del 97 % de sus ataques fueron realizados usando direcciones IP pertenecientes a las redes de Shaghai. Debido al tamaño de la infraestructura de ataque, se especula que este grupo emplea a cientos de personas encargadas en diversas tareas de ciberespionaje, donde se incluyen lingüistas, desarrolladores de software, creadores de malware, expertos analistas de industrias y economistas; todos ellos orientados a penetrar empresas, hurtar información, interpretarla y distribuirla a los interesados y especialmente al Gobierno Chino (Mandiant, 2013) [14].

Finalmente, como podemos analizar, la vigilancia a las actividades que realizan los usuarios de Internet, resulta ser uno de los mayores objetivos de Gobiernos que pretenden tener el control de la Red de Internet. Aunque la tecnología permita ser utilizada como herramienta para la censura y vigilancia, es importante que los usuarios e incluso periodistas, aprendan a *"calcular mejor los riesgos potenciales de la vigilancia y el tipo de datos o de comunicaciones que hay que proteger, a fin de encontrar la solución adaptada al uso que hacen de Internet".* (Reporteros sin Fronteras, 2013)[12].

3.3. Primavera Árabe.

La Primavera Árabe se convirtió en el suceso de revolución y protestas más importante de la región árabe en los últimos años. Esto generó controversias y análisis alrededor del mundo, no solo por las realidades políticas, económicas y sociológicas muy diferentes que se viven en esta región del mundo, sino también de los efectos que provocaron las

redes sociales como medios de protestas y revolución para una posible democratización de los gobiernos dictatoriales árabes.

Una nueva generación tecnológica ha invadido a todas las regiones del mundo, y los gobiernos árabes vivieron la más grande movilización de personas sobre la web como protesta ante sus regímenes; siendo el año 2010, cuando las redes sociales se consagran como instrumento de movilización y de difusión de información en esta región y el mundo.

Según los Reporteros sin Fronteras, las redes sociales como Facebook y Twitter y sitios de "streaming" *(transmisión en vivo de audio y video)* se convirtieron en medios de difusión de todas las frustraciones y reivindicaciones de los manifestantes árabes. Esto permitió que resto del mundo siguiera en directo los acontecimientos, pese a la censura de los medios de comunicación tradicionales. Los revolucionarios árabes se vieron en la necesidad de inundar estas redes sociales con información, imágenes y videos con el fin de buscar *"la cobertura de los medios de comunicación extranjeros a fin de presionar a sus gobiernos y a la comunidad internacional"* ("Primavera árabe: ¿apogeo de la Web?", 2011) [15].

Los términos *"revolución Twitter"* y *"revolución Facebook"* se pusieron de moda en todo el mundo debido a los acontecimientos antidemocráticos y dictatoriales que marcaron el mundo árabe del 17 de diciembre de 2010 hasta mediados de noviembre de 2011.

Las revoluciones tunecina y egipcia demostraron ser, ante todo, revoluciones humanas, impulsadas por Internet y las redes sociales. Los movimientos generados sobre Internet se combinaron con las manifestaciones en las calles, precipitando la caída de los dictadores. Las manifestaciones en la Web se propagaron en otros países: Libia,

Yemen, Bahréin, Omán, Siria, Irak, Marruecos, incluso en China y Vietnam, entre otros. Y aunque Internet fue ampliamente invadido por los revolucionarios árabes, las autoridades de estos regímenes dictatoriales, lo utilizaron como medio para *"difundir la propaganda oficial y reforzar la vigilancia y el control de la población"* ("Primavera árabe: ¿apogeo de la Web?", 2011) [15].

El potencial de difusión de información que tiene Internet y los ineficaces métodos tradicionales de censura provocó una gran irritación en los dictadores. Por este motivo, algunos regímenes se dotaron de recursos para *"vigilar a los disidentes, especialmente vía Facebook y Twitter, e infiltrarse en sus redes"* ("Primavera árabe: ¿apogeo de la Web?", 2011) [15].

Un año después del inicio de las sublevaciones prodemocráticas en el mundo árabe, Reporteros sin Fronteras realizó un balance de la censura y de las violaciones a la libertad de informar que se produjo durante el período de revolución árabe. En el informe *"Rebeliones árabes: los medios de comunicación, testigos clave de las revoluciones y de los retos del poder"* (Reporteros sin Fronteras, 2011) [16], se describen *"los métodos empleados por las autoridades para impedir la circulación de la información durante las seis rebeliones populares"* suscitadas en Túnez, Egipto, Libia, Bahréin, Siria y Yemen.

Para el 2010, los regímenes autoritarios de los países árabes influían en la velocidad de conexión a Internet en sus respectivos países. *"El ancho de banda en periodos de elecciones o de manifestaciones se volvía más lento".* La velocidad de conexión a Internet se convirtió en *"el barómetro de la situación política y social"* de estos países ("Aumenta la potencia de Control 2.0", 2011) [17].

Irán se volvió un maestro en la materia, los regímenes derrocados de los dictadores Ben Ali y Mubarak utilizaron ese procedimiento la víspera y el día de cada manifestación organizada por la oposición. En Bielorrusia durante las manifestaciones contra la reelección del presidente Lukashenko, se re-direccionaron los sitios de la oposición o de los críticos del gobiernos, hacia sitios parecidos, pero cuyo contenido coincida más con la visión de las autoridades (“Aumenta la potencia de Control 2.0”, 2011) [17].

Durante la semana que precedió a las elecciones parlamentarias, Egipto vivió un nuevo episodio revolucionario. Hubo violentos enfrentamientos entre las fuerzas del orden y los manifestantes que pedían el cese del poder de los militares (Reporteros sin Fronteras, 2011)[16].

Además, desde la noche del 27 de enero de 2011, durante cinco días, el acceso a Internet en Egipto fue suspendido casi por completo. En cuanto a Libia, el 19 de febrero de 2011, las autoridades cortaron el acceso a Internet y los días que siguieron se registraron fuertes perturbaciones en la conexión (“Aumenta la potencia de Control 2.0”, 2011) [17].

Finalmente, la primavera árabe demostró al mundo que las revoluciones no solo se dan en las calles, sino también se las hace sobre la Web, y con el carácter instantáneo de las redes sociales se puede tener una cobertura en tiempo real de acontecimientos importantes que se suscitan alrededor del mundo. Internet ha demostrado ser una herramienta primordial para los periodistas debido a que se ha convertido en un medio complementario para los demás medios de comunicación tradicionales.

3.4. Propiedad Intelectual: Ley PIPA, Ley SOPA.

La Organización Mundial de la Propiedad Intelectual define a la *Propiedad Intelectual* como "*las creaciones de la mente: invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizadas en el comercio*" (2009, OMPI-450/S) [18].

La propiedad intelectual se divide en dos categorías: la propiedad industrial, que incluye las patentes de invenciones, las marcas, los diseños industriales y las indicaciones geográficas; y el derecho de autor que incluye obras literarias, como novelas, poemas y obras de teatro, películas, obras musicales, obras artísticas, tales como dibujos, pinturas, fotografías y esculturas, y diseños arquitectónicos.

Los derechos de propiedad intelectual se asemejan a cualquier otro derecho de propiedad, los cuales permiten al creador o al titular de una patente, marca o derecho de autor, beneficiarse de su obra o inversión (2009, OMPI-450/S)[18].

Los proyectos de ley *Stop Online Piracy Act (SOPA*), presentada por la Cámara de Representantes de los Estados Unidos, y *Protect Intelectual Property Act (PIPA),* presentada por el Senado americano, tenían por finalidad generar un mayor número de herramientas de protección en materia de propiedad intelectual, específicamente regular las descargas ilegales de archivos realizados a través de Internet, en otras palabras terminar con la piratería. Cabe recalcar que estas leyes, PIPA y SOPA, son análogas, sino que pertenecen a las diferentes cámaras americanas (Pereda, 2012) [19].

Para el Magíster en Derecho Informático y de Telecomunicaciones y actual Subsecretario de Telecomunicaciones de Chile, Pedro Huichalaf:

> *"estos proyectos de ley podían generar repercusiones graves para la actual estructura de Internet, pues faculta principalmente al Departamento de Justicia y a los titulares o cesionarios de derechos intelectuales, obtener órdenes judiciales contra aquellos sitios webs o servicios que, entre otras, permitan o faciliten una supuesta vulneración o violación de los derechos de autor"* (Huichalaf, 2012, p. 1) [20].

Entre las medidas facultadas se encontraban:

- *"Órdenes para el bloqueo por parte de los proveedores de Internet (mayoritariamente norteamericanas) al sitio web o servicio denunciado, incluyendo el hosting e inclusive a nivel DNS.*
- *Empresas facilitadoras de cobro de Internet como PayPal, debían dejar de ofrecer sus servicios, congelar fondos y restringir el uso del mismo.*
- *Los servicios de publicidad en cuya participación existían empresas norteamericanas debían dejar de funcionar en el sitio web denunciado.*
- *Respecto a algunos generadores de contenidos o servicios de búsqueda como Google, se los ordenaba a eliminar los enlaces al sitio web o servicio denunciado, incluso si este enlace estuviese ubicado en servidores fuera del territorio jurisdiccional de EEUU"* (Huichalaf, 2012, p. 2)[20].
- *"Podía cerrar páginas alojadas en EEUU que permitan descargas de contenido protegido por derechos de autor,*

> *violando por tanto la propiedad intelectual, aunque sus dueños residan en el extranjero"* (Pereda, 2012, p.18)[19].

Esto implicaba que:

> *"la ley responsabilizaría a buscadores, portales y páginas que publiquen links a contenido protegido y otras webs de descargas. Mediante una orden judicial, cualquier productora de cine que descubra una página ofreciendo copias ilegales de sus películas, podía obligar a Google a eliminarla de los resultados de su buscador. Sitios como Facebook, YouTube o Flickr debían responder por el contenido que recomienden los usuarios en cuanto haya sospecha de que viola la propiedad intelectual. Los usuarios, por tanto, serían responsabilizados al compartir en páginas personales, redes sociales y correos electrónicos, links a webs que alojen copias ilegales, aunque no los hayan hecho ellos mismos ni se beneficien económicamente de su distribución"* (Pereda, 2012, p.18)[19].

El artículo periodístico "Wikipedia lidera apagón virtual" (2012, Enero 18) [21] argumentó que:

> *"el proyecto de ley goza de un amplio apoyo por parte del sector de entretenimiento, empresas farmacéuticas, y publicaciones, entre otros grupos que buscan combatir la piratería en Internet. Sin embargo, la Casa Blanca se opone a la medida en su versión actual por considerar que ésta podría suscitar demandas contra empresas cibernéticas y perjudicar a negocios legítimos, además de atropellar el derecho a la libertad de expresión".*

En protesta a la ley SOPA se unieron grandes empresas de Internet como Wikipedia, en su versión en inglés, Redditt, Google, entre otros. Wikipedia interrumpió su servicio por un día, mientras que Google publicó un “doodle” *(cambio decorativo en el logotipo de Google)* especial en el que su logo parecía censurado y con una petición en línea que fue firmada por más de 4.5 millones de firmas. Facebook y Twitter también mostraron desacuerdo con la norma. Mark Zuckerberg, fundador de Facebook, comentó en su perfil que Facebook se oponía a SOPA y PIPA, y continuarán en contra de cualquier ley que vaya a herir Internet. Como consecuencia a todos estos eventos, algunos senadores de las diferentes cámaras anunciaron oposición a PIPA y SOPA (“Internet cierra filas”, 2012) [22].

3.5. Open Access.

El Open Access de Unesco (2013) [23] indica que el derecho de autor está en el corazón del Acceso Abierto debido a que la accesibilidad depende enteramente del propietario de ese derecho. Si el propietario del derecho de autor está de acuerdo, el Acceso Abierto procede, caso contrario el Acceso Abierto no es posible para este trabajo. El más elemental enfoque para asegurar que un trabajo puede ser de Acceso Abierto sin ningún problema es retener el derecho para que así sea.

Los científicos que envían un artículo a una revista por lo general transfieren los derechos de autor, que en realidad es un paquete de derechos, al editor firmando un acuerdo de transferencia de derechos. Incluido en ese paquete está el derecho a publicar, que es lo que quiere el autor. Es posible para los científicos tener sus trabajos publicados sin firmar todos los derechos, permitiéndoles hacer lo que ellos quieran en

términos de diseminación a través de canales alternativos, así como en revistas en las cuales han escogido publicar; esto lo pueden lograr otorgando a los editores una licencia para publicar, mientras que los autores retienen el resto de paquetes de derechos (UNESCO, 2013) [23].

Se están realizando diferentes negociaciones por parte de los autores con la finalidad de retener los derechos, una de éstas es mediante los apéndices de autor que son piezas específicas de la redacción legal que los autores pueden añadir al acuerdo de transferencia de derechos del editor, estableciendo los derechos que el autor retendrá después de pasar un artículo al editor para su publicación (UNESCO, 2013)[23].

Asimismo, algunas universidades como la Berkeley, apoya a la facultad de retener los derechos de propiedad intelectual usando editoriales que mantienen una práctica razonable de negocios. El Instituto Tecnológico de Massachussets desarrolló un apéndice de tutores para sus investigadores, así como un consorcio de doce universidades crearon un apéndice del Comité para Cooperación Institucional. Esto demuestra que las universidades han estado buscando proteger futuras salidas de investigación de caer bajo la propiedad del editor (UNESCO, 2013)[23].

Para el caso de establecimientos de investigación gubernamentales, los derechos sobre los resultados producidos por los empleados usualmente los tiene el empleador. Este acuerdo predomina sobre cualquier negociación con el editor y lo invalida. Algunas universidades han usado esta fórmula, como la Universidad de Harvard, que después de una votación unánime de una serie de encuentros entre facultades, le dieron a la universidad el derecho irrevocable, no exclusivo, de distribuir sus artículos académicos con fines no comerciales (UNESCO, 2013)[23].

Es necesario hablar sobre la importancia de una licencia, ya que éstas establecen las condiciones para el rehúso y tranquilizan a potenciales usuarios para que puedan utilizar con impunidad un material en particular. Esto es relevante tanto para los individuos que están buscando entender cómo utilizar los materiales, así como para los que se enfocan en la extracción de textos y de datos en la creación de conocimientos. En otras palabras, las licencias de trabajo científico dejan claro al usuario qué puede hacerse con un trabajo dado y a la vez estimular su uso.

La iniciativa de Acceso Abierto de Budapest, la Declaración de Berlín y la Declaración de Bethesda expusieron como condiciones para el Acceso Abierto:

- *"Que la literatura revisada por pares sea accesible sin suscripción o barreras de precios.*
- *Que la literatura sea accesible inmediatamente.*
- *Que los materiales publicados puedan ser reusados de diversos modos sin requerir un permiso"* (UNESCO, 2013)[23].

La iniciativa de Budapest establece que:

> "*la única limitación sobre la reproducción y distribución, y el único papel del derecho de autor en este dominio, deberá ser dar a los autores el control sobre la integridad de su trabajo y el derecho a ser propiamente reconocido y citado. Esto significa que artículos y libros con Acceso Abierto, incluyendo datos, gráficos y suplementos, pueden ser conectados, arrastrados por mecanismos de búsqueda, cortados e insertados dentro de otros artículos, blogs y todo esto sin costo alguno. La única condición es la acreditación correcta de la fuente, el editor*

también puede ser parte de esta acreditación" (UNESCO, 2013)[23].

Existe un conjunto de licencias creadas por la organización "Creative Commons". Algunos editores de Acceso Abierto usan estas licencias para asegurar que el contenido de los artículos publicados en sus revistas sean reutilizables en un sentido amplio (Acceso Abierto libre); es decir que pueden ser reproducidos, resumidos, fundidos con otros materiales para generar información, y así sucesivamente. Las licencias Creative Commons son la mejor práctica de licenciamiento porque:

- *"Existe casi con certeza una licencia modelo que se adaptará a los requerimientos de la editorial, lo que ahorrará tiempos y esfuerzos en redactar una licencia.*
- *Estas licencias son fácilmente entendidas y muy usadas, de modo que un lector potencial o usuario de un trabajo entenderá inmediatamente las condiciones de la licencia.*

  Las licencias tienen metadatos de lectura por máquina, que simplifica los procesos en aplicaciones tales como herramientas de recolección y extracción de textos que llevan a cabo tareas automatizadas; esas herramientas pueden reconocer, mediante la licencia leíble por la máquina, qué contenidos están permitidos para reunirlos y trabajar sobre ellos" (UNESCO, 2013)[23].

3.6. La Agenda Global de la Ciberseguridad de la UIT.

De acuerdo a la Resolución No. 181 de la Conferencia de Plenipotenciarios de Guadalajara (20) [24], se adoptó como definición de ciberseguridad al:

> *"conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:*
>
> - *disponibilidad;*
> - *integridad, que puede incluir la autenticidad y el no repudio;*
> - *confidencialidad".*

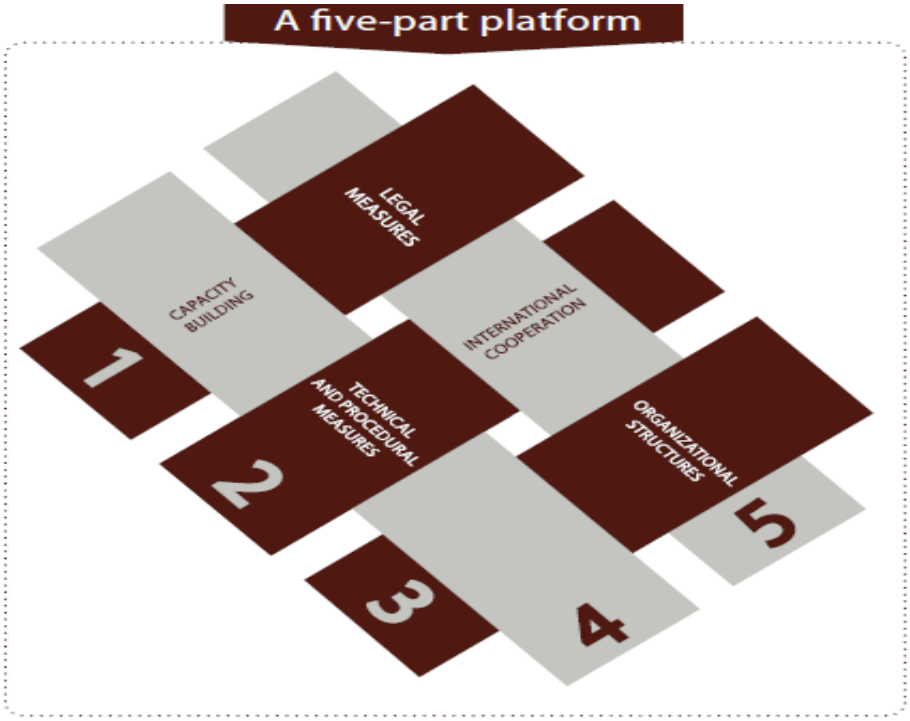
La Secretaría General de la UIT plantea una Sociedad de la Información Global en la cual la confianza y la seguridad en el uso de las tecnologías de la información y el conocimiento son las normas para el beneficio de la humanidad. Por esta razón, el 17 de mayo del 2007, la

UIT presentó la Agenda Global de la Ciberseguridad (AGC, 2007) [25] para proveer *"una estructura en donde una respuesta internacional a los retos cada vez mayores de ciberseguridad puedan ser coordinados y direccionados".*

La Agenda se basa en la cooperación internacional y los esfuerzos para comprometer a todas las partes interesadas, para construir confianza y seguridad en la sociedad de la información. Está construida sobre cinco pilares estratégicos, también conocidos como áreas de trabajo.

Los cinco pilares de la Agenda, mostrados en la Figura 3.1, son:

1. Medidas Legales
2. Medidas Técnicas y de Procedimiento
3. Estructuras Organizacionales
4. Fortalecimiento de Capacidad
5. Cooperación Internacional



Fuente: Agenda Global de la Ciberseguridad – AGC [25].

Figura 3.1: Cinco pilares de la Agenda Global de la Ciberseguridad.

Como parte del primer pilar, la UIT se encuentra trabajando para asistir a los países en el entendimiento de aspectos legales de la ciberseguridad mediante su Legislación de Recursos del Cibercrimen con la finalidad de avanzar en la armonización de los diferentes marcos legales. Además, a través de esta legislación, la UIT direcciona su primer objetivo estratégico que llama a la elaboración de estrategias para el desarrollo de una legislación contra el cibercrimen, la cual es aplicable globalmente y opera conjuntamente con medidas legislativas nacionales y regionales.

La Legislación de Recursos del Cibercrimen mencionada en la Agenda, consta actualmente de dos tareas principales, en las publicaciones de la UIT tituladas *"Herramientas para la Legislación del Cibercrimen"* y

"*Entendiendo el Cibercrimen: Una guía para países en vías de desarrollo".* La última mencionada, tiene como objetivo ayudar a países en vías de desarrollo a tener un mejor entendimiento sobre las implicaciones nacionales e internacionales que conllevan el creciente número de ciberamenazas, a evaluar los requisitos de instrumentos nacionales e internacionales existentes, y asistir a países en el establecimiento de una base jurídica sólida. La guía provee una visión sobre los temas más relevantes relacionados con los aspectos legales del cibercrimen.

Por otra parte, las Herramientas para la Legislación están diseñadas para avanzar en la armonización mundial de las leyes contra el cibercrimen, sirviendo como un recurso central de ayuda para legisladores, abogados, oficiales gubernamentales, políticos y representantes de la industria a nivel mundial, para de esta manera construir un marco legal consistente que los proteja del mal uso de las TICs.

En el segundo pilar de la Agenda, se reconoce "*el potencial de las TICs y la continua exposición que éstas tienen a malos usuarios, convirtiéndolo en un fenómeno relacionado al crimen organizado en la red"*. Los malos usuarios buscan deliberadamente vulnerabilidades en aplicaciones de software, para crear malware que permitan el acceso no autorizado y la realización de modificaciones de estas aplicaciones; comprometiendo así, la integridad, autenticidad, confidencialidad de las redes y sistemas de información y comunicación. Con el incremento en sofisticación de malware, estas amenazas no pueden ser sobreestimadas y podrían existir graves consecuencias en caso de que infraestructuras de información crítica se vean afectadas.

La Agenda menciona como parte de las medidas técnicas y de procedimiento al Sector de Estandarización de la UIT (UIT-T), el cual mantiene una posición única en el campo de estandarización. Tiene como trabajo coordinar la armonización de las políticas y estándares de seguridad a nivel internacional. La UIT ha desarrollado directrices de seguridad para autores de protocolos, especificaciones de seguridad para sistemas basados en IP, guías en cómo identificar ciberamenazas y medidas para mitigar los riesgos que conllevan las amenazas. El UIT-T Grupo de Estudio 17 es el grupo líder en seguridad de telecomunicaciones, es responsable de estudios sobre ciberseguridad y la forma para contrarrestar “spam” *(mensajes no solicitados)*.

En el tercer pilar de la Agenda, se destaca la dependencia en redes interconectadas por parte de organizaciones, gobiernos e individuos. Con el fin de proteger la infraestructura de las redes y reconocer las amenazas es necesario acción nacional para prevenir, responder y recuperarse de los diferentes incidentes. Se requiere colaboración gubernamental, del sector privado, instituciones educativas y organizaciones regionales e internacionales para concienciar sobre posibles ataques informáticos y tomar medidas para solucionarlos. En fin, esta área de trabajo involucra un marco genérico y estrategias de respuesta óptimas para la prevención, detección y manejo de ciberataques, incluyendo la protección de los sistemas de infraestructuras de información de los países.

Para la cuarta área de trabajo o pilar, se reconoció en la Agenda que “*el fortalecimiento de capacidad necesita ser promovido para desarrollar una cultura sobre ciberseguridad sostenible y proactiva*”. Uno de los desafíos claves de la ciberseguridad está en el educar al usuario final, ya sea a nivel de escuela o de hogar. Además, la UIT para ayudar a sus

estados miembros en desarrollar capacidad para la ciberseguridad, facilita la implementación y el despliegue de las capacidades de ciberseguridad necesarias para combatir el cibercrimen.

La UIT Ciberseguridad Nacional/CIIP Herramienta de Autoevaluación es una iniciativa práctica para asistir a los estados miembros de la UIT que deseen diseñar un enfoque nacional para ciberseguridad y protección de infraestructura de información crítica (CIIP). También se menciona en la Agenda el *"UIT Herramientas para Promover una Cultura de Ciberseguridad"* que tiene como propósito proporcionar directrices en el conocimiento de temas de ciberseguridad para consumidores y usuarios finales en países en vías de desarrollo. Además, la UIT se encuentra trabajando en un grupo de Herramientas para la Mitigación de "Botnets" *(conjunto de robots informáticos),* para eliminar el impacto de botnets, grandes redes de ordenadores infectados con "malware" *(software malicioso),* poniendo énfasis en los problemas de las economías emergentes de Internet.

Al hablar de Cooperación Internacional, la Agenda hace un llamado a encontrar soluciones mundiales; para esto es necesario que se establezca cooperación internacional, no sólo a nivel gubernamental sino apoyo de la industria y diferentes organizaciones internacionales.

Como ayuda a esta área de trabajo, existe IMPACT (Alianza Internacional Multilateral contra las Ciberamenazas), "*una iniciativa internacional dedicada a mejorar la capacidad de la comunidad mundial para prevenir, defender y responder a las ciberamenazas*". De la misma manera está la iniciativa COP (Protección de Niños en Línea) que fue establecida como una red internacional para promover la protección de niños y jóvenes en línea proporcionando orientación sobre la seguridad en línea.

El Informe "*Cuestión 22/1*" de la Comisión de Estudio 1 del Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D, 2010) [26], ofrece a los estados un panorama general de los módulos esenciales necesarios para abordar el tema de la ciberseguridad en el plano nacional, así como para estructurar su enfoque en materia de ciberseguridad nacional. Los elementos clave del informe referido son los siguientes:

- *"Elaboración de una estrategia nacional de ciberseguridad.*
- *Establecimiento de relaciones de colaboración entre el Estado y el sector privado en el plano nacional.*
- *Disuasión del ciberdelito.*
- *Creación de capacidades nacionales para la gestión de incidentes.*
- *Promoción de una cultura nacional de ciberseguridad"* (UIT-D, 2010) [26].

La Comisión de Estudio 1 del Sector de Desarrollo de las Telecomunicaciones de la UIT sostiene que:

> *"el diseño y la implementación de un plan nacional de ciberseguridad hace necesario adoptar una estrategia global que entrañe un amplio análisis inicial de la adecuación de las prácticas nacionales de un país y la consideración de la función desempeñada por todas las partes interesadas (autoridades públicas, sector privado y ciudadanos) en este asunto. Por motivos de seguridad nacional y para preservar el bienestar económico, los gobiernos deben posibilitar, promover y*

> *garantizar la protección de sus infraestructuras de información esenciales. Actualmente, esas infraestructuras son comunes a varios sectores industriales y sobrepasan las fronteras nacionales".*

La Comisión de Estudio 1 de la UIT-D recomienda que el plan nacional debe tener como metas: incorporar en las políticas nacionales la cuestión de la ciberseguridad/protección de las infraestructuras de la información esenciales y reconocer la necesidad de tomar medidas en el plano nacional y de cooperar internacionalmente; preparar una estrategia nacional para proteger las infraestructuras de información esenciales y el ciberespacio contra ataques electrónicos y físicos; y participar en las acciones internacionales que se emprendan para coordinar las actividades nacionales relativas a la prevención, respuesta y recuperación ante incidentes y a la preparación contra los mismos.

Como al Estado y al sector privado les interesa garantizar de manera constante la resistencia de la infraestructura, resulta crucial que exista la colaboración entre los ámbitos público-privado para fomentar la ciberseguridad, ya que ninguno de ellos puede proteger por sí solo toda la infraestructura. En un gran número de países es el sector privado quien posee o explota la infraestructura, por lo que se recomienda que el Estado y el sector privado, cada uno dentro de sus respectivas esferas de competencia, colaboren en grado apreciable (UIT-D, 2010)[26].

Es posible mejorar en gran medida la ciberseguridad, entre otras formas, estableciendo y modernizando los elementos de apoyo, el derecho, los procedimientos y las políticas penales para impedir, desalentar y perseguir el ciberdelito, así como responder al mismo. Todos los países necesitan leyes que se opongan al ciberdelito,

además de los procedimientos necesarios para realizar investigaciones por vía electrónica y la asistencia de otros países. Estas leyes pueden quedar incorporadas en uno o varios códigos nacionales; por lo tanto, es necesario que los países examinen su código penal vigente, a fin de determinar si éste procede para afrontar los problemas actuales y futuros (UIT-D, 2010) [26].

Es importante que el Estado cree o identifique una organización nacional que sirva de piedra angular para la seguridad del ciberespacio y la protección de las infraestructuras de la información esencial, y cuya misión principal abarque esfuerzos de vigilancia, advertencia, respuesta y recuperación y la facilitación de la colaboración entre las entidades gubernamentales a nivel nacional, estatal y local, las entidades pertinentes del sector privado, el sector académico y la comunidad internacional (UIT-D, 2010) [26].

La Comisión de Estudio 1 del Sector de Desarrollo de las Telecomunicaciones de la UIT sostiene que:

> *"considerando que los computadores personales son cada día más potentes, que las tecnologías convergen, que cada vez se utilizan más las TIC y que cada día son más las conexiones transfronterizas, quienes creen o posean servicios, los suministren o los gestionen y utilicen redes de información deben comprender los problemas de la ciberseguridad y tomar las medidas que correspondan a sus funciones para proteger las redes. Los gobiernos deben desempeñar un papel primordial en la creación de esta cultura de ciberseguridad y en el apoyo de los esfuerzos de los demás actores."*

La promoción de una cultura nacional de ciberseguridad tiene que ver no solamente con el papel que desempeña el Estado a la hora de garantizar el funcionamiento y la utilización de las infraestructuras de información; sino también proporcionar información sobre el particular al sector privado, la sociedad civil y los particulares (UIT-D, 2010) [26].

Los países deberían adoptar, mediante actividades colaborativas y a través de algún tipo de acuerdo, una óptica multidisciplinaria y multipartita para implementar la ciberseguridad. La sensibilización y las iniciativas de educación, así como la cooperación internacional, el intercambio de prácticas óptimas y la utilización de normas internacionales, se consideran aspectos de gran relevancia para fomentar una cultura de seguridad (UIT-D, 2010) [26].

Teniendo presente las recomendaciones de la AGC y del Informe de la Comisión de Estudio 1, cabe recalcar que debido a las diferentes capacidades nacionales y a la evolución de las amenazas planteadas, estos documentos no proporcionan una receta prescriptiva para proteger la seguridad del ciberespacio; en lugar de ello, se ha preferido describir un enfoque flexible aplicable para ayudar a las administraciones nacionales a revisar y mejorar sus instituciones, políticas y relaciones sobre ciberseguridad.

CAPÍTULO 4:

CASOS DE ESTUDIO.

4.1. España.

Al analizar el modelo de Gobernanza de Internet en España, es destacable por parte de este país, que con el apoyo de representantes del sector empresarial, usuarios de las telecomunicaciones e Internet, la comunidad científica y el apoyo técnico de Fundación Telefónica, logró crear el Foro de la Gobernanza de Internet en España. Este Foro Nacional constituye una plataforma abierta y de debate sobre los principales problemas de actualidad que plantea Internet. El hecho de que exista una plataforma de estas características en España permite dar visibilidad a las iniciativas españolas y vincularlas con las diferentes iniciativas europeas y mundiales, así como dar voz a los actores y

agentes españoles en los foros internacionales en materia de Gobernanza (Pérez & Olmos, 2009) [27].

En el último Foro Nacional (2013) se constató la existencia del concepto y el fenómeno del ciberacoso como un nuevo tipo de conflicto que reúne características propias y diferenciadas del tradicional acoso al realizarse a través de medios tecnológicos y de Internet. Se solicitó la actualización de una normativa penal, civil y administrativa debido a la existencia de un vacío legal para la prevención y sanción de las conductas relacionadas con el ciberacoso. Además, se pidió la creación de una plataforma de coordinación que permita aglutinar los esfuerzos de todos los agentes implicados en la detección y prevención del ciberacoso priorizando la educación en los centros escolares como herramienta fundamental y básica (FGI España, 2013) [28].

Asimismo, se trató sobre el tema de contenidos digitales y propiedad intelectual. Se reconoció el apoyo a la industria cultural, a la existencia de leyes de propiedad intelectual que permita a los creadores ser recompensados por su trabajo y que existan incentivos para la creación cultural. Debido a la apertura de Internet y las oportunidades brindadas para todos los actores, sean éstos creadores de contenidos o usuarios, se apostó a mantener un entorno abierto a la innovación y un equilibrio entre dichos actores. Además, se acordó una necesaria reforma de la Ley de Propiedad Intelectual para el control de las entidades de gestión colectiva de derechos de propiedad intelectual (FGI España, 2013) [28].

Por otra parte, en febrero del 2013 el Gobierno Español aprobó la *Agenda Digital para España* (ADpE, 2013) [29] como marco de referencia para:

> *"establecer una hoja de ruta en materia de Tecnología de la Información y Comunicación y de administración electrónica; establecer la estrategia de España para alcanzar los objetivos de la Agenda Digital para Europa; maximizar el impacto de las políticas públicas en TIC para mejorar la productividad y la competitividad; y transformar y modernizar la economía y sociedad española mediante un uso eficaz e intensivo de las TIC por la ciudadanía, empresas y administraciones".*

Para el desarrollo óptimo de la Agenda se elaboraron un conjunto de planes específicos. En el proceso de elaboración de todos los planes, se partió de un análisis detallado de la situación actual y de los resultados de planes anteriores; se analizaron las debilidades, amenazas, fortalezas y oportunidades de la situación actual así como las consecuencias de las distintas alternativas de actuación que se presentaban. Entre los planes constan:

- Plan de confianza en el ámbito digital
- Plan de inclusión digital y empleabilidad.

La Agenda Digital para España (ADpE) incorporó como uno de sus objetivos principales el compromiso de desarrollar las medidas necesarias para contribuir a la construcción de un clima de confianza en el ámbito digital. Este compromiso se materializa a través del *Plan de Confianza Digital* (2013) [30] cuyo alcance se restringe exclusivamente al mercado digital interior, la ciudadanía, las empresas, la industria, los profesionales y con carácter prioritario las empresas de especial trascendencia económica. Las medidas que se proponen contribuyen a dar respuesta a los compromisos estratégicos de la ADpE, la Estrategia Europea de Ciberseguridad (EUCS) y la Estrategia de Seguridad Nacional (ESN), así como a los objetivos establecidos en el Plan,

reconociendo, complementando y reforzando las iniciativas que en materia de confianza digital se están realizando por distintos agentes públicos y privados en el ámbito del Plan en mención, favoreciendo la coordinación de todos los actores, impulsando la racionalización de los esfuerzos y la mejora de la eficacia y del impacto de las actuaciones. Las medidas se organizan en los siguientes ejes:

- Eje I: Experiencia digital segura
- Eje II: Oportunidad para la industria TIC
- Eje III: Nuevo contexto regulatorio
- Eje IV: Capacidades para la resiliencia: INTECO 2.0
- Eje V: Programa de excelencia en ciberseguridad

En el primer eje la ADpE, la EUCS y la ESN y las estrategias para la protección de la infancia y la adolescencia, consideran esencial la sensibilización y la concienciación de los usuarios para aumentar la confianza y el buen uso de Internet. En este ámbito, se han realizado numerosas actuaciones públicas y privadas en los últimos años, con el objetivo de incrementar la confianza en Internet, especialmente en aspectos relacionados con la seguridad de la información, la protección de la privacidad, el comercio electrónico seguro y el uso responsable y seguro de la tecnología por la infancia y la adolescencia, entre otros (2013) [30].

En el Eje II, la ADpE, la ESN y la EUCS establecen líneas de acción estratégica para el impulso de la industria de la ciberseguridad y de los servicios de confianza. Las tres estrategias apuestan por establecer mecanismos de impulso a la investigación, desarrollo e innovación, de estímulo a la demanda por medio de la adopción de normas y buenas prácticas, la apuesta por la normalización como valor diferencial, el estímulo de los esquemas de certificación y acreditación, y la apuesta

por la cooperación público-privada como herramienta para la mejora de los ciclos de innovación entre la industria y el mundo académico (2013) [30].

La adopción temprana de la nueva regulación europea combinada con el impulso de la autorregulación y la disponibilidad de un mapa de indicadores fiable sobre el nivel de confianza digital en España, se configuran como elementos claves para aumentar la confianza de ciudadanos y empresas en Internet, así como para mejorar los niveles de ciberseguridad en España (2013) [30].

La EUCS y la ESN plantean la necesidad de reforzar las capacidades de prevención, detección y respuesta frente a los ciberataques. La ADpE por otro lado, plantea como línea de actuación convertir a INTECO en un centro de referencia para la confianza digital, especialmente en materia de ciberseguridad (2013) [30].

En el último eje, la ESN establece como línea de acción estratégica la promoción de la capacitación de profesionales en ciberseguridad, al igual que la ADpE plantea la necesidad de crear talento en ciberseguridad. Los principales países del entorno español están llevando a cabo actuaciones innovadoras para la generación de talento en ciberseguridad; debido a esto se sugiere que España debe hacer un esfuerzo en esta línea para que profesionales puedan encaminarse hacia la investigación avanzada, la incorporación a centros de respuesta a incidentes y la formación de otros expertos (2013) [30].

El Plan de Inclusión Digital y Empleabilidad (2013) [30]:

> *"se ha desarrollado con la participación de un conjunto amplio de agentes público y privados y sirve de paraguas a las iniciativas de todos ellos, aúna esfuerzos y multiplica el efecto*

> *de las medidas que se adopten. El Plan es el resultado de las aportaciones de múltiples actores, públicos y privados, que se han incorporado para sumar esfuerzos en el objetivo común de aumentar la accesibilidad de Internet, avanzar en la alfabetización digital, disminuir la brecha digital de género y mejorar la empleabilidad en España".*

También es necesario destacar acerca de la Gobernanza en España, la existencia y funcionamiento de un dominio de nivel superior patrocinado (sTLD), como lo es .cat; para promocionar la lengua y cultura catalana en Internet ("ICANN aprueba el dominio .cat," 2005) [31].

Asimismo, ya se encuentran aprobados los proyectos para los dominios .gal, para la cultura gallega, y .eus, para la cultura vasca. Está previsto que los dominios .gal podrán comenzar a registrarse a principios del año 2014 y pocos meses después podrá navegarse por estas direcciones. Para el caso de dominios .eus a partir de marzo o abril del 2014 será posible registrar este tipo de dominios ("Aprobado el dominio .gal," 2013) [32].

La Agenda Digital para Europa se planteó como meta alcanzar el 100% de acceso a Internet en el 2013 en sus países miembros, por lo que ha promocionado la banda ancha satelital. España, como los demás países miembros, la ha implementado en su mercado para dar acceso a zonas rurales o aisladas donde la banda ancha móvil o por fibra no tienen cobertura (Comisión Europea, 2013) [33].

4.2. Colombia.

Como se enfatiza en los Foros Internacionales para la Gobernanza de Internet, los Gobiernos deben elaborar estrategias locales tanto de infraestructura, legislación y Gobernanza de Internet. Los países de América Latina han cambiado sus estrategias, y hoy en día ya no son simples observadores en la Gobernanza de Internet sino que se han convertido en participantes activos en esta gestión de Internet.

Colombia es uno de los países de América Latina que ha tomado el control en la Gobernanza de Internet, y sus estrategias en dicha gestión sirven de ayuda a otros países de la Región. Diversos representantes de los sectores interesados en la Gobernanza de Internet vienen participando de forma constante y activa en las cuestiones de regulación y gestión de Internet en Colombia.

El Gobierno Colombiano a través de la Comisión de Regulación de Comunicaciones (CRC), ha desarrollado un Plan de Acción como estrategia para mejorar el estado de la Gobernanza de Internet en Colombia. Dicho Plan de Acción ha sido socializado en varios eventos regionales realizados por el Estado Colombiano, como en el LACNIC XIX y en la Escuela Regional de Gobernanza de Internet.

Uno de los principales objetivos del plan en mención, es la creación de una escuela local de Gobernanza y el fortalecimiento del modelo *“multistakeholder” (Múltiples Partes Interesadas)* en Colombia, que permita la participación de todos los sectores colombianos interesados en la Gobernanza de Internet.

Entre los retos del Plan de Acción para la Gobernanza de Internet en Colombia, encontramos (CRC, 2013)[34]:

- *“Una plataforma de web libre: para la gestión de recursos educativos y contenidos digitales.*
- *Nuevas alianzas estratégicas con órganos representativos de la Gobernanza de Internet en América Latina y del Mundo.*
- *Un Plan de Mercadeo Digital: para aumentar la diversidad de participación y espacios participación remota.*
- *Creación de mesas de trabajo para discutir los temas principales de gobernanza y la forma en que participaran como país en las reuniones mencionadas.*
- *Presentar los resultados del Proyecto de Gobernanza de Internet colombiano a través de una declaración oficial del grupo Multistakeholder”.*

Cumpliendo con uno de los objetivos de este plan estratégico para la Gobernanza de Internet en Colombia, Bogotá fue sede de la *"Escuela del Sur de Gobernanza de Internet”* del 19 al 23 de marzo de 2012 (“Colombia, sede de la escuela”, 2012) [35].

La realización de la Escuela del Sur de Gobernanza de Internet, fue importante porque permitió *“capacitar a profesionales en todos los aspectos relacionados con la Gobernanza de Internet, desde una perspectiva global y con foco en la región de América Latina y el Caribe”*. Además, incentivó a que nuevas generaciones de profesionales colombianos, latinoamericanos y del Caribe sean partícipes activos de *“reuniones donde se conforma el futuro de la red Internet”,* y a jóvenes estudiantes de la región, a involucrase en *“el desarrollo internacional de las políticas de Internet y temas asociados con su gobierno”* (“Colombia, sede de la escuela”, 2012)[35].

La Comisión de Regulación de Comunicaciones, fomenta la constante y activa participación de Colombia como país, en las reuniones regionales y globales del Foro de Gobernanza de Internet.

Aunque el Plan de Acción antes mencionado sea la nueva estrategia para optimizar la Gobernanza de Internet en Colombia, el Gobierno Colombiano ya viene trabajando en el tema desde un tiempo atrás. En el año 2011, el Ministerio de Comunicaciones desarrolló una estrategia nacional para fomentar un *"Internet Sano"* que busca controlar la explotación sexual infantil sobre la red. Esta estrategia nacional se ubica en el marco de la *Ley 679 del 3 de agosto 2001* y *decreto reglamentario 1524 del 24 de julio de 2004* con el fin de *"prevenir y contrarrestar la pornografía, la explotación sexual y el turismo sexual con menores".* Los ciudadanos son incentivados a estar activos en la prevención de la explotación sexual infantil en internet ("Estrategia Internet Sano", 2010) [36].

Además, con la finalidad de integrar a los prestadores de servicio en la estrategia para un Internet sano y la prevención de la pornografía infantil en Internet, el Gobierno Colombiano complementa su estrategia dando cumplimiento a la *Ley 1336 del 21 de julio de 2009* que ordena a los proveedores de servicios de internet a *"incorporar cláusulas obligatorias en los contratos de portales de internet relativas a la prohibición y bloqueo de páginas con contenido de pornografía con menores de edad en Internet".*

De la misma manera, el Gobierno Colombiano consciente que *"la información es el activo más importante en el mundo actual"*, tomó medidas al respecto y proyectó una nueva estrategia para proteger los datos personales de los usuarios colombianos. Mediante la *Ley Estatutaria 1581 del 17 de octubre de 2012* y *decreto reglamentario*

1377 de 2013 se busca *"proteger los datos personales registrados en cualquier base de datos"*, y obliga a todas las entidades públicas y empresas privadas a *"revisar el uso de los datos personales contenidos en sus sistemas de información, y replantear sus políticas de manejo de información y fortalecimiento de sus herramientas".* Sin duda alguna, esta estrategia que se implementó en Colombia permite proteger los datos personales y la información que en los últimos años ha tenido un crecimiento acelerado (CCD, 2013) [37].

El Gobierno Colombiano a través del Ministerio de Tecnologías de la Información y las Comunicaciones, elaboró *"El Plan Estratégico Vive Digital"* para el periodo de Gobierno del 2009 al 2014 (MinTIC, 2011) [38].

El objetivo principal de este Plan es *"impulsar la masificación del uso de Internet para dar el salto hacia la prosperidad democrática de todos los colombianos"*, con la finalidad de lograr reducir el desempleo y la pobreza, aumentando la competitividad del país.

El Plan Estratégico Vive Digital puntualizó algunas metas concretas para lograr la masificación del uso de Internet en Colombia hasta el año 2014:

- *"Triplicar el número de municipios conectados a la autopista de la información".* Se pretende expandir la infraestructura de la red de fibra óptica nacional para pasar de 200 municipios que estaban conectados por fibra óptica en el 2009, a conectar a aproximadamente 700 municipios en el 2014.
- *"Conectar a Internet al 50% de las MIPYMES y al 50% de los hogares"* hasta el 2014, debido a que sólo el 27% de los

hogares y el 7% de MIPYMES contaban con conexión a Internet en el 2009.

- *"Multiplicar por 4 el número de conexiones a Internet"*. Se requiere aumentar las 2.2 millones de conexiones a Internet (conexiones fijas de más de 1024kbps e inalámbricas de 3G/4G) del 2009, a aproximadamente 8.8 millones de conexiones a Internet en el 2014.

Las metas del Plan Estratégico Vive Digital se fundamentan en un modelo de *Ecosistema Digital* desarrollado por el Banco Mundial para visualizar los distintos componentes que permiten la masificación del uso de Internet en una sociedad y sus interacciones. El Ecosistema Digital está conformado por cuatro grandes componentes: *Infraestructura, Servicios, Aplicaciones y Usuarios.* Este modelo permite analizar el estado de cada uno de las componentes mencionadas y se puedan diseñar estrategias nacionales para mejorarlas (MinTIC, 2011)[38].

La estrategia de *Infraestructura* del Plan Vive Digital fomenta la expansión de la red de fibra óptica nacional, compuesta por *"el backbone y backhaul nacional, las conexiones internacionales, la conectividad para zonas rurales, las conexiones de última milla e incluso las redes al interior de edificaciones"*. El presupuesto asignado por el Gobierno Colombiano para lograr este objetivo es de 200 millones de dólares. Aunque se espera conectar 500 municipios adicionales a las redes de fibra óptica nacional, aproximadamente 400 municipios restantes continuarán sin estar conectados a dichas redes, sin embargo, seguirán conectados a través de otras tecnologías como microondas, inalámbricas o satelitales (MinTIC, 2011)[38].

En cuanto a *Los Servicios*, el Plan Vive Digital establece una serie de iniciativas que pretenden mejorar la asequibilidad de los colombianos a estos servicios y a los terminales necesarios para usarlos. El alto costo del servicio de Internet en relación al ingreso de los habitantes, especialmente de los estratos más bajos, es *"una de las principales razones por las cuales las personas en Colombia no contratan servicio de Internet en su hogar"* (MinTIC, 2011)[38].

Una de las estrategias del Gobierno Colombiano para hacer más asequible el servicio de Internet es *"la reducción del Impuesto al Valor Agregado (IVA) al servicio de Internet fijo"* para los estratos sociales 1, 2 y 3, que corresponden a estratos bajos que albergan a los usuarios con menores recursos, y para las MIPYMES. Además, se espera *"subsidiar parcialmente el costo de este servicio y por lo tanto disminuir el costo para el usuario final*", con lo cual se espera que *"más usuarios que antes no lo podían pagar, se encuentren así en condiciones de hacerlo"* (MinTIC, 2011)[38].

De la misma manera, el Gobierno Colombiano planteó *"una serie de iniciativas para aumentar la penetración de equipos terminales"* con el fin de proveer el acceso a Internet a través de éstos. Las estrategias del Plan Vive Digital involucran al Estado, operadores, fabricantes y establecimientos de crédito estatales. Las estrategias a cumplir son:

- *"Articular a los involucrados en la importación, producción, comercialización y venta de terminales para reducir costos y aumentar la asequibilidad.*
- *Promover el acceso a crédito a través de fondos de garantías y préstamos blandos, con el apoyo de la banca multilateral.*
- *Incentivar la producción local de computadoras y otros terminales a bajo costo.*

- *Alargar la Cláusula de Permanencia Mínima de contratos de telecomunicaciones para que los operadores comercialicen planes de Internet que incluyan terminales a crédito.*
- *Reducir los aranceles de importación para los equipos de conexión y servicio de Internet, incluyendo no sólo los terminales del usuario, sino todos los equipos involucrados en la prestación del servicio".*

El desarrollo de *Aplicaciones* con interés social es importante porque permite que Internet se vuelva mucho más útil para los usuarios, y de esta manera, el número de interesados en acceder a Internet se incremente. El modelo de Ecosistema Digital permitió que el Gobierno Colombiano reconozca que *"una de las principales razones por las que tanto usuarios como MIPYMES no tienen servicio de Internet en sus hogares o lugar de trabajo es la percepción de que el servicio no es necesario o útil para ellos",* esto principalmente a *"la falta de aplicaciones y de contenido local útil para el usuario y microempresas nacionales"* (MinTIC, 2011)[38].

El Ministerio TIC consciente del problema que debe resolver, apoya *"la generación de aplicaciones y contenidos digitales útiles y relevantes al usuario nacional, que aumenten la demanda de Internet"*. Además, el Plan Vive Digital tiene como objetivo hasta el 2014, lograr que el 50% de las aproximadamente 1.500.000 microempresas que existen en Colombia tengan servicio de Internet, para ello, es fundamental *"impulsar el desarrollo de aplicaciones que sean útiles para las microempresas".* Con esto, el Gobierno Colombiano espera que *"más y más microempresas encuentren la utilidad de las TIC para su negocio y adquieran el servicio de Internet",* permitiéndoles también mejorar la productividad y la competitividad (MinTIC, 2011)[38].

Los Usuarios son el elemento más importante del Ecosistema Digital debido a que son ellos *"quienes hacen uso de las aplicaciones, los servicios y la infraestructura".* Para el Gobierno Colombiano es necesario que *"los usuarios tengan acceso a la tecnología, aprendan a usarla y se apropien de ella",* ya que *"entre más personas usen la tecnología, se genera una mayor demanda de aplicaciones y servicios, que estimula el ecosistema digital".* (MinTIC, 2011)[38].

Otra de las estrategias del Plan Vive Digital es poner en marcha hasta el 2014, alrededor de 800 nuevos Tecnocentros. Estos Tecnocentros contarán con más equipos y servicios que los más de 3.000 Telecentros que ya existían en los 1.050 municipios de Colombia en el 2009. La escala y oferta de servicios de los Tecnocentros *"estará acorde con el tamaño de la población donde se encuentren ubicados".* Los más completos tendrán áreas de: *"servicios y bienes; acceso a Internet con áreas de trabajo colaborativo; teleeducación y proyección; entretenimiento, y Gobierno en Línea, entre otras"* (MinTIC, 2011)[38].

Además, los programas de capacitación que el Gobierno Colombiano brinda a las personas y MIPYMES, permite que los usuarios puedan aprovechar *"las aplicaciones y contenidos digitales generados por las otras iniciativas del Plan Vive Digital".* Las estrategias de capacitación incluyen también la implementación de tecnologías para personas con discapacidad sensorial en los Tecnocentros de al menos 20 ciudades, con la finalidad de *"reducir las brechas digitales y sociales y promover la inclusión educativa, laboral y social"* de la población con discapacidad (MinTIC, 2011)[38].

Finalmente, el Plan Vive Digital impulsa iniciativas de ciberdefensa y ciberseguridad a través del Ministerio de Defensa Nacional, con el objetivo de propiciar *"un ciberespacio más seguro para todos los*

colombianos". La propuesta principal de ciberseguridad fue crear para el 2011, *"El Centro de Respuesta de Emergencias Cibernéticas, ColCERT"* que tiene como objetivo, coordinar *"la protección del ciudadano y del Estado";* y junto con la Policía y el Comando Conjunto de las Fuerzas Militares deben garantizar a la ciudadanía mayor protección contra delitos cibernéticos, facilitando así *"la confianza en Internet y aumentando su uso".* Mientras tanto para el 2014, el Estado colombiano contará con *"El Comando Conjunto Cibernético",* que se ocupará de *"proteger la infraestructura crítica contra ataques cibernéticos*" como medida de Ciberdefensa Nacional (MinTIC, 2011)[38].

CAPÍTULO 5:

DIAGNÓSTICO DE LA GOBERNANZA DE INTERNET EN ECUADOR.

5.1. Constitución de la República del Ecuador.

La Constitución de la República del Ecuador fue elaborada por la Asamblea Nacional Constituyente y presentada el 25 de julio de 2008, siendo aprobada por los ecuatorianos en Consulta Popular el 28 de septiembre de 2008 y entró en vigencia desde su publicación en el Registro Oficial No. 449 el 20 de octubre de 2008.

La Constitución está por encima de cualquier norma jurídica dentro de la política ecuatoriana debido a su supremacía constitucional, proporcionando los lineamentos en los que el Estado ecuatoriano se

organiza, y la relación en la que el Gobierno y la ciudadanía ecuatoriana se desenvuelven.

La Constitución contempla el derecho que tienen los ecuatorianos a comunicarse, fomentando también la diversidad de información con la finalidad de promover el acceso universal al conocimiento.

El numeral 1 del artículo 16 enfatiza que todos los ecuatorianos tienen derecho a *"una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos",* garantizando *"el acceso universal a las tecnologías de información y comunicación"* como lo contempla el numeral 2 del artículo en mención. De la misma manera, el numeral 1 del artículo 18 destaca que todas las personas tienen derecho a *"buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior".*

Además, la Constitución protege la integridad de las niñas, niños y adolescentes. El numeral 7 del artículo 46, exhorta al Estado para que adopte medidas que aseguren a las niñas, niños y adolescentes, como:

> *"Protección frente a la influencia de programas o mensajes, difundidos a través de cualquier medio, que promuevan la violencia, o la discriminación racial o de género. Las políticas públicas de comunicación priorizarán su educación y el respeto a sus derechos de imagen, integridad y los demás específicos de su edad. Se establecerán limitaciones y sanciones para hacer efectivos estos derechos".*

De esta manera, se busca que los niños no sean vulnerables a información inadecuada que en la mayoría de los casos acceden con mucha facilidad.

En cuanto a la protección de los usuarios y consumidores, el artículo 52 enfatiza que los ecuatorianos tienen derecho a *"disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características".* Con esto se evita los monopolios en los servicios y salvaguarda a los usuarios en la libertad a contratar el servicio deseado de acuerdo a su conveniencia.

El numeral 8 del artículo 347 hace responsable al Estado de *"incorporar las tecnologías de la información y comunicación en el proceso educativo y propiciar el enlace de la enseñanza con las actividades productivas o sociales".* Para el Estado es importante que la educación que ofrece a los ecuatorianos sea integral, incluyendo a las nuevas tecnologías en las instituciones educativas, a fin de evitar que se incremente la brecha digital en la sociedad ecuatoriana.

Finalmente, el artículo 384 protege el derecho a la libertad de expresión, mencionando que *"el sistema de comunicación social asegurará el ejercicio de los derechos de la comunicación, la información y la libertad de expresión, y fortalecerá la participación ciudadana",* siendo el Estado quien *"formulará la política pública de comunicación, con respeto irrestricto de la libertad de expresión y de los derechos de la comunicación consagrados en la Constitución y los instrumentos internacionales de derechos humanos".* Sin duda alguna, la Constitución tiene normas claras que ampara todos los derechos que poseemos los ciudadanos ecuatorianos, pero resulta importante que de la misma manera se elaboren políticas públicas acordes a los

lineamentos que contempla la Carta Magna, con el objetivo de poseer estrategias que permitan el desarrollo integral de la sociedad ecuatoriana.

5.2. Plan del Buen Vivir.

De acuerdo al objetivo número once del *Plan del Buen Vivir: Asegurar la soberanía y eficiencia de los sectores estratégicos para la transformación industrial y tecnológica* (2013 - 2017) [39] se declara que:

> *"el Ecuador tiene una oportunidad histórica para ejercer soberanamente la gestión económica, industrial y científica, de sus sectores estratégicos. Esto permitirá generar riqueza y elevar en forma general el nivel de vida de nuestra población. Para el Gobierno de la Revolución Ciudadana, convertir la gestión de los sectores estratégicos en la punta de lanza de la transformación tecnológica e industrial del país, constituye un elemento central de ruptura con el pasado".*

Se expresa en el Plan del Buen Vivir que:

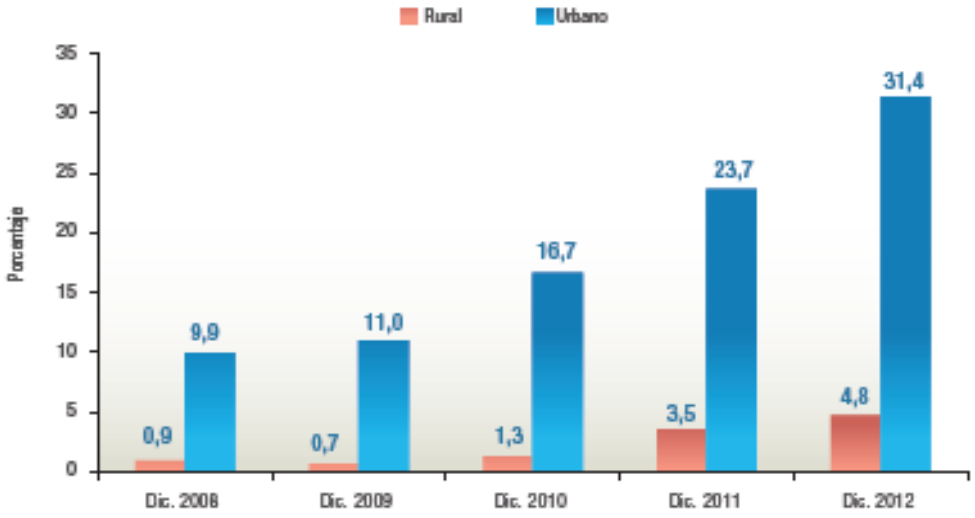
> *"el Plan de Gobierno 2013-2017 (Movimiento Alianza PAÍS), señala que el país debe gestionar sus recursos estratégicos en el marco de una inserción internacional, que permita que el ciclo tecnológico actual basado en la automatización, la robótica y la microelectrónica, contribuya al incremento generalizado del bienestar para sus habitantes. Esto se conseguirá mediante un conjunto de políticas para la sustitución de importaciones, la transferencia de tecnología, la*

> *generación de valor agregado local, la industrialización para la exportación, la redistribución de la riqueza y la implementación de industrias de producción de bienes intermedios y finales, dentro del territorio nacional."*

El documento afirma que la información y el conocimiento tienen un rol principal en la construcción de una nueva sociedad. Esto ha generado un nuevo impulso del gobierno hacia los territorios digitales. La mayoría de las instituciones públicas y privadas a nivel nacional no proporcionan servicios ni trámites que permitan acceder a servicios de calidad por medios electrónicos. En el mejor de los casos, se ofertan aplicaciones informativas, cuando el verdadero requerimiento es transaccional. Esta problemática es más grave cuanto más lejos se encuentre la población de las oficinas centrales en las que se realizan los trámites administrativos y/o la prestación física de estos servicios, lo que acentúa la exclusión social y castiga a la población más alejada de los centros urbanos.

Un mayor uso de las TICs en el país se ve reflejado en el crecimiento de los servicios móviles, el uso de Internet se ha cuadruplicado, el acceso a Internet en los hogares considerados pobres ha aumentado y la conectividad de fibra óptica ha incrementado de 1251 km en el 2006 a 8689 km hasta junio de 2012 (Plan del Buen Vivir, 2013 - 2017) [39].

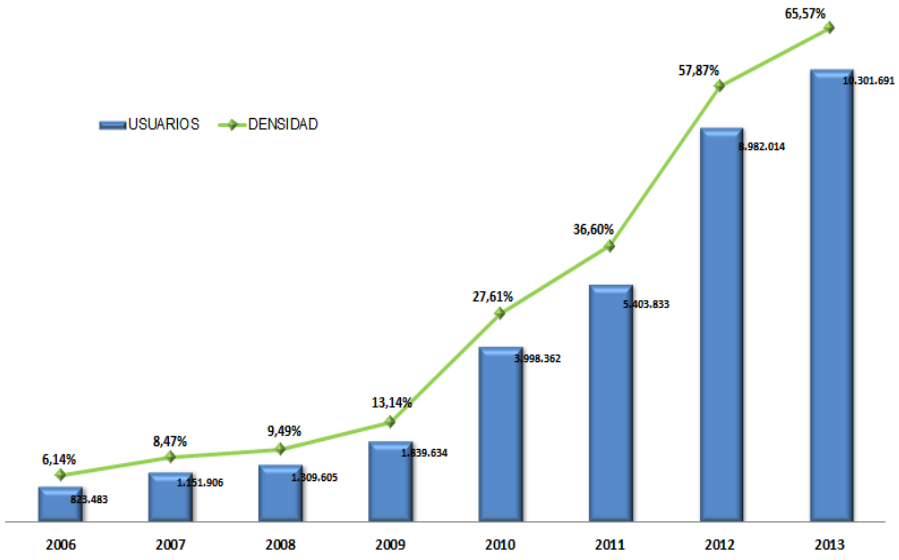
Podemos observar en la Figura 5.1 que según el Instituto Nacional de estadísticas y censos (INEC), el porcentaje de hogares urbanos y rurales con acceso a Internet por zona en diciembre de 2012 son de 31.4% en la zona urbana y 4.8% en la zona rural.



*Fuente: Instituto Nacional de Estadísticas y Censos – INEC. (*Gráfico 6.11.3, p. 320) [39].

Figura 5.1: Porcentaje de hogares urbanos y rurales con acceso a Internet por zona.

Por otra parte, en la Figura 5.2; según la SENATEL, el acceso a Internet en el 2013 llega al 65.57%. A partir del año 2010 se incluyen líneas activas de datos e Internet de Servicio Móvil Avanzado (SMA).



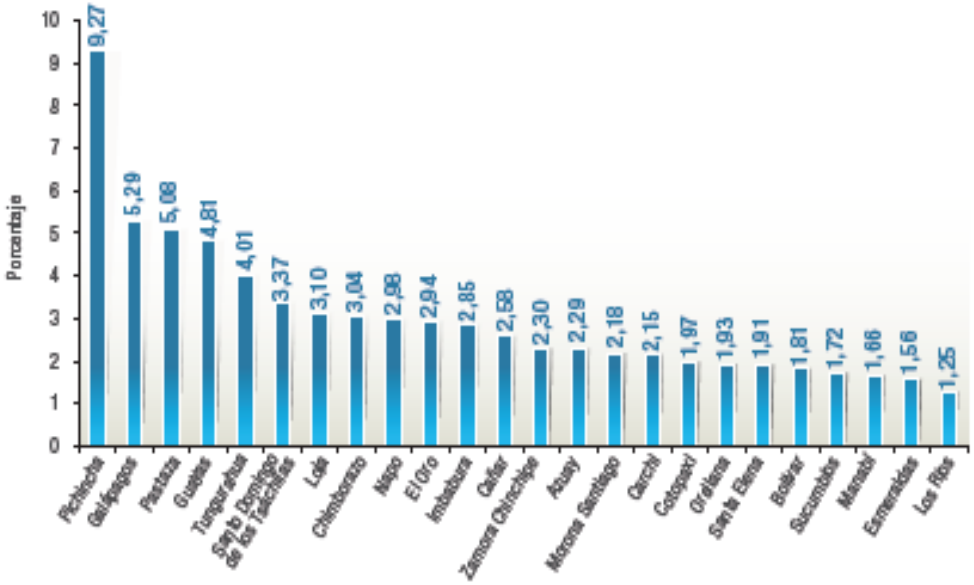
Fuente: Secretaría Nacional de Telecomunicaciones – SENATEL [40].

Figura 5.2: Acceso anual a Internet en Ecuador.

Otro elemento importante a considerar mencionado en el Plan del Buen Vivir, es la velocidad en el acceso a Internet. El servicio de banda ancha es concebido como uno de los componentes principales de conectividad para el desarrollo digital.

Uno de los grandes problemas que se está generando en el país es el de la brecha digital y exclusión debido a una diferencia marcada de acceso dentro del país, siendo notoria en las provincias más pobladas como Pichincha y Guayas, en las capitales provinciales y en las cabeceras cantonales. Asimismo, esta brecha se ve reflejada a nivel internacional, estando Ecuador ubicado por debajo de países de Europa, del Asia del Pacífico y de ciertos países de Latinoamérica en lo que respecta a la densidad de conexiones de banda ancha fija (Plan del Buen Vivir, 2013 - 2017) [39].

En la Figura 5.3, podemos observar la densidad de conexiones de banda ancha fija en las distintas provincias del país.



Fuente: Secretaría Nacional de Telecomunicaciones – SENATEL. (Gráfico 6.11.4, p. 321) [39].

Figura 5.3: Densidad de conexiones de banda ancha fija.

Entre las políticas del Plan del Buen Vivir se encuentra la de democratizar la prestación de servicios públicos de telecomunicaciones y de tecnologías de información y comunicación con los siguientes lineamientos estratégicos:

- *"Garantizar la calidad, la accesibilidad, la continuidad y tarifas equitativas de los servicios, especialmente para el área rural, los grupos sociales más rezagados y los actores de la economía popular y solidaria.*
- *Fortalecer las capacidades necesarias de la ciudadanía para el uso de las TIC, priorizando a las MIPYMES y a los actores de la economía popular y solidaria.*
- *Impulsar la calidad, la seguridad y la cobertura en la prestación de servicios públicos, a través del uso de las telecomunicaciones y de las TIC; especialmente para promover el acceso a servicios financieros, asistencia técnica para la producción, educación y salud.*
- *Facilitar la competencia entre operadores de servicios de telecomunicaciones para establecer una distribución más uniforme del mercado y evitar monopolios y oligopolios.*
- *Fortalecer la seguridad integral usando las TIC.*
- *Desarrollar redes y servicios de telecomunicaciones regionales para garantizar la soberanía y la seguridad en la gestión de la información.*
- *Impulsar el gobierno electrónico transaccional y participativo para que la ciudadanía acceda en línea a datos, información, trámites y demás servicios.*
- *Establecer mecanismos de transferencia de tecnología en la normativa de telecomunicaciones, para permitir el desarrollo local de nuevas aplicaciones y servicios.*

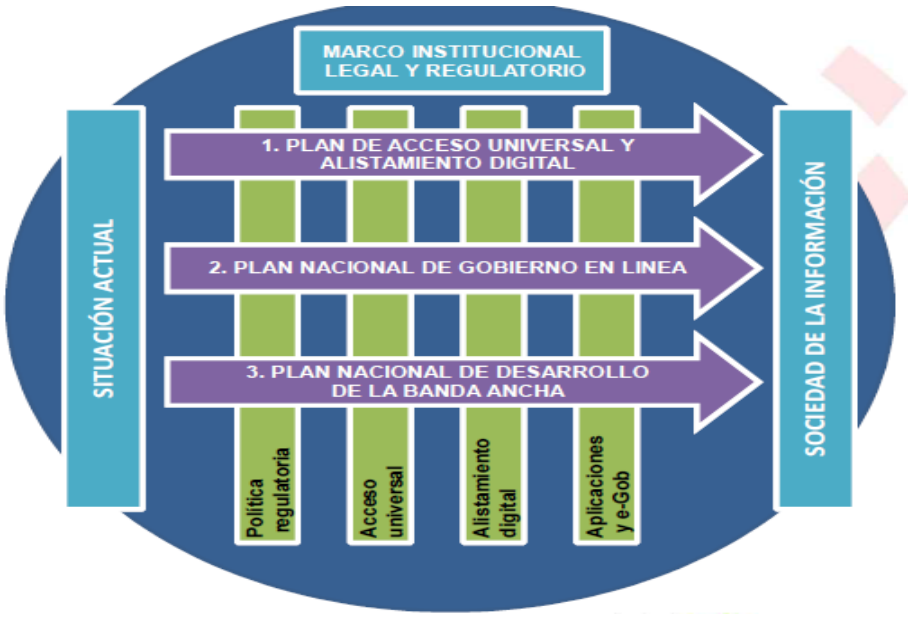
Las metas trazadas para el 2017 en este documento son:

- *Alcanzar un índice de digitalización de 41.7.*
- *Aumentar el porcentaje de personas mayores a cinco años que usan TIC del 41.4 al 50%.*
- *Reducir el analfabetismo digital del 21.4 al 17.9%.*
- *Alcanzar un índice de gobierno electrónico de 0.55".*

5.3. Ecuador Estrategia Digital 2.0.

En el año 2009, el Gobierno ecuatoriano se planteó la meta de eliminar la inequidad geográfica y social en la provisión y acceso a las TICs. Para ello, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) puso en marcha un plan para fomentar la participación de la ciudadanía, recrear la interculturalidad, valorar la diversidad y fortalecer la identidad plurinacional. Este plan se basa en el conjunto de políticas sectoriales denominado *La Estrategia Ecuador Digital 2.0 (EED)*, cuyo objetivo es que todos los ciudadanos accedan y generen información y conocimiento, mediante el uso efectivo de las TIC, como parte del proceso de desarrollo social del Ecuador ("Gobierno destina", 2012) [41].

Al principio, la estrategia digital se basó en ejes como equipamiento, conectividad, capacitación, aplicación y contenidos. Para el año 2011, el MINTEL y la Comisión Económica para América Latina y el Caribe (CEPAL) actualizaron la estrategia e implementaron tres planes que hasta la actualidad buscan resolver los problemas que limitan la conectividad en el país. En la Figura 5.4 mostramos el modelo de Estrategia Ecuador Digital con sus respectivos planes.



Fuente: Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL [42].

Figura 5.4: Modelo Estrategia Ecuador Digital 2.0.

El Plan Nacional de Acceso Universal y Alistamiento Digital consiste en delinear políticas de acceso a los beneficios sociales y productivos asociados a las TICs, garantizando igualdad de oportunidades a todos los habitantes, con especial énfasis en los sectores con escaso acceso, mediante programas de capacitación sobre el uso de herramientas para el desarrollo social, cultural, comercial y educativo. El Plan de Gobierno Digital tiene como objetivo proveer de mayores y mejores servicios públicos en línea para ciudadanos, mediante una adecuada infraestructura tecnológica y la promoción de servicios digitales del Estado; y el Plan Nacional de Banda Ancha apunta a la masificación del acceso a Internet a escala nacional, dando prioridad a las zonas rurales con un ecosistema de redes, servicios y recursos para eliminar barreras económicas, técnicas, sociales y de mercado, que limitan el despliegue de infraestructura y servicio. También se han definido medidas

regulatorias a fin de eliminar políticas de mercado que restringen el acceso (“Gobierno destina”, 2012) [41].

El MINTEL define al *Programa de Acceso Universal a las Tecnologías de Información y Comunicación (TIC)* como la agrupación de proyectos interrelacionados de vital importancia para el progreso de las TIC en el Ecuador, como el Programa Internet para Tod@s en Aulas Móviles y los Infocentros Comunitarios.

Las Aulas Móviles son medios de transporte equipados con la más alta tecnología que promueven, por todos los rincones del país, el uso de herramientas tecnológicas, construyendo confianza y seguridad en el buen uso de las TIC de manera gratuita. Desde noviembre de 2011, el MINTEL ha estado desarrollando esta importante iniciativa, teniendo actualmente en circulación siete Aulas Móviles (“Aulas Móviles”, 2013) [43].

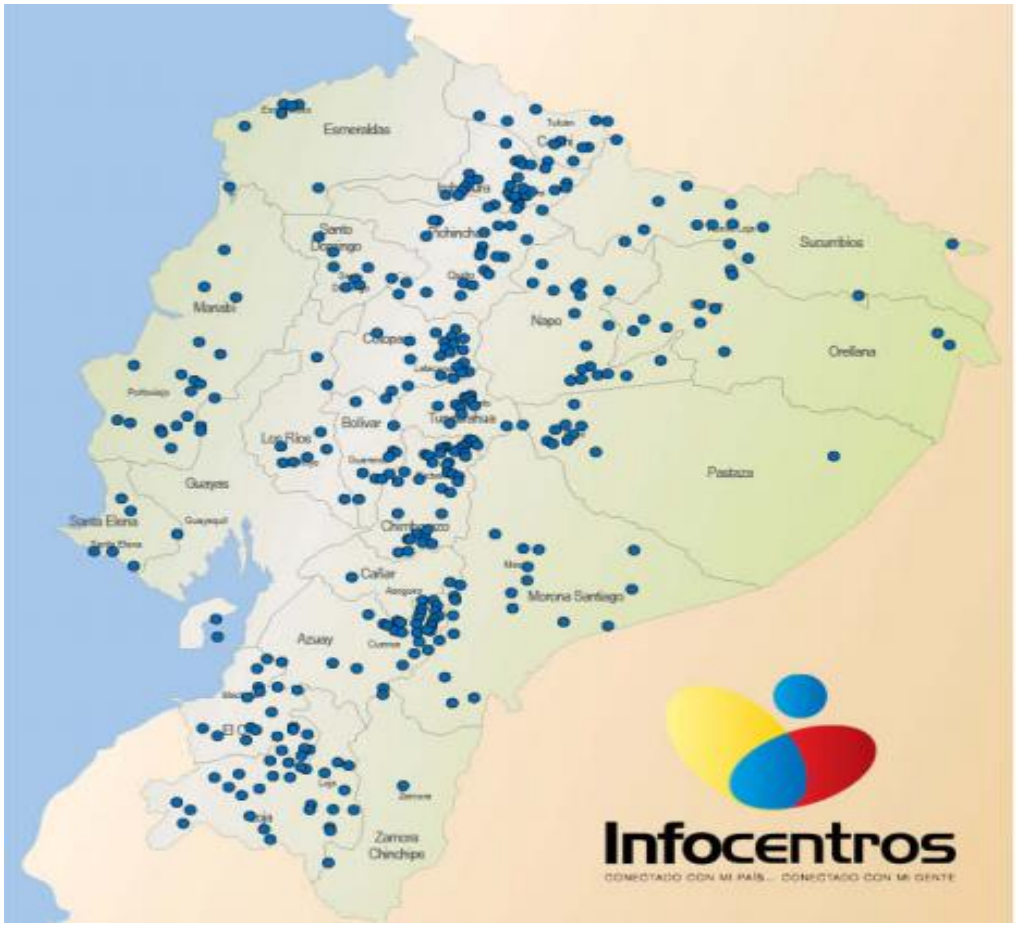
Los Infocentros son espacios comunitarios de participación y desarrollo que garantizan el acceso inclusivo a las TIC de las poblaciones de parroquias rurales y urbanas marginales del Ecuador. La propuesta es introducir al ciudadano en el conocimiento de las TIC con el fin de reducir la brecha y analfabetismo digital, motivándole a emplear la tecnología para su aprovechamiento y mejorando así su calidad de vida y desarrollo productivo de su comunidad (“Infocentros Comunitarios”, 2012) [44].

El *Plan de Alistamiento Digital* (2012) [45] tiene como objetivos permitir a los ciudadanos utilizar las TICs de acuerdo a su interés y beneficio, promover el aprendizaje significativo, para lo cual se han desarrollado procesos de acompañamiento, así como una serie de contenidos y una cantidad de aplicaciones. La propuesta del plan es que la comunidad

genere conocimiento para beneficio propio y de la sociedad, además de aprender a utilizar la tecnología en una situación de su vida. Está dirigido a todas las comunidades y personas que deseen involucrarse en el mundo de las TICs sin límites de edad a través de los Infocentros Comunitarios. Entre los programas que se han considerado en el plan mencionado para brindar capacitación son: Contenidos y Estrategias TIC, Redes Sociales, Sociedad de la Información, TIC para Niñ@s, eGOBIERNO y Formación de Formadores.

De acuerdo con la finalidad del Plan de Acceso Universal y Alistamiento Digital, el Ministro Guerrero, en el Enlace Ciudadano 335, señaló que con los Infocentros Comunitarios no sólo se facilita el acceso a equipos tecnológicos como computadores, sino que se imparten capacitaciones gratuitas de gran utilidad que posibilitan aprovechar las ventajas de la tecnología.

Además, en el Informe de Rendición de Cuentas del MINTEL 2013, el Ing. Guerrero precisó que a diciembre del 2013 Ecuador ya contaba con 489 Infocentros, como se muestra en la Figura 5.5, y que éstos habían recibidos 1 millón 600 mil visitas, realizando capacitaciones en TIC a 87 mil ecuatorianos de escasos recursos.



Fuente: Ministerio Coordinador de Sectores Estratégicos – MCSE [46].

Figura 5.5: Cobertura de Infocentros.

Dentro de una encuesta realizada por el MINTEL para establecer el porcentaje de visitas a los Infocentros según el tipo de ocupación, desde enero de 2012 hasta mayo de 2013, se determinó que el 70% de los visitantes corresponde a estudiantes menores, seguidos por madres de familia con un 7%, estudiantes adultos 6%, otros 4%, empleados públicos 3%, agricultores 3%, entre otros. Asimismo, en otra encuesta realizada por el MINTEL, en abril de 2013, se definió que las razones por la que más se visitan los Infocentros son: investigación, capacitaciones, uso del correo electrónico, tareas escolares, recreación, comunicación con sus familiares, entre otras.

Por otra parte, el *"Plan Nacional de Banda Ancha"* (2012) [42] tiene como objetivos mejorar la calidad de vida de los ecuatorianos mediante el uso, introducción y apropiación de las TICs; incrementar el uso y apropiación TIC en educación y en todos los sectores productivos de la sociedad, como salud, seguridad, MIPYMES, servidores públicos; permitir a todos los ecuatorianos independientemente de su condición socio-económica y ubicación geográfica el acceso a los servicios de banda ancha con calidad y calidez; impulsar el despliegue de redes y servicios a nivel nacional; y crear condiciones de mercado para desarrollo de la banda ancha.

El Plan Nacional de Banda Ancha consta de tres programas:

- Despliegue de infraestructura y condiciones de mercado para banda ancha.
- Gestión eficiente de recursos, insumos y calidad para banda ancha.
- Banda ancha con responsabilidad social y ambiental.

Actualmente, dentro del Plan Nacional de Banda Ancha se ejecuta el programa Conectividad Escolar que permite al Ministerio de Telecomunicaciones y Sociedad de la Información brindar los mejores servicios en equipamiento tecnológico y acceso a Internet. Con este programa se fortalecen los procesos educativos sobre el aprovechamiento de las TICs, donde también se promueve el crecimiento económico del país, la inclusión social y la reducción en la desigualdad del aprendizaje escolar ("Programa Conectividad Escolar", 2012) [47].

A través del programa de Conectividad Escolar, el estado se propone proveer de aulas informáticas con acceso a Internet al 100% de

establecimientos educativos urbanos y rurales. Hasta diciembre del 2012, se entregaron equipos y conectividad a 5.040 instituciones educativas, beneficiando a 1.628.615 estudiantes en las 24 provincias del Ecuador. La meta del programa es dotar de conectividad a las 9.732 escuelas a nivel nacional en el periodo del 2007 hasta el 2015. Entre los equipos que se proporcionan a los centros educativos están computadoras de escritorio, impresoras, proyectores, pizarras digitales, reguladores de voltaje, routers, alarmas y mobiliario ("Programa Conectividad Escolar", 2012) [47].

Entre las metas trazadas en el Plan Nacional de Banda Ancha están:

- Al 2014 decrementar significativamente el precio del kbps.
- Al 2015 incrementar en 80% las MIPYMES conectadas a Banda Ancha.
- Al 2015 lograr que la mayoría de parroquias rurales tenga conexión a Banda Ancha.
- Al 2015 incrementar al menos en 50% los hogares ecuatorianos del Quintil 1 y 2 con acceso a Banda Ancha.
- Al 2015 incrementar al menos en 60% los hogares ecuatorianos con acceso a Banda Ancha.
- Al 2016 triplicar el número de conexiones a Banda Ancha.
- Al 2017 alcanzar al menos el 75% de la población ecuatoriana con acceso a Banda Ancha.

Es importante recalcar que en las metas del plan sólo se menciona el aumento de acceso a conexiones de banda ancha, mas no en velocidades e inclusive no se define el ancho de banda para el país. Sin embargo, el Plan Nacional de Desarrollo de las Telecomunicaciones (2007 - 2012) [48] *"establece una meta realista de 256 Kbps para la banda ancha para los próximos años, y una meta ideal que busque*

alcanzar el 1 Mbps". La meta planteada por el Gobierno Nacional de proveer a los ecuatorianos de una velocidad de 256 Kbps y en el mejor de los casos de 1 Mbps, definitivamente no puede ser llamada Banda Ancha.

5.4. Delitos Informáticos.

Los delitos informáticos se los define como cualquier actividad delictiva en la que se utilizan como herramienta los computadores o redes, o éstos son las víctimas de la misma, o bien el medio desde donde se efectúa dicha actividad delictiva; se refieren a los actos dirigidos contra la confidencialidad, integridad y la disponibilidad de los datos y sistemas informáticos (CdE, 2001) [49].

Existen cuatro técnicas consideradas como las más usadas por los delincuentes informáticos en el país, éstas son:

- *Phishing:* Es la más usada, consiste en el robo de información que es ingresada por la propia víctima a través de páginas web o correos electrónicos falsos, pero que simulan ser de una entidad financiera con la que la persona tiene relación. Por lo general se solicita el nombre completo de la persona, su número de cédula, número de cuenta, dirección y teléfono.
- *Scanning:* Consiste en el escaneo o copia de la información contenida en las bandas magnéticas de las tarjetas de débito o crédito, creando una réplica del documento.
- *Scanning* por redes sociales: Consiste en el envío de un correo electrónico a la víctima, haciendo creer que se trata de un correo proveniente de la red social; pero al momento de abrir el correo, este programa copia toda la información del usuario.

También consiste en el envío de invitaciones de amistad que al ser aceptadas permite al malhechor acceder a información de la víctima llevándolo a conocer sus datos, incluso a conocer los movimientos y forma de vida de la víctima.

- *Sniffing:* Los hackers colocan aparatos que cumplen las funciones de espía en una terminal o una red informática logrando intervenir claves, direcciones de correo o incluso suplantar identidades en los chats (“Las técnicas”, 2012) [50].

Según estadísticas reveladas por Dmitry Bestuzhev, responsable del equipo de investigación y análisis para Latinoamérica de Kaspersky, en Ecuador ocurren cuatro intentos por atacar un canal electrónico cada segundo, sea para robarse datos personales y claves del banco a un cliente, para hacer compras online con tarjetas de crédito ajenas o hasta para desprestigiar con pornografía a algún ciudadano. Se basa en el hecho de que solo como Kaspersky, se han detectado de enero a noviembre del 2013 un ataque por segundo, sumando las computadoras protegidas con otros proveedores de antivirus y las que no tienen ningún tipo de protección; Bestuzhev afirma con certeza que han ocurrido más de cuatro ataques por segundo (“Cibercrimen: cuatro ataques”, 2013) [51].

Pichincha y Guayas son las provincias donde mayor se registra el cibercrimen con 54% y 32% respectivamente (“Cibercrimen: cuatro ataques”, 2013) [51].

La banca ecuatoriana trabaja constantemente para brindar canales seguros a sus clientes debido a que gran parte del pago de las cuentas de éstos se las realiza utilizando servicios de la web. En Banco Pichincha, que concentra cerca del 30% de los depósitos bancarios, los delitos prácticamente se han eliminado. De acuerdo a lo mencionado

por Juan Carlos Beltrán, gerente de Riesgo de Banco Pichincha, "*por cada 10 millones de dólares transados por Internet, el ratio de pérdidas por fraudes es de $ 0,04*" ("Cibercrimen: cuatro ataques", 2013) [51].

5.4.1. El Centro de Respuesta Inmediata contra Ciberdelitos de la SUPERTEL.

El Ing. Fabián Jaramillo, Superintendente de Telecomunicaciones del Ecuador, anunció el 9 de mayo del 2012 a la comunidad internacional que asistía al evento LACNIC XVII realizado en Quito, la próxima implementación del Centro de Respuesta a Incidentes Informáticos del Ecuador (CERT o CSIRT), para permitir que los usuarios ecuatorianos sean protegidos en su navegación por Internet (Rodríguez, 2013) [52].

La idea de un Centro de Respuesta a Incidentes Informáticos debe ser:

> *"detectar e identificar la amenaza, bloquearla, monitorizarla, reportar, guardar registros y evidencias de la amenaza, responderla, pedir información a los organismos o actores involucrados dentro de la respuesta a la amenaza de ser necesario, hacer uso de la infraestructura disponible y necesaria y comunicar a los demás equipos de apoyo o CSIRTs conectados, para así mitigar las posibles consecuencias que produce un incidente de seguridad informática"* (Revista SUPERTEL No. 13, 2012, p. 5) [53].

El CERT Ecuador/CC será creado bajo el marco de las siguientes funciones:

- *“Diseñar y ejecutar los procedimientos que se utilizarán para la identificación de los componentes de infraestructura informática de alto riesgo, evaluando sus vulnerabilidades con la finalidad de tomar las acciones apropiadas para controlar el nivel de riesgo en el ambiente de operación, tales como sistemas informáticos y personal involucrado.*
- *Realizar actividades proactivas y reactivas para ayudar a proteger y asegurar la integridad y confidencialidad de los datos de empresas y organizaciones públicas y privadas que utilizan TICs.*
- *Determinar el impacto, el alcance y la naturaleza del evento o incidente informático mediante la comprensión de la causa técnica, con el objetivo de recomendar, coordinar y apoyar la implementación de la solución a los casos presentados por ciberdelito.*
- *Dar respuesta a los incidentes Informáticos presentados a través de su investigación, recopilación de pruebas o evidencias de un indicio del cometimiento de fraude en las TICs.*
- *Mantener una relación de cooperación con los CSIRT de otros países a fin de tener apoyo y soporte en la solución de incidentes dentro del Ecuador.*
- *Elaborar registros de las investigaciones realizadas por el Centro de Respuesta a Incidentes, para tener los antecedentes y referencias de los casos presentados.*
- *Proponer y elaborar proyectos de investigación, innovación y transferencia tecnológica relacionados a temas de respuesta a incidentes informáticos y control de ciberdelitos.*

- *Gestionar a nivel interno y externo de este organismo, la elaboración de convenios con organizaciones nacionales e internacionales los cuales permitirán las investigaciones de casos de fraude en las TICs.*
- *Coordinar y colaborar con organizaciones públicas y privadas, tales como proveedores de servicio de internet (ISP), empresas proveedoras de seguridad del Ecuador, CSIRT de otros países, Fiscalía General del Estado y otras instituciones que por la naturaleza de los servicios prestados, cuentan con departamentos de seguridad informática con la finalidad de hacer cumplir la reglamentación correspondiente"* (Revista SUPERTEL No. 13, 2012, ps. 7-8) [53].

Dentro del proceso de implementación del CERT Ecuador/CC se ha previsto dos fases. La primera fase constituye la conformación del grupo de trabajo, coordinar los servicios del CERT Ecuador/CC con organizaciones públicas y privadas del sector y el equipamiento con herramientas de hardware y software de seguridad. La segunda fase corresponde a la consolidación a nivel nacional e internacional del CERT Ecuador/CC. Se tenía planificado la ejecución de este proyecto hasta fines del año 2012 (Revista SUPERTEL No. 13, 2012, p. 7) [53].

5.4.2. Código Orgánico Integral Penal.

Mediante la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, que entró en vigencia desde su publicación en el Registro Oficial No. 557 el 17 de abril del 2002, se reformaron los artículos 202, 353, 415, 553, 563, 606 del Código Penal del Ecuador; correspondiendo en la ley mencionada a los artículos del 58, 60, 61, 62,

63 y 64. Además, a través del artículo 59 de la ley, se sustituyó el artículo 262 del Código Penal (Fiscalía General del Estado, 2009) [54].

En el nuevo Código Orgánico Integral Penal (COIP), que se estima entrará en vigencia a partir de agosto del 2014, se castiga los delitos contra la integridad sexual y reproductiva.

Mediante el artículo 103 del COIP, se sanciona con pena privativa de la libertad de trece a dieciséis años, a la persona que fotografíe, filme, transmita o edite materiales visuales, informáticos, electrónicos o de cualquier soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual.

Asimismo; a través del artículo 173 del COIP, se sanciona con pena privativa de la libertad de uno a tres años, a la persona que proponga un encuentro con una persona menor de dieciocho años a través de algún medio electrónico o telemático, siempre que esta propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual. En caso de que el acercamiento se obtenga mediante intimidación o coacción se aplicará una pena de tres a cinco años.

De la misma manera, se sancionará con prisión de siete a diez años de acuerdo al artículo 174, a la persona que:

> *"utilice o facilite el correo tradicional, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad…"*

Además, en el COIP también se castiga a los delitos contra la seguridad de los activos de información.

En el artículo 190 se sanciona como delito de apropiación fraudulenta al sniffing, con entre uno y tres años de cárcel a quien:

> *"utilice fraudulentamente un sistema informático o redes electrónicas para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos modificando o manipulando el funcionamiento de redes electrónicas."*

Para el caso de que alguna persona revele información registrada en un banco de datos que bajo la disposición de alguna ley ésta deba preservarse en secreto, el artículo 229 del COIP menciona que dicha persona será sancionada con pena privativa de la libertad de uno a tres años. En caso de que esta persona esté en ejercicio de un servicio o función pública, sea empleado bancario interno o contratista, será sancionada con pena privativa de la libertad de tres a cinco años.

Según el artículo 230, inciso 2 del COIP, se sancionará con prisión de tres a cinco años a la persona que:

> *"diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes (…), de tal manera que induzca a una persona a ingresar a una dirección o sitio de Internet diferente a la que quiere acceder."*

Además, mediante este mismo artículo en el inciso 3 se sanciona con la misma pena a la persona que:

> *"a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro*

> *dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares."*

Debido a este artículo se sancionan dos de las técnicas más usadas por los delincuentes informáticos en el país, como lo son el phising y el scanning.

De la misma manera se sancionará conforme al artículo 232 con pena privativa de libertad de tres a cinco años a:

> *"la persona que destruya, dañe, borre, deteriore cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen,…"*

En el artículo 233 se sanciona con pena privativa de libertad de tres a cinco años a la servidora o servidor público que, utilizando cualquier medio electrónico o informático, obtenga información clasificada de conformidad con la ley. En caso de que la información revelada por un funcionario público sin la autorización correspondiente, comprometiere la seguridad del Estado, éste será sancionado con prisión de siete a diez años y la prohibición de ejercer un cargo público por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Con lo anteriormente señalado sobre los delitos informáticos, diferenciamos que la ejecución de un CERT es de orden preventivo; mientras que el COIP se encarga de sancionar los delitos cometidos, es decir, es de orden correctivo.

5.5. Libertad de Expresión en Línea.

El gran impacto de Internet en la sociedad mundial como herramienta indispensable para el progreso de los países, originó en los Gobiernos la necesidad de establecer un marco legal adecuado que permita delinear las estrategias para el fortalecimiento de Internet, garantizando sobre todo, el desarrollo de la sociedad. La magnitud de Internet ha provocado que dicho marco legal sea cuidadosamente elaborado, para no negar a la sociedad los derechos que brinda el Internet; por otra parte, para evitar que tanto usuarios como la red estén desprotegidos y sean afectados.

Internet brinda a los usuarios gran cantidad de recursos para acceder a la información y el conocimiento, y para potencializar la libertad de expresión. En el Ecuador no existen estrategias para garantizar la Libertad de Expresión en Línea debido a que las regulaciones no son adecuadas para dicho cometido. Sin embargo, analizaremos el *Reglamento para los Abonados/Clientes-Usuarios de los Servicios de Telecomunicaciones y de Valor Agregado*, que incluye una disposición que podría afectar la Libertad de expresión en Internet; y la *Ley Orgánica de Comunicaciones* que en ciertos artículos menciona los procedimientos que tanto periodistas como usuarios deben seguir para el uso de Internet como medio de comunicación.

5.5.1. Reglamento para los Abonados/Clientes-Usuarios de los Servicios de Telecomunicaciones y de Valor Agregado: Resolución TEL-477-16-CONATEL-2012.

El Consejo Nacional de Telecomunicaciones (CONATEL), en Sesión 16-CONATEL-2012, llevada a cabo el 11 de julio de 2012, aprobó la

Resolución TEL-477-16-CONATEL-2012 que expide el Reglamento para los Abonados/Clientes-Usuarios de los Servicios de Telecomunicaciones y de Valor Agregado; y entró en vigencia el 20 de julio de 2012, una vez que fue publicado en el Registro Oficial # 750.

El artículo 29, numeral 9 del presente reglamento aparentemente atenta con la privacidad de los usuarios de Internet, debido a que exige a los prestadores de servicios de telecomunicaciones y de valor agregado a *"remitir a solicitud de la Superintendencia de Telecomunicaciones (SUPERTEL), información relativa a direcciones IP asignadas a sus abonados/clientes-usuarios"*, en un plazo de noventa días contados a partir de la entrada en vigencia del presente Reglamento.

Esta disposición sin duda alguna genera gran temor en los usuarios ecuatorianos que usan Internet; y podría constituir una amenaza contra la libertad de expresión sobre Internet en nuestro país. La confianza de los ecuatorianos en el uso Internet se ve afectada debido a que sus direcciones IP dejan de ser privadas, ya que la SUPERTEL cuenta con el registro personal de dichas direcciones IP; lo que le permitiría fácilmente, y con el software adecuado, rastrear y monitorear las actividades que realizamos en Internet; puesto que cuando visitamos una página web o realizamos algún comentario en cualquier medio digital en Internet, nuestra dirección IP queda registrada.

Es oportuno citar el llamado de atención sobre el reglamento en mención, en la entrevista realizada por Diario Hoy al Ingeniero José Pileggi, ex presidente del CONATEL. Para el Ing. José Pileggi, *"el acceso al IP, ya sea de parte del Estado o una persona, aunque no pueda acceder a la información, disminuye las defensas del usuario de los servicios de telecomunicaciones y valor agregado"*. ("La entrega del IP", 2012) [55].

El registro de las direcciones IP podría verse afectado, tal y como indica el Ing. José Pileggi, *"todo radica en la discrecionalidad del usuario, no sabemos quién va a manejar toda esta información. Incluso se pueden crear una base de datos en la que conste la dirección IP del cliente y que esta pueda ser mal utilizada".* ("La entrega del IP", 2012) [55].

En la entrevista, el Ing. José Pileggi manifiesta que:

> *"En el campo académico, el tema de investigación personal o institucionalmente debe tener privacidad en el manejo de sus redes. Porque, al entregar sus IP, pueden entrar en sus redes y sustraerse toda la información. Lo mismo es aplicable en temas de índole comercial. Una de ellas es la bancaria: conocer las IP de las entidades financieras es peligroso, porque significa que puede ingresar y vulnerar los sistemas de protección y alterar todo"* ("La entrega del IP", 2012) [55].

El reglamento en mención, abre puertas que en ninguna buena práctica internacional de tecnologías se están ejecutando. Es importante que se aclare lo más pronto posible cuál es la intencionalidad del registro de las direcciones IP para evitar confusiones; sobre todo cuando ya existen otros medios institucionales del Estado para acceder a esa información, como la Función Judicial. ("La entrega del IP", 2012) [55].

El Ing. José Pileggi considera que aunque esta medida ya está dada, sí debe ser revisada, porque *"el propio Gobierno también se puede ver afectado".* Además, se debe tomar en cuenta que *"una dirección IP implica que una información pueda ser rastreada de manera más fácil",* dejando expuesto a los usuarios, ya que antes de llegar a la SUPERTEL, el registro de direcciones IP debe pasar por terceras

personas, que podrían querer acceder a esa información. (“La entrega del IP”, 2012) [55].

Como usuarios de Internet simplemente debemos confiar en que el Estado garantizará la seguridad de este registro de millones de direcciones IP con los datos de cliente, evitando ser divulgados o usados incorrectamente.

5.5.2. Ley Orgánica de Comunicaciones.

La nueva Ley Orgánica de Comunicación fue aprobada por la Asamblea Nacional, el 14 de Junio del 2013; y entró en vigencia el 25 de junio de 2013, una vez que fue publicado en el Registro Oficial # 22. Esta Ley tiene por objetivo desarrollar, proteger y regular el ejercicio de los derechos a la comunicación; y vigilar, controlar e intervenir en los medios de comunicación tradicionales. Debido a la relación que en los últimos años alcanzó Internet con estos medios de comunicación, ha provocado que dentro de esta ley se incluyan casos en el que el mal uso de Internet por parte de los medios, su personal o los usuarios, pueda ser sancionado.

El Artículo 4 de la Ley, garantiza la libertad de expresión en Internet, al mencionar que *“Esta ley no regula la información u opinión que de modo personal se emita a través de internet”,* es decir que los contenidos personales en internet no son controlados. Sin embargo, el artículo resalta que dicha disposición *“no excluye las acciones penales o civiles a las que haya lugar por las infracciones a otras leyes que se cometan a través del internet”; e*sto pretende, que si a través de Internet se atenta contra los derechos de los demás o si se incumple otras leyes

vigentes en el país, no se excluya de culpas y serán sancionados quienes incurran en estos actos.

Cabe mencionar que el artículo 5 de la Ley en mención, hace una definición sobre los Medios de Comunicación Social, en la que consolida la importancia que tiene Internet para dichos medios de comunicación tradicionales, reafirmando que los *"contenidos pueden ser generados o replicados por el medio de comunicación a través de internet".*

Los medios de comunicación tradicionales usan Internet como una herramienta para la interacción con los usuarios, sus páginas web suelen permitir que los usuarios dejen comentarios de la información a la que acceden. Por este motivo, y con la finalidad de librar de responsabilidad a los medios de comunicación, por comentarios de personas particulares realizados en sus páginas web; en el Artículo 20 de la Ley, se enfatiza que:

> *"los comentarios formulados al pie de las publicaciones electrónicas en las páginas web de los medios de comunicación legalmente constituidos serán responsabilidad personal de quienes los efectúen, salvo que los medios omitan cumplir con una de las siguientes acciones:*
>
> 1. *Informar de manera clara al usuario sobre su responsabilidad personal respecto de los comentarlos emitidos;*
> 2. *Generar mecanismos de registro de los datos personales que permitan su identificación, como nombre, dirección electrónica, cédula de ciudadanía o identidad, o;*
> 3. *Diseñar e implementar mecanismos de autorregulación que eviten la publicación, y permitan la denuncia y eliminación de contenidos*

que lesionen los derechos consagrados en la Constitución y la ley".

Definitivamente, con esta disposición el anonimato en línea se ve afectado, y deja de ser el elemento fundamental para la libertad de expresión en Internet. Además, la Ley no establece cómo los medios de comunicación deben gestionar los datos personales que están obligados a solicitar en sus páginas Web, poniendo en riesgo la privacidad de los ecuatorianos en el uso de Internet.

Así también, la Ley exhorta a los medios de comunicación a que *"solo podrán reproducir mensajes de las redes sociales cuando el emisor de tales mensajes esté debidamente identificado".* Si los medios de comunicación no cumplen con esta obligación, *"tendrán la misma responsabilidad establecida para los contenidos publicados en su página web que no se hallen atribuidos explícitamente a otra persona"*. Esto sin duda alguna, obliga a que todos los usuarios asuman su responsabilidad por los contenidos generados en Internet, y garantiza que los medios de comunicación solo reproduzcan contenidos seguros, de fuentes y personas confiables, pero esto también podría ser considerado por algunas personas como una restricción a su derecho a la libertad de expresión.

Las disposiciones descritas en el artículo 20 son los aspectos más polémicos de la Ley, y resulta importante mencionar que organismos internacionales y medios de comunicación de América y del mundo se han visto alertados sobre la posible afectación del derecho a la libertad de expresión en Ecuador. A pesar de estos intentos de censura, Internet sigue siendo la herramienta más utilizada por los ecuatorianos para expresar su opinión.

Para la Magíster en Comunicación Pública de Ciencia y Tecnología, Lady Rodríguez:

> *"El análisis conjunto de los artículos 5, 18, 19 y 20 permite establecer que puede configurarse una amenaza a la privacidad y protección de datos de los usuarios de Internet, aunque no en las redes sociales, pero sí en los medios de comunicación social en línea. En algunos Estados los gobiernos han esgrimido la salvaguarda de la seguridad interna del país como justificación de medidas de filtraje, identificación y represión de ciberciudadanos y en el bloqueo de las versiones en línea de los medios de comunicación social".* (Rodríguez, 2013, p. 117) [52].

De la misma manera es importante resaltar que el 28 de junio del 2013 se presentó ante la Corte Constitucional una demanda de inconstitucionalidad de la Ley Orgánica de Comunicación, la cual se encuentra en trámite (Rodríguez, 2013, p. 117) [52].

Siendo recién el 23 de enero de 2014 cuando *"la Corte Constitucional del Ecuador admitió a trámite la acción de inconstitucionalidad contra la Ley Orgánica de Comunicación (LOC) que plantearon 60 ciudadanos. Sin embargo, la Corte negó las medidas cautelares solicitadas por considerarlas improcedentes".* (Fundamedios, 2014) [56].

Finalmente, en la investigación de la Magíster Lady Rodríguez sobre la Ley Orgánica de Comunicación, para ella:

> *"Es oportuno mencionar que en la evaluación sobre el estado de la libertad de expresión en Ecuador contenida en 30 páginas en el Informe Anual 2012 de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de*

> *Derechos Humanos (CIDH), se establece que existe un caso que tiene relación con la libertad de expresión en línea. La observación No. 195 manifiesta que la relatoría Especial ha sido informada que el Secretario Nacional de Comunicación mediante misiva enviada a diario El Comercio le habría advertido el 18 de septiembre del 2012 sobre su intención de iniciar investigaciones penales en razón de comentarios publicados en la versión online del diario, y que se "reservaba el derecho de solicitar la información de las personas cuyos comentarios pueden ser difamatorios, ofensivos o lesivos y que puedan configurar en algún delito, para lo cual la justicia será la que determine la responsabilidad de la persona y de ser el caso el resarcimiento por los daños y perjuicios ocasionados". A raíz de esta comunicación, el diario El Comercio habría suprimido la opción de comentarios en su sitio Web".* (Rodríguez, 2013, p. 117) [52].

5.6. Protección de niños en línea.

Internet ofrece una infinidad de posibilidad por realizar, y muchos de sus contenidos resultan atractivos para los niños, motivándolos a acceder a la red de Internet con mayor frecuencia. Aunque Internet les permite a los niños interactuar con amigos, jugar y realizar proyectos escolares, también tiene contenidos con imágenes y lenguaje no adecuados para el acceso de los niños.

El Gobierno Ecuatoriano a través del *Reglamento para los Abonados/Clientes-Usuarios de los Servicios de Telecomunicaciones y de Valor Agregado,* establece estrategias que garantizan el *"acceso,*

seguridad, contenidos y aplicaciones destinados a público adulto, niñas, niños y adolescentes". En el artículo 38 de dicho reglamento, se protege a los menores de edad de un posible mal uso de las telecomunicaciones, y se evita que puedan acceder a contenidos para adultos. Por ello, se exhorta a quienes prestan los servicios de acceso, descarga, recepción o cualquier modalidad de prestación de contenido dirigido a público adulto a ser los responsables exclusivo de dicho control; y se les exige la incorporación de *"mecanismos de control para verificar que estos servicios sean prestados exclusivamente a personas adultas, previa solicitud expresa, así como proveer dichas facilidades o servicios en horarios específicos de acceso a contenido de adultos".*

Cabe señalar que últimamente, los casos de niños que sufren ataques por otros menores de edad a través de mensajes de SMS e Internet, o conocido como *"ciberbullying"*, se ha convertido en uno de los principales problemas que afectan a los menores en el uso de las TICs. Es importante resaltar que *"Roberto Martínez, analista de 'malware' para Kaspersky Lab en América Latina, se refiere al ciberbullying como una forma de amenazar, avergonzar, intimidar y criticar a una persona a través de los medios tecnológicos",* según lo menciona Diario El Comercio ("El 'bullying' se viraliza", 2013) [57].

El ciberbullying en Ecuador se ha ido masificando y cada vez son más los niños que sufren el acoso a través de las redes sociales, correo electrónico y sitios web.

Podemos evidenciar este problema en el artículo periodístico *"El 'bullying' se viraliza en la Internet"* publicado por Diario El Comercio ("El 'bullying' se viraliza", 2013) [57], el cual hace referencia a:

> *“un estudio realizado por Programas Educativos Psicología y Salud (Proeps), con estudiantes de centros educativos de Pichincha, revela que 252 de 700 mujeres (36%) entre octavo de básica hasta tercero de bachillerato han sido acosadas por Internet. También, 171 varones de 500 (31%) afirmaron ser víctimas de ciberbullying.*
>
> *Napoleón Vásquez, director de Proeps, recalca que la principal plataforma de ataque es Facebook”.*

Además, el artículo citado, menciona que:

> *“según un estudio de la Organización de las Naciones Unidas, al menos el 50% de los jóvenes latinoamericanos ha sido víctima de acoso por Internet”; pero “en Ecuador, un estudio del Observatorio de la Niñez y Adolescencia del 2010 mostró que más del 60% de los niños o adolescentes ecuatorianos ha sido víctima del ciberbullying”.*

Esto pone en evidencia que el problema de ciberbullying en nuestro país está por encima de los otros países de la región, debido a la falta de estrategias gubernamentales tanto en la educación como en la ciberseguridad.

Es importante que los padres de familia sean quienes protejan a los niños contra los peligros de Internet. Los padres deben supervisar y controlar tanto las actividades que realizan, como las personas que conocen, y educarles sobre los riesgos del ciberespacio y de la información y datos personales que comparten por Internet.

5.7. Participación del Ecuador en los foros para la Gobernanza de Internet.

La Gobernanza de Internet en el Ecuador, es un tema que tiene aún mucho por debatirse. Las Políticas Públicas para la gestión de Internet son insuficientes, o en muchos de los casos no existen las medidas adecuadas que garanticen los objetivos que exige la Gobernanza de Internet.

Si analizamos la situación de las participaciones del Ecuador en los Foros para la Gobernanza de Internet, según la SUPERTEL, *"la participación ecuatoriana en los espacios de Gobernanza de Internet tiene el mismo matiz que la gran mayoría de participaciones de países subdesarrollados o en vías de desarrollo".* Resulta ser que las participaciones son *"principalmente individuales motivadas por diversos intereses profesionales que al ser personales y generalmente financiadas por los mismos participantes, se dan con mayor o menor intensidad de acuerdo a las condiciones particulares de la persona".* Esto sin duda alguna no representa *"una verdadera presencia nacional"* en los Foros para la Gobernanza de Internet. (Revista SUPERTEL No. 14, 2012, p. 19) [58].

Cabe resaltar que en Ecuador existen instituciones que cuentan con recursos humanos, tecnológicos y económicos suficientes para convertirse en integrantes importantes para la gestión nacional de Internet; y profesionales con un alto nivel de conocimientos y amplia experiencia en participaciones nacionales e internacionales de Gobernanza de Internet.

A pesar de que en Ecuador hay todavía mucho por hacer en materia de Gobernanza de Internet, para la SUPERTEL, *"la participación*

ecuatoriana en los foros y debates de Internet no ha dejado de ser importante y relevante en varios casos". (Revista SUPERTEL No. 14, 2012, p. 20) [58].

Cabe destacar que el Ecuador organizó del 6 al 11 de mayo del 2012, la reunión LACNIC XVII en Quito, *"el evento de más importante de la Región de América Latina y el Caribe, con connotación mundial".* Para traer este evento al Ecuador, se necesitó del esfuerzo del *"Comité Organizador local"* que fue encabezado por la SUPERTEL y con la activa participación de la Corporación Ecuatoriana de Comercio Electrónico y la Sociedad de Internet del Ecuador. El LACNIC XVII contó con la asistencia de decenas de delegados nacionales e internacionales, y fue la oportunidad propicia para que Ecuador concretara sus postulados constitucionales e impulsara *"la Sociedad de la Información con acuerdos pragmáticos entre todos los actores sociales, empresariales y gubernamentales, con el fin legítimo de lograr un desarrollo social, económico y cultural, homogéneo, integral y justo".* (Revista SUPERTEL No. 14, 2012, p. 20) [58].

La organización de estos eventos regionales en Ecuador es de suma importancia porque permite que los sectores estratégicos de nuestro país se interesen en participar en la gestión nacional de Internet.

Finalmente, la organización de reuniones de transcendencia tanto nacional, regional y mundial en Ecuador, permite que nuestro país se involucre con mayor presencia en las decisiones que se toman en los Foros Internacionales para la Gobernanza de Internet, y hacer de nuestra presencia una nueva condición para generar más opciones en la Gestión de Internet, contribuyendo también al desarrollo tecnológico, económico y social del país.

5.8. Transición de iPv4 a iPv6 en Ecuador.

El protocolo IPv4 ha permitido el funcionamiento de Internet en todas las regiones del Mundo desde hace más de 30 años. La administración de las direcciones IP ha sido manejada de forma jerárquica, la IANA (“Internet Assigned Numbers Authority”) es la entidad principal encargada de administrar todo el espacio de direccionamiento disponible a nivel global y distribuir bloques de direcciones a organizaciones regionales denominadas RIRs (“Regional Internet Registry”) de acuerdo a la demanda existente; y éstas a su vez se encargan de la asignación a los proveedores de Internet. La RIR para la región de América Latina y Caribe es la Asociación Latinoamericana y del Caribe para el Registro de Direcciones en Internet (LACNIC).

Debido al uso y éxito inimaginable que llegó a tener Internet a nivel global, las direcciones IPv4 disponibles en la IANA se agotaron definitivamente en febrero de 2011. Sin embargo; en la década de los 90, la IETF (“Internet Engineering Task Force”) creó IPv6 para dar solución a la necesidad creciente de direcciones. Esta nueva versión de IP usa direcciones de 128 bits, lo que permite tener más de 340 sextillones de direcciones disponibles. Esta cantidad de direcciones IP resulta ser suficiente para la importante demanda de servicios y usuarios futuros, permitiendo también, que millones de dispositivos tengan su propia identificación IP y puedan comunicarse entre sí. Además, este protocolo introduce nuevas funcionalidades y mejoras en la seguridad de las redes y servicios de Internet.

Para la transición a esta nueva versión de protocolo IP es necesario contar con los mecanismos técnicos adecuados y las políticas públicas correctas. Dicha transición es realizada de manera que las dos versiones de IP coexistan hasta lograr una completa implementación de

la IPv6 periódicamente a nivel mundial según el desarrollo de las regiones y su necesidad.

Según la SUPERTEL (Revista SUPERTEL No. 14, 2012, p. 10) [58], *"la transición a IPv6 en Ecuador inició el 8 de abril de 2012 cuando fueron asignados Bloques IPv6 al país".*

La situación de la implementación de IPv6 en Ecuador cuenta con:

- *"23 bloques IPv6 asignados/distribuidos por LACNIC a organizaciones ecuatorianas*
- *12 bloques utilizados (vistos en el Internet Global)*
- *11 organizaciones diferentes utilizan prefijos IPv6".*

La oferta de servicios con soporte de IPv6 en Ecuador:

- *"ISPs que pueden proveer tránsito IPv6 nativo: 3*
- *ISPs que proveen servicio HOME con soporte IPv6 nativo: 0*
- *El punto de intercambio de tráfico local de Internet (NAP.EC) tiene IPv6 nativo habilitado.*
- *El dominio .EC tiene un servidor con IPv6 fuera del Ecuador y otro en NAP.EC. NIC.EC acepta registros AAAA para dominios .EC".*

Las páginas locales con soporte IPv6 al momento son:

- *"www.aeprovi.org.ec*
- *www.ipv6tf.ec*
- *www.cedia.org.ec*
- *Páginas de algunas universidades ecuatorianas (listado en ipv6tf.ec)"*

Además, la SUPERTEL enfatiza que *"la transición a IPv6 dentro del territorio ecuatoriano requiere mayor difusión y capacitación".* Así también, menciona que el liderazgo de la IETF fue delegado en el Ecuador, al MINTEL y sus acciones han sido posibles gracias al apoyo principal de AEPROVI y NIC.EC. AEPROVI por iniciativa propia creó la Fuerza de Trabajo de IPv6 de Ecuador (IPv6TF-EC), con la finalidad para contribuir con esta transición a IPv6. (Revista SUPERTEL No. 14, 2012, p. 11) [58].

Según la SUPERTEL (Revista SUPERTEL No. 14, 2012, p. 11-12) [58], este grupo de trabajo tiene los siguientes objetivos:

- *"Ser fuente de información relacionada con el Protocolo de Internet versión 6 (IPv6).*
- *Coordinar labores de capacitación y difusión sobre IPv6.*
- *Coordinar los esfuerzos de los diferentes actores del Internet ecuatoriano para una eficaz y pronta adopción del IPv6.*
- *Fomentar el uso de IPv6.*
- *Establecer permanente comunicación e identificar oportunidades de colaboración con los Grupos de Trabajo de otros países y regiones.*
- *Elaborar un plan de acción para la implementación de IPv6 en el país y propiciar su uso".*

El IPv6TF-EC no es una persona jurídica, es simplemente un grupo de trabajo con participación abierta sobre IPv6 en Ecuador, que busca incentivar la participación del gobierno nacional, el sector industrial, sector educativo y de los usuarios ecuatorianos entorno a este tema.

Cabe mencionar, que el MINTEL en su obligación de diseñar políticas y mecanismos técnicos para una transición ordenada y adecuada,

garantizando el avance tecnológico en el País, emitió el Acuerdo N° 0133 del 25 de marzo del 2011, el cual exhorta a las instituciones y organismos del Ecuador para que *"en los nuevos procedimientos de contratación de equipamiento tecnológico, productos y aplicaciones que utilicen el Protocolo de Internet tengan como exigencia primordial el soporte y compatibilidad con IPv6"*.

Además, mediante el Acuerdo N° 007-2012 publicado en el Registro Oficial # 608 del 18 de enero del 2012, el MINTEL emitió *"lineamientos de política pública vinculados con la incorporación de IPv6 en sitios web y aplicativos del sector público, en el ccTLD.ec y en el curso normal de tráfico IPv6 en las redes de ISPs y Portadores".* Acordando los siguientes artículos:

> ***"****Artículo 1: Requerir a las Instituciones y Organizaciones del Sector publico señalados en el Art. 225 de la Constitución de la República del Ecuador, que implementen en sus sitios web y plataformas de servicios electrónicos, el soporte y compatibilidad con el protocolo IPv6 de manera coexistente con el protocolo IPv4, con la finalidad de generar tráfico IPv6 a nivel nacional y permitir que dichos recursos públicos sigan siendo visibles desde el resto del mundo, dado que en algunos países ya se está empezando a utilizar IPv6.*
>
> *Artículo 2: Requerir a la Secretaría Nacional de Telecomunicaciones SENATEL, que en el plazo de 60 días contados a partir de la fecha de publicación del presente acuerdo, coordine los procedimientos administrativos y normativos necesarios para asegurar y garantizar la incorporación y correcto funcionamiento del protocolo IPv6 en el sistema de nombres de dominio bajo el código de país .ec, la*

misma calidad que los servicios ofrecidos con IPv4, y sin incremento de costes para los usuarios.

Artículo 3: Requerir a la Secretaría Nacional de Telecomunicaciones SENATEL, que ejecute las acciones y procedimientos administrativos y normativos necesarios con el fin de que los Proveedores de Servicio de Internet ISPs y portadores nacionales, admitan en sus redes, plataformas y sistemas el curso norma de tráfico de IPv6 en coexistencia con IPv4.

Artículo 4: Requerir a la Secretaría Nacional de Telecomunicaciones SENATEL, que ejecute las acciones necesarias con el fin de que los Proveedores de Servicio de Internet (ISPs), establezcan sus planes de direccionamiento, y en función de los mismos, inicien los trámites para la solicitud de recursos de direccionamiento (direcciones IP) IPv6".

Dicho acuerdo exige como Disposición Transitoria que:

"en el plazo de 90 días contados a partir de la publicación del presente acuerdo, el Ministerio de Telecomunicaciones y de la Sociedad de la Información publicará un plan de compras de equipamientos ICT con soporte IP para las entidades del sector público, el cual servirá como marco de referencia en los procesos de adquisiciones de infraestructura para garantizar el adecuado soporte IPv6"

Cabe destacar que el MINTEL mediante Acuerdo N° 039-2012 publicado en el Registro Oficial # 805 del 4 de junio del 2012, define un *"Plan Nacional para la implementación del IPv6 en el Ecuador"*, tal y como lo contempla la meta 4 del Plan de Acción eLAC2015, que:

> *“insta a los países miembros a colaborar y trabajar en forma coordinada con todos los actores regionales, para que la región logre un amplio despliegue del Protocolo de Internet versión 6 (IPv6), así mismo hace un llamado a implementar con brevedad planes nacionales que permitan acceder a los portales de servicios públicos gubernamentales de los países de la región a través de IPv6 y que las redes estatales trabajen de forma nativa con IPv6”.*

Según este Acuerdo, al ser el MINTEL el órgano rector en la transición de los protocolos, es necesario que coordine con las entidades del sector público la coexistencia de los protocolos IPv4 e IPv6.

En ejercicio de sus atribuciones, acordó los siguientes dos artículos:

> ***“****Artículo 1: Aprobar las siguientes estrategias de acción para el fomento en la adopción y coexistencia de los protocolos IPv4 e IPv6 en todo el territorio nacional bajo las siguientes estrategias:*

1. *El proceso de incorporación y adopción del Protocolo de Internet IPv6 en Ecuador, será impulsado por el MINTEL, dentro del programa de Recursos de Banda Ancha, que forma parte del Plan Nacional de Banda Ancha.*
2. *Las Instituciones y Organismos del Sector Público deberán realizar las gestiones necesarias para que implementen sus sitios web y plataformas de servicios electrónicos, con el soporte y compatibilidad con el protocolo IPv6 de manera coexistente con el protocolo IPv4, en el plazo de un año contado a partir de la entrada en vigencia del presente acuerdo.*

3. *Las empresas públicas de telecomunicaciones, realizarán las acciones que correspondan, para que en el plazo de 45 días contados a partir de la publicación del presente acuerdo, admitan en sus redes, plataformas y sistemas el curso normal de tráfico de IPv6 nativo en coexistencia con IPv4.*
4. *Incorporación del protocolo IPv6 de forma coexistente con IPv4 en los sitios Web www.mintel.gob.ec, y www.conatel.gob.ec así como en las plataformas de servicios electrónicos asociadas a los portales web tanto del Ministerio de Telecomunicaciones y de la Sociedad de la Información como del Consejo Nacional de Telecomunicaciones y Secretaría Nacional de Telecomunicaciones.*
5. *El MINTEL organizará talleres, charlas, foros y jornadas teórico-prácticas sobre aspectos técnicos IPv6, de carácter gratuito a los largo del territorio nacional, con participación de expertos internacionales con amplia experiencia en el despliegue real de IPv6.*
6. *El MINTEL en el plazo de 90 días contados a partir de la publicación del presente acuerdo, publicará el "Plan de recursos y adquisiciones de tecnología con soporte IPv6", el cual servirá como marco de referencia para inclusión del nuevo protocolo en los procesos de adquisición de infraestructura, servicios, y aplicaciones para garantizar el adecuado soporte de IPv6 tanto en el sector público como privado.*

Artículo 2: El MINTEL se encargará del seguimiento y monitoreo respecto al cumplimiento del presente acuerdo".

Finalmente, la Superintendencia de Telecomunicaciones (SUPERTEL), es la institución encargada de controlar el proceso de transición de IPv4

a IPv6. Dicha institución junto al MINTEL, deberán elaborar parámetros técnicos adecuados para hacer posible el proceso de transición y posterior migración a IPv6. Y con el fin de garantizar la implementación tecnológica debe supervisar el tipo de infraestructura que tendrán que emplear las ISPs.

El Estado ecuatoriano garantiza el acceso universal a las tecnologías de la información desde la Constitución que tiene supremacía en la política ecuatoriana. Los lineamientos de la Gobernanza de Internet en el Ecuador tratan de seguir las recomendaciones del FGI, aunque no ha existido una verdadera participación nacional en las reuniones del FGI.

Para la transición del protocolo IPv4 a IPv6 en Ecuador, ya se ha comenzado a implementar estrategias de acción como la elaboración de parámetros técnicos para la implementación tecnológica y la incorporación del protocolo IPv6 en los portales web de la Instituciones y Organismos del Sector Publico.

El gobierno ecuatoriano asumió la responsabilidad de ser el encargado de brindar acceso a las TICs a las zonas rurales y marginales mediante los Infocentros Comunitarios y Aulas Móviles que corresponden a la Estrategia Ecuador Digital 2.0., cumpliendo con los objetivos que plantea el FGI.

Al analizar la situación de la libertad de expresión en Línea, podríamos mencionar las medidas gubernamentales que podrían afectar a los usuarios ecuatorianos, como el reglamento de abonados que no aclara la intencionalidad del registro de las direcciones IP, y la Ley Orgánica de Comunicación que estable acciones de identificación en las páginas web de los medios de comunicación. Esto sin duda alguna puede

configurarse como una amenaza a la privacidad o a la libertad de expresión en Línea según sea el caso.

Por otra parte, en Ecuador se sancionan los delitos informáticos según el Código Orgánico Integral Penal, castigando los delitos como el phising, scanning y el sniffing. Además, se pretende identificar y prevenir este tipo de delitos mediante el CERT planificado por la SUPERTEL, que aún no ha sido culminado en todas sus fases.

CAPÍTULO 6:

PLAN DE ACCIÓN PARA GARANTIZAR LA GOBERNANZA DE INTERNET EN ECUADOR.

El análisis de la Gobernanza de Internet en Ecuador refleja los intentos del Gobierno nacional por lograr el desarrollo armónico de la Sociedad de la Información e Internet. Aunque no existe un marco legal eficiente, incluyente y flexible para la gestión de Internet en el Ecuador, las estrategias que implementa el Gobierno nacional buscan siempre garantizar a los usuarios ecuatorianos el uso seguro de Internet pero en ocasiones, aquellas estrategias afectan a otros derechos.

El *Plan de Acción para garantizar la Gobernanza de Internet en Ecuador* que se propone en el presente estudio, tiene como objetivo incorporar nuevos compromisos en la gestión de Internet para mejorar las estrategias y políticas públicas que están en vigencia en el país, a fin de colaborar con el Gobierno

nacional a alcanzar los objetivos propuestos contenidos en el Plan del Buen Vivir y la Estrategia Ecuador Digital 2.0, sin afectar a ningún derecho de los usuarios de Internet que son protegidos por el FGI.

Este Plan de Acción tiene como meta la elaboración de estrategias para estructurar un Marco Legal adecuado para el desarrollo de la Gobernanza de Internet en Ecuador. Se proponen un conjunto de medidas que permitan incluir la colaboración de múltiples entidades y organizaciones nacionales tanto públicas como privadas, que son claves para dar cumplimiento a las estrategias del Plan.

Es importante mencionar que el Plan de Acción requiere la participación principal del Gobierno nacional junto con el MINTEL, debido a que son ellos quienes pueden incorporar las estrategias de este documento en sus propuestas y acciones de corto y largo plazo, con el fin de contribuir a la Gobernanza de Internet en el Ecuador.

6.1. Estructura del Plan de Acción.

El *Plan de Acción para garantizar la Gobernanza de Internet en Ecuador*, propone estrategias y medidas que refuercen los Planes Estatales actuales sobre el desarrollo de Internet en el país.

El Plan de Acción combina estrategias para la implementación de infraestructuras de hardware y software, así como también medidas legales para garantizar la correcta gestión de Internet en Ecuador. Por ello, es importante mencionar que se pretende que este Plan de Acción contemple un periodo de ejecución desde este mismo año 2014 hasta el año 2020, tiempo en el cual, la Gobernanza de Internet en Ecuador contemplaría un sólido Marco Legal, de manera que permitiría que el

país siga correctos lineamientos en el futuro, adaptándose a la evolución de Internet y a los cambios en la gestión del mismo.

Las medidas legales que el Estado ecuatoriano debería implementar según el Plan, tienen un alcance a corto plazo; se pretende que hasta el año 2015 la estructura legal del país esté delineada para lograr cumplir con el Plan de Acción mencionado. Sin embargo, el despliegue de la infraestructura para la red de Internet en Ecuador debería llevarse a cabo hasta el año 2020, tiempo límite de la ejecución del Plan.

Las estrategias y medidas del *Plan de Acción para garantizar la Gobernanza de Internet en Ecuador* se organizan de la siguiente manera:

Figura 6.1: Organigrama del Plan de Acción para la gobernanza de Internet en Ecuador.

6.1.1. Eje de Implementación Tecnológica.

Mediante este Eje pretendemos que Ecuador cuente con acceso a la red de Internet de manera eficiente, moderna y segura; priorizando el beneficio para todos los ecuatorianos. Además, se pretende incentivar la participación activa de todas las partes interesadas en lo que respecta a la Gobernanza de Internet de nuestro país; y así aportar y adoptar experiencias con los demás países en la gestión de Internet.

6.1.1.1. Creación de un grupo de trabajo para la gobernanza de Internet.

El Estado ecuatoriano debería tomar medidas que le permitan tener una participación activa en la gestión de Internet. Debería existir un *"Grupo de Trabajo"* encabezado por el MINTEL, con profesionales expertos en Gobernanza de Internet que con sus conocimientos y experiencia permitirán no solo asegurar la presencia del Ecuador en los Foros Internacionales para la Gobernanza de Internet, sino garantizar la permanencia y continuidad del país en el FGI.

Es importante que el *Grupo de Trabajo* involucre también a las Instituciones interesadas, sean éstas privadas, públicas o universidades, en la gestión de Internet en el Ecuador. La consolidación de todos los sectores estratégicos del país logrará que nuestras futuras participaciones en el FGI sean relevantes, y que además nos convierta en una de las naciones protagónicas en la gobernanza de Internet de la Región e incluso a nivel mundial.

De la misma manera, el gobierno ecuatoriano debería elaborar estrategias siguiendo los lineamientos, objetivos y recomendaciones del FGI. Es importante que las estrategias y el *Grupo de Trabajo*

mencionado anteriormente, estén guiados al único objetivo de alcanzar una solidez en los temas Gobernanza de Internet, para que tanto los sectores estratégicos gubernamentales como la Sociedad Civil alcancen la madurez necesaria, con la finalidad de implementar políticas públicas buscando lograr el acceso universal a Internet de manera equitativa e integral, principalmente garantizando la seguridad de la red y los usuarios.

6.1.1.2. Despliegue de nuevas redes para Banda Ancha móvil y fija.

Todos los ecuatorianos tenemos derecho de tener una infraestructura robusta de la red de Internet que nos permita el acceso fijo y móvil a una verdadera banda ancha, y mecanismos adecuados que nos facilite el uso Internet de manera segura.

Podemos notar que la infraestructura de nuestro país carece de modernización y requiere del despliegue de nuevas redes con cobertura nacional. Resulta necesario que el Gobierno Nacional impulse mecanismos para gestionar la conexión del país a nuevas redes de fibra óptica internacional con gran capacidad de Banda Ancha, con la finalidad de incrementar el acceso de Ecuador a las redes de Internet internacionales, y permitiendo implementar un backbone nacional mucho más robusto con verdaderas autopistas de información cubriendo todo el territorio nacional.

La Figura 6.2 muestra la estructura para garantizar el despliegue de nuevas redes de banda ancha fija y móvil.

Figura 6.2: Estructura para el despliegue de nuevas redes de banda ancha.

Para el despliegue de nuevas redes para Banda Ancha fija, el Gobierno Nacional debería gestionar el aterrizaje de nuevos cables submarinos en el Ecuador de manera inmediata, permitiendo que máximo hasta finales del año 2017 se alcance la conexión internacional del país a redes de Internet con grandes velocidades.

El Gobierno ecuatoriano debería ampliar la infraestructura de la red troncal de fibra óptica nacional, permitiendo de esta manera la existencia de nuevas rutas con topología de anillo para llevar acceso a Internet a todos los rincones de la patria, especialmente a los lugares más remotos del país donde el acceso es inexistente.

De la misma manera es necesario, no sólo por parte del Gobierno sino también por parte de los Gobiernos seccionales y la empresa privada, lograr la implementación del sistema de fibra en el lazo (Fiber In The Loop - FITL) en todas las ciudades del país con la finalidad de proveer servicios residenciales de mayor calidad. Los gobiernos seccionales deberían ser los encargados de juntar a las empresas proveedoras de servicio de Internet, y conjuntamente realizar de manera planificada los

ductos urbanos para el soterramiento de los cables de telecomunicaciones con el fin de ordenar y proteger las redes de telecomunicaciones. Además, con ello se lograría también descontaminar visualmente a las ciudades de los tendidos aéreo de cables, contribuyendo a la modernización que buscan alcanzar todas las ciudades del Ecuador.

Siendo consecuentes con el crecimiento de las redes nacionales y las redes locales de fibra óptica, es importante que el servicio de banda ancha fija pueda llegar por fibra hasta nuestros hogares, implementando las redes FTTH (Fiber To The Home). Es necesario que la inversión nacional y de la empresa privada permita la modernización completa de toda la infraestructura de la red de Internet, para que de esta manera los usuarios ecuatorianos sean beneficiados al recibir una verdadera Banda Ancha.

Asimismo, es necesario que el Gobierno asigne espectro a las operadoras móviles privadas de Telecomunicaciones actuales o entrantes, adicionales a las que ya fueron asignadas a la Corporación Nacional de Telecomunicaciones (CNT E.P.), permitiendo a dichas operadoras dar también servicio de Banda Ancha móvil 4G. De esta manera, los ecuatorianos contamos con otras alternativas de acceso a la web a gran velocidad.

Es importante que el Gobierno también redefina la velocidad del servicio de Internet para los usuarios; una Banda Ancha mínima de 10 Mbps resulta conveniente para nuestro país aunque esta velocidad resulte ser menor a las que ofrecen otros países. Hasta el año 2020 la cobertura de Banda Ancha en el país debería alcanzar un 100% de la población.

La implementación de la infraestructura en el país debería ir de la mano con una regulación nacional que no sólo facilite el acceso a las autopistas de información a todos los ecuatorianos desde cualquier lugar del Ecuador, sino que además garantice la innovación de nuevas tecnologías, incluya la participación de los usuarios en la evolución de la red y de la sociedad de la Información, y permita el crecimiento constante de la infraestructura nacional, aumentando la velocidad del servicio y reduciendo el costo del acceso para el usuario.

6.1.1.3. Agilidad en la implementación del Protocolo IPv6 en Ecuador.

La transición del protocolo IPv4 a IPv6 en nuestro país aún no ha empezado a desarrollarse, son pocas las medidas gubernamentales que garantizan la transición del IP, y sólo son unas cuantas instituciones las que han implementado el IPv6 en sus páginas Web. Por ello, es importante la creación de un *"Grupo de Trabajo e Investigación*" que en primera instancia sea el encargado de coordinar la transición del protocolo IP en el Ecuador, para luego ser el gestor técnico de Internet en el país y esté pendiente del constante desarrollo de los aspectos técnicos de Internet en el Ecuador.

El Grupo debería estar conformado por el Estado y la empresa privada, entrando en funcionamiento este mismo año 2014 para no retrasar más el desarrollo de las estrategias que ya fueron dispuestas por el Gobierno, pero que aún no han sido implementadas. Luego debería elaborar las estrategias más convenientes para lograr con éxito la transición del IPv4 a IPv6 en el país, en el período que establezcan los entes internacionales encargados de controlar dicha transición.

6.1.1.4. Programa Nacional de Ciberseguridad.

El establecimiento de un clima de confianza en el ámbito digital es imprescindible para que las TICs contribuyan al desarrollo económico y social del país; conseguirlo es una tarea compleja que corresponde al Estado, empresas públicas y privadas de telecomunicaciones y la sociedad en general.

Ecuador debería elaborar una Estrategia Nacional de Ciberseguridad según sus capacidades nacionales, necesidades y amenazas, tal como lo recomienda la UIT; siendo una estrategia basada en los valores nacionales para que gane el apoyo de los interesados, como el poder judicial y el sector privado.

De la misma manera, este año 2014 se debería llevar a cabo la ejecución de las fases planificadas para la implementación del CERT por parte de la SUPERTEL que estaban previstas a ser culminadas para fines del 2012. Es de suma importancia contar con este Centro de Respuesta Inmediata en el país para poder identificar, gestionar y responder a las ciberamenazas que afectan a los usuarios ecuatorianos. Por ello, la SUPERTEL debería poner en total funcionamiento el CERT para el año 2015.

El Estado debería crear también un programa de excelencia en ciberseguridad, siguiendo el modelo de países europeos. Es necesario formar talentos en ciberseguridad para que estos profesionales puedan incorporarse a los centros de respuesta inmediata, realizar investigación avanzada y estar capacitados para formar a otros profesionales.

6.1.2. Eje de Estrategia Política.

En el Eje de Estrategia Política se espera, por parte del gobierno nacional, la inclusión de incentivos económicos tanto para las empresas proveedoras de servicio de banda ancha, como para los usuarios, con la finalidad de garantizar que el acceso a las TICs esté al alcance de todos los ecuatorianos, permitiendo no sólo incrementar la densidad de conexiones de banda ancha fija y móvil sino también la posibilidad de adquisición de modernos equipos terminales.

6.1.2.1. Regulación de precios del servicio de Internet.

El Gobierno debería evaluar los precios del servicio de Internet en el mercado nacional, debido a que sus precios resultan elevados con respecto al ancho de banda y a la calidad que se oferta. Para ello, es indispensable que la SENATEL regule las tarifas en los precios del servicio de Internet, debido que al momento, no existe dicha regulación en la tarifación de la Banda Ancha en nuestro país. Esto ha provocado que las empresas con mayor presencia en el mercado implanten sus condiciones afectando el derecho a la libre competencia.

La SENATEL debería fijar *"techos tarifarios"* para banda ancha tanto fija como móvil, tal y como se hace en el servicio de telefonía. Además, se debería reducir en un 40% el precio actual del Kbps. Estas medidas deberían ser acogidas inmediatamente, con el objetivo de proteger principalmente al usuario de los elevados precios del servicio que actualmente se ofertan, y para garantizar que todas las empresas brinden la misma calidad de servicio con iguales condiciones de tarifación, permitiendo mantener la libre competencia del mercado siendo los usuarios nuevamente beneficiados.

6.1.2.2. Subsidio del servicio de Internet.

El precio para poder acceder a Internet es mayor en los países en vías de desarrollo que los países desarrollados; lo cual llama la atención debido a que el nivel de vida en los países en vías de desarrollo, como es el caso de Ecuador, dificulta que la mayoría de los habitantes puedan contar con este servicio. Por lo tanto, se debería implementar medidas que se ajusten a la realidad de nuestro país.

A pesar de que una de las propuestas del presente Plan de Acción es la interconexión del país a más redes de fibra óptica internacionales, lo cual reduce el precio a los usuarios de Internet, el Gobierno debería implementar otro tipo de soluciones que ayuden directamente a las personas que por su nivel de vida, les resulta difícil acceder al servicio de Internet.

La Figura 6.3 representa el ciclo que se determina en este estudio al subsidiar el costo de Internet para los sectores socio-económicos bajos en el país:

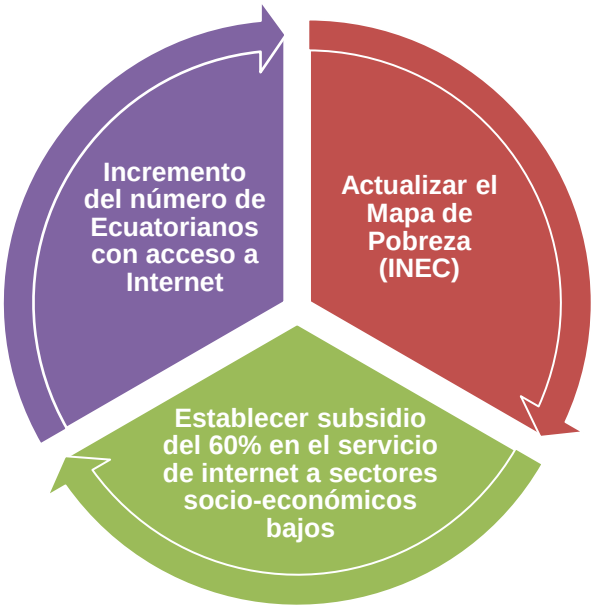


Figura 6.3: Ciclo al subsidiar el servicio de Internet.

Para el efecto es necesario que el INEC actualice el mapa de pobreza donde se establezca la ubicación de los sectores con menor nivel económico del país. Con esta información, el Gobierno debería a corto plazo gestionar el subsidio para que todos los ecuatorianos sean parte del acceso universal a Internet.

La solución gubernamental al problema que se propone es implementar un subsidio estatal de mínimo el 60% del costo del servicio de Internet para los usuarios de los sectores con un nivel socio-económico bajos.

Con estas medidas se pretende incentivar que los habitantes de los sectores en mención, adquieran el servicio de Internet en sus hogares; y de esta manera seamos más los ecuatorianos con acceso a la red.

6.1.2.3. Exoneración de impuestos arancelarios a equipos terminales con acceso a Internet.

Para lograr el completo desarrollo de Internet en Ecuador es importante también tener una gran capacidad de innovación tecnológica con el fin de lograr la masificación del uso de Internet a través de modernos equipos terminales.

Para mejorar la penetración de equipos terminales con acceso a Internet, el Gobierno ecuatoriano debería cambiar las estrategias políticas y económicas principalmente entorno al impuesto arancelario que afecta a los productos tecnológicos que ingresan al país.

La Figura 6.4 muestra el impacto que produciría la reducción de impuestos arancelarios a equipos terminales con acceso a Internet.

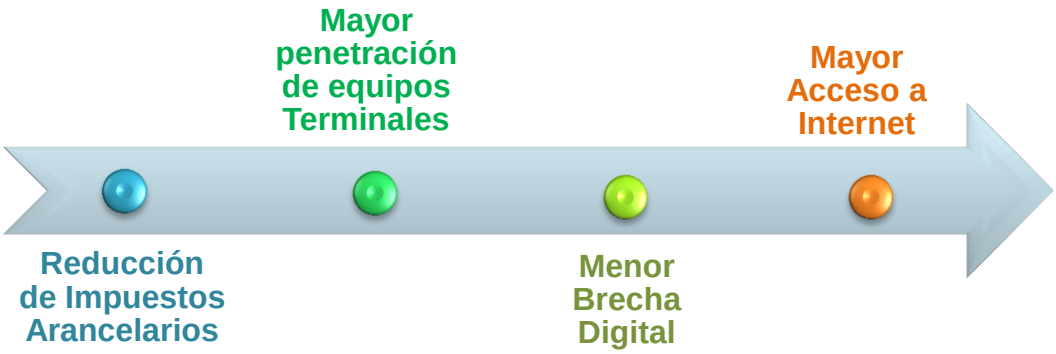


Figura 6.4: Impacto de impuestos arancelarios en equipos terminales.

La propuesta de este Plan de Acción es la exoneración de impuestos arancelarios a todos los equipos tecnológicos terminales que permitan el acceso a Internet. La medida permite reducir de manera considerable el precio de venta de estos equipos a los usuarios ecuatorianos,

consiguiendo de esta manera que cada vez más usuarios sean los interesados en acceder a Internet.

El Gobierno debería ejecutar esta medida inmediatamente, ya que el ingreso al país de estos equipos terminales con acceso a Internet sin ningún impuesto, ayudaría a reducir la brecha tecnológica a tal punto que para el año 2020 el país tendría equipos de primera tecnología al alcance de los usuarios.

6.1.3. Eje de Inclusión Social.

A través del Eje de Inclusión Social, se busca implementar la formulación y ejecución de políticas que garanticen el derecho de todos los ecuatorianos al acceso universal a las TICs. Asimismo, se pretende que el acceso brindado por parte del gobierno vaya de la mano con capacitaciones en todos los sectores del país; además de que se incluya en la red de Internet a todas las comunidades indígenas del Ecuador.

6.1.3.1. Acceso a Internet para Áreas Rurales.

Teniendo en cuenta que en las áreas rurales ecuatorianas existen barreras topográficas y mayores distancias geográficas entre poblados, el acceso a los servicios de telecomunicaciones e Internet en estas zonas se vuelve restringido.

Para garantizar el acceso universal en las áreas rurales, el Estado ecuatoriano debería crear estrategias con el respectivo marco político para el diseño e implementación de infraestructuras apropiadas en

estas áreas. Además, el Gobierno ecuatoriano debería proveer incentivos suficientes a las empresas privadas para que atiendan la demanda de los usuarios en estas zonas. Los proveedores privados no llevan sus servicios a las áreas rurales debido a la dificultad que les representa la falta de mecanismos compensativos en el país que les garantice los costos de inversión.

Con el propósito de garantizar el acceso universal a toda la población ecuatoriana y cumplir las metas trazadas por parte del Plan Nacional de Banda Ancha y del Plan del Buen Vivir, se debería aprovechar los beneficios que ofrecen tecnologías con características de propagación, que permitan tener un mayor rango de cobertura para las zonas alejadas. Debido a esto, el Estado ecuatoriano debería explotar mucho más la red CDMA 450 que ya viene usando la Corporación Nacional de Telecomunicaciones (CNT E.P.) sólo para brindar telefonía fija inalámbrica en las áreas rurales. Este proyecto realizado por el MINTEL debería ser mejorado, de tal manera que además de brindar servicios de voz, se brinden servicios de datos. Para esto es necesario que la CNT E.P. implemente un mayor número de radiobases en los distintos lugares del país donde no exista ningún tipo de acceso a estos servicios, o no sea el adecuado; con la finalidad de cubrir totalmente las zonas rurales del país.

Asimismo, es importante la implementación del servicio de banda ancha satelital para las áreas rurales que se encuentren muy alejadas. Este servicio tiene como ventaja su fácil accesibilidad en cualquier lugar tan sólo con la instalación de una antena parabólica en el exterior de la vivienda, muy parecida al de la televisión satelital, y un decodificador en el interior. Sin embargo, el costo de este servicio es muy elevado, resultando difícil para los pobladores de zonas rurales financiar su pago

aunque lo necesiten. Por ello el Estado, debería generar mecanismos que permitan subsidiar su costo para que de esta manera ningún ecuatoriano se quede sin acceder a Internet.

6.1.3.2. Incorporación de más Aulas Móviles e Infocentros Comunitarios.

El gobierno debería garantizar el acceso a las TICs de la mejor manera a la población ecuatoriana, por lo que se propone aumentar el número de Aulas Móviles, teniendo en cuenta lo costoso que es este proyecto, de tal manera que se disponga una Aula Móvil por cada dos provincias del país; es decir un total de doce Aulas Móviles educando a los ecuatorianos simultáneamente.

De acuerdo a los costos menores que representa la implementación y mantenimiento de los Infocentros con respecto a las aulas móviles, la aplicación de este proyecto es mucho más viable; por ello, es necesario que el Gobierno Nacional logre implementar un Infocentro en cada una de las 807 parroquias rurales del país. Actualmente, como se señaló en la sección 5.3 de este trabajo, existen un total 489 infocentros en todo el país, de los cuales aproximadamente el 96% se encuentran ubicados en parroquias rurales.

De la misma manera, el Gobierno debería construir al menos un Infocentro en cada una de las 15 ciudades más pobladas e importantes del país; Guayaquil, Quito, Cuenca, Manta, Portoviejo, Machala, Santo Domingo, Ambato, Loja, Riobamba, Quevedo, Babahoyo, Esmeraldas, Durán y Milagro. Dichos Infocentros deben estar ubicados estratégicamente en los sectores urbanos marginales que es donde se concentra la mayor densidad poblacional de las ciudades en mención; aun en el caso de que ya existiera algún Infocentro, es importante la

evaluación de la densidad poblacional que permita la construcción estratégica de más Infocentros en otros sectores de dichas ciudades.

Conjuntamente al desarrollo de los proyectos, el MINTEL debería realizar campañas de promoción para que todos los ecuatorianos estén constantemente informados sobre las diferentes capacitaciones que se brindan en los Infocentros y sobre la cronología de visitas de las Aulas Móviles.

6.1.3.3. Programa Integral para la Seguridad de los niños en Línea

El Plan de Acción propone la creación de un entorno seguro en Internet que garantice la protección de niños, niñas y adolescentes, incluyendo mecanismos a disposición de los padres y de los menores de edad, permitiéndoles la utilización de una Internet libre de contenidos y conductas inadecuadas.

El Plan de Acción tiene como objetivo seguir las recomendaciones de la UIT en la protección de los niños, niñas y adolescentes en línea, y aplicarla a la necesidad inmediata de nuestro país por controlar los contenidos que resultan un riesgo para la seguridad de los menores en el uso de la Red.

Es importante mencionar que el Plan de Acción propone la colaboración conjunta de todos los interesados en el tema, con la finalidad de que no solo sea el Estado el encargado de la seguridad de los niños sino que sean también los Padres de familia, los responsables de su propia seguridad.

La Figura 6.5 representa la colaboración conjunta que debería existir en el país para garantizar la seguridad de los niños ecuatorianos al usar Internet:

Figura 6.5: Colaboración conjunta para garantizar la seguridad de los niños en línea.

Estado y Gobierno ecuatoriano:

Las herramientas gubernamentales deberían centrarse principalmente en la lucha contra el material pornográfico infantil en línea. Deberían crearse sanciones más drásticas en el COIP que castiguen con pena privativa de la libertad, que no sea menor a los 10 años, a quienes afecten a los niños y sus derechos.

El Gobierno debería fomentar la investigación policial para el control de las mafias que invaden la red diariamente; y debería promover soluciones técnicas innovadoras de control parental siendo brindadas a

los padres de familia desde las instituciones educativas para que todos los ecuatorianos tengan la confianza de beneficiarse de forma segura de Internet.

Se deberían establecer mecanismos de atención a las denuncias de abusos de niños en la red, ya sea a través de líneas telefónicas y chats en línea activas las 24 horas, como de centros de atención.

De la misma manera, el Ministerio de Educación debería impulsar una campaña masiva en todas las escuelas del Ecuador, siendo estas últimas las encargadas de fomentar en los estudiantes ecuatorianos de todos los niveles de educación, una nueva cultura digital especialmente en la enseñanza de la seguridad en línea y la responsabilidad en el uso de Internet.

Industria de Internet:

La Industria de Internet en el Ecuador está constituida principalmente por la Empresa Privada; por ello resulta importante que el Estado brinde la debida cooperación a esta Industria nacional, con medidas técnicas y tecnológicas permitiéndoles crear sistemas de control parental, y amparándolas con medidas judiciales que permitan la sanción inmediata al identificar a los responsables de afectar la integridad de los niños en línea.

Los propietarios de cibercafés de todo el país deberían colaborar de forma activa, observando situaciones por parte de los usuarios que resulten ser riesgosas; y denunciar a los Organismos Nacionales para que hagan cumplir la Ley.

Maestros y padres de familia:

La falta de conocimiento tecnológico de los padres familia y de gran parte de maestros ecuatorianos, resulta hacer más grande el problema de que los niños sean vulnerables a los riesgos de Internet.

Es importante la concientización de los padres de familia sobre los riegos que pueden estar afectando a los niños, y la colaboración de los maestros en la educación integral desde las escuelas. Para esto, el Gobierno ecuatoriano debería brindar oportunidades en la educación de los padres de familia y de los maestros.

Los programas de capacitación se deberían llevar a cabo en las mismas instituciones educativas a la que asisten sus hijos, además mediante la propuesta de aumentar el número de Infocentros y Aulas Móviles, en donde también se brinden capacitaciones de este tipo. Esto permitirá a los padres involucrarse mucho más en la interacción de los niños en Internet.

6.1.3.4. Garantías para la Libertad de expresión en línea.

La Libertad de expresión en Ecuador se ha convertido en un tema de profundo análisis y frecuentes debates. Debido a las posibles violaciones de este derecho a los usuarios ecuatorianos, resulta importante la revisión de los actuales mecanismos estatales, con la finalidad de tener políticas públicas que verdaderamente garanticen el derecho a la libertad de expresión en línea de todos los ecuatorianos.

El Plan de Acción tiene como objetivo la elaboración de un nuevo modelo regulatorio nacional que le permita al Estado establecer los

instrumentos adecuados de acuerdo a sus deberes, poniéndolos a disposición de los ecuatorianos para garantizar su derecho a la libertad de expresión.

Asimismo, el Gobierno nacional debería permitir el acceso libre de los ecuatorianos a Internet, garantizando la neutralidad en la red sin ningún tipo de bloqueo ni reducción de velocidad de conexión. Por lo tanto, el Estado debería aprobar una Ley a favor de la neutralidad en la red, que evite restricciones en contenidos, sitios y plataformas por parte de los proveedores de Internet.

El Plan de Acción contribuye con ideas que buscan a través del trabajo conjunto entre el Estado y la Sociedad Civil, lograr que Internet en el país sea seguro e innovador; donde el Estado garantice la libre expresión y el libre acceso a la información, y los usuarios de Internet sean incentivados a generar conocimiento e información útil y veraz.

6.1.3.5. Promoción de Internet en lengua Quechua.

Como una medida de integración a las TICs y promoción de la lengua quechua y la cultura indígena, se debería crear un dominio patrocinado de primer nivel “.que”, permitiendo a las comunidades indígenas navegar por la red en su propia lengua.

Lo beneficioso de la propuesta es que se incentiva a la población de estas comunidades a solicitar el dominio mencionado para promocionar sus propias páginas webs. De la misma manera, este dominio sirve para fomentar el turismo, permitiendo que las personas puedan conocer la historia e identidad de las distintas comunidades indígenas.

Es importante que el gobierno utilice este dominio para ofrecer las distintas páginas de Internet de sus Ministerios e Instituciones Públicas que están disponibles, también en lengua quechua.

Con esta iniciativa, se espera que exista un gran número de artículos en quecha disponibles en buscadores de Internet con este mismo idioma, con el objetivo de incluir a las comunidades indígenas del país y de la región, formando parte del gran conocimiento y multilingüismo que engloba la red de Internet.

CONCLUSIONES

1. La Declaración de Principios de la Sociedad de la Información marcó el origen del término de Gobernanza de Internet, siendo en la Agenda de Túnez donde se establecieron los lineamientos que marcaron el inicio del control y la gestión de Internet por parte de los gobiernos, empresas privadas, sociedad civil y demás partes interesadas; fomentando la participación activa de cada uno de ellos.

2. Las reuniones anuales que realiza el Foro para la Gobernanza de Internet analizan la situación mundial de Internet y desarrollan estrategias que permitan principalmente a los usuarios tener acceso universal a la red con mayor seguridad y diversidad. De la misma manera, el FGI siempre está buscando mecanismos que le permitan el correcto manejo de los recursos críticos de la web, diseñando modelos que incluyen a Organizaciones Internaciones, Gobiernos Nacionales y Sociedad Civil, siendo partícipes activos en la gestión de Internet.

3. Una de las mayores gestiones de la Gobernanza de Internet radica en la apertura y seguridad en la Red, donde la decisión final está encaminada a eliminar todo tipo de restricciones en la web; aunque se reconoce la legitimidad de determinadas políticas públicas con la finalidad de proteger al público, especialmente los niños, y evitar los delitos informáticos.

4. La Gobernanza de Internet reconoce una Internet plurilingüe, donde todas las personas puedan usar Internet en su propio idioma; así como generar y obtener información en varias lenguas. Asimismo, garantiza el acceso con mejoras e incorporación de nuevas infraestructuras,

especialmente en zonas rurales con el objetivo de cerrar la brecha digital.

5. En Ecuador se ve reflejada la Gobernanza de Internet mediante las garantías de acceso a las TICs en la Constitución, así como en las estrategias y metas gubernamentales presentes en el Plan del Buen Vivir y la Estrategia Ecuador Digital 2.0. Además, se adoptan recomendaciones de la UIT como la de sancionar los delitos informáticos en el COIP y la de implementar un Centro de Respuesta a Incidentes Informáticos; a pesar de que este último no ha sido implementado en todas sus fases.

RECOMENDACIONES

1. El Estado ecuatoriano debería realizar inversiones estatales para la implementación de la infraestructura que permita ofrecer el servicio de Internet en las zonas rurales y sectores urbanos marginales. La operadora CNT E.P. debería ser la encargada de desplegar la red en los sectores mencionados, ofreciendo el servicio a nivel nacional.

2. El Gobierno ecuatoriano debería fijar tarifas especiales en los precios del servicio de Internet para que los habitantes de los sectores rurales y urbano marginales que en su mayoría son personas con un nivel socio-económico bajo, puedan pagar por el servicio y se interesen en acceder a Internet.

3. El Gobierno ecuatoriano debería exigir a través de los planes de expansión que las empresas privadas brinden el servicio de Internet con la misma calidad tanto para las zonas urbanas como para las zonas rurales, debido que actualmente la calidad del servicio ofrecido en las zonas de poco interés económico es pésimo comparado con las ciudades.

4. El Gobierno ecuatoriano debería incentivar al sector productivo del país para que sean parte del desarrollo de tecnología desde equipos terminales hasta los equipos que son parte de la red de Internet, con el fin de reducir el costo de los mismos, y fomentar el acceso a Internet a través de estos equipos. Esto puede ir de la mano con la reducción de impuestos arancelarios para que la importación de nuevos equipos permitan reducir la brecha tecnológica en el país.

5. La SUPERTEL debería implementar inmediatamente el Centro de Respuesta a Incidentes Informáticos en Ecuador para que así exista un mayor control y seguimiento de los delitos informáticos que ocurren cada vez con mayor frecuencia a nivel nacional.

6. El Estado ecuatoriano debería preocuparse por la preparación integral de profesionales en materia de ciberseguridad para tener un mayor número de profesionales expertos para de esta manera exista investigación avanzada en la detección y prevención de delitos informáticos en el país.

BIBLIOGRAFÍA

[1] Unión Internacional de Telecomunicaciones – UIT. (2003, WSIS-03/GENEVA/4-S). Cumbre Mundial de la Sociedad de la Información. Declaración de Principios. Construir la Sociedad de la Información: Un desafío global para el nuevo milenio. Ginebra, Suiza: Publicación de la UIT.

[2] Unión Internacional de Telecomunicaciones – UIT. (2003, WSIS-03/GENEVA/5-S). *Cumbre Mundial de la Sociedad de la Información. Plan de Acción*. Ginebra, Suiza: Publicación de la UIT.

[3] Unión Internacional de Telecomunicaciones – UIT. (2005, WSIS-05/TUNIS/DOC/6(Rev.1)-S). Cumbre Mundial de la Sociedad de la Información. Agenda de Túnez para la Sociedad de la Información. Ginebra, Suiza: Publicación de la UIT.

[4] Foro para la Gobernanza de Internet – FGI. (2006, WSIS-2006/1). Reunión inaugural. Informe de antecedentes. Atenas, Grecia: Publicación del FGI.

[5] Foro para la Gobernanza de Internet – FGI. (2007, WSIS-2007/1). Segunda reunión. Documento de síntesis. Río de Janeiro, Brasil: Publicación del FGI.

[6] Foro para la Gobernanza de Internet – FGI. (2009, WSIS-2009/1). Cuarta reunión del FGI. Documento de antecedentes. Sharm el-Sheikh, Egipto: Publicación del FGI.

[7] Foro para la Gobernanza de Internet – FGI. (2011, WSIS-2011/1). Sexta reunión del FGI. Documento de antecedentes. Nairobi, Kenia: Publicación del FGI.

[8] Foro para la Gobernanza de Internet – FGI. (2012, WSIS-2012/1). Séptima reunión del FGI. Documento de antecedentes. Bakú, Azerbaiyán: Publicación del FGI.

[9] Foro para la Gobernanza de Internet – FGI. (2008, WSIS-2008/1). Tercera reunión. Documento de síntesis. Hyderabad, India: Publicación del FGI.

[10] Foro para la Gobernanza de Internet – FGI. (2010, WSIS-2010/1). Quinta reunión del FGI. Panorama dela Gobernanza de Internet. Documento de síntesis. Vilna, Lituania: Publicación del FGI.

[11] Relatores de Libertad de expresión de la Organización de Estados Americanos (OEA), Naciones Unidas (ONU), Organización para la Seguridad y la Cooperación en Europa (OSCE) y la Comisión Africana de los Derechos del Hombre y de los Pueblos (ACHPR). (2011, Junio 1). *Declaración Conjunta sobre Libertad de Expresión e Internet*. Washington D.C., Estados Unidos: Publicaciones de la OEA.

[12] Reporteros sin Fronteras. (2013). *Informe Internet 2013: Enemigos de Internet.* Obtenido de: http://files.rsf-es.org/200002874-996559a5f5/2013_INFORME_INTERNET.pdf

[13] Descubierta una red de espionaje informático desde China a 103 países. (2009, Marzo 30). Diario *El Mundo*. Visto el 10 de diciembre del 2013 en: http://www.elmundo.es/elmundo/2009/03/30/navegante/1238395043.html

[14] MANDIAT. (2013). APT-1: Exposición de una de las unidades de Ciber Espionaje de China. Obtenido de: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

[15] Reporteros sin Fronteras. (2011). *Primavera árabe: ¿apogeo de la Web?*. Visto el 15 de diciembre del 2013 en: http://www.rsf-es.org/grandes-citas/dia-contra-censura-en-internet/a2011-dia-mundial-contra-la-censura-en-internet/frente-a-la-censura-solidaridad-en-la-red/

[16] Reporteros sin Fronteras. (2011, Noviembre). *Los medios de comunicación, testigos clave de Las revoluciones y de Los retos del poder: Rebeliones Árabe.* Obtenido de: http://files.rsf-es.org/200001779-6cd016ec49/2011_PRIMAVERA.ARABE.pdf

[17] Reporteros sin Fronteras. (2011). *Aumenta la potencia de Control 2.0.* Visto el 15 de diciembre del 2013 en: http://www.rsf-es.org/grandes-citas/dia-contra-censura-en-internet/a2011-dia-mundial-contra-la-censura-en-internet/aumenta-la-potencia-de-control-2-0/

[18] Organización Mundial de la Propiedad Intelectual – OMPI. (2009, OMPI-450/S). *¿Qué es la Propiedad Intelectual?* Ginebra, Suiza: Publicación de la OMPI.

[19] Pereda, C. (2012, Enero 19). *Las claves de las leyes SOPA y PIPA.* Diario *El País*, p. 18. Visto el 18 de diciembre del 2013 en: http://tecnologia.elpais.com/tecnologia/2012/01/19/actualidad/1326967261_850215.html

[20] Huichalaf, P. (2012). *Minuta explicativa sobre Proyectos de Ley SOPA y PIPA de EEUU y sus posibles efectos jurídicos en Chile.* Obtenido

de: http://culturadigital.cl/wp/wp-content/uploads/2012/01/Minuta-explicativa-sobre-Proyectos-de-ley-SOPA-y-PIPA-de-EEUU.pdf

[21] Wikipedia lidera apagón virtual contra la polémica ley antipiratería. (2012, Enero 18). Diario *ABC*. Visto el 18 de diciembre del 2013 en: http://www.abc.es/20120118/medios-redes/abci-wikipedia-apagon-sopa-201201180609.htmlf

[22] Internet cierra filas contra la Ley SOPA. (2012, Enero 19). Diario *ABC*. Visto el 18 de diciembre del 2013 en: http://www.abc.es/20120119/medios-redes/abci-sopa-reacciones-201201191138.html

[23] Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) Sector de Comunicación e Información (2013). *Directrices para Políticas de Desarrollo y Promoción del Acceso Abierto*. París, Francia: publicado por la UNESCO.

[24] Unión Internacional de Telecomunicaciones – UIT. (2010). *Actas Finales de la Conferencia de Plenipotenciarios. Resolución No. 181: Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación.* Guadalajara, México: Publicación de la Conferencia de Plenipotenciarios de la UIT.

[25] Unión Internacional de Telecomunicaciones – UIT. (2007). *Agenda Global de la Ciberseguridad*. Ginebra, Suiza: Publicación de la UIT.

[26] Unión Internacional de Telecomunicaciones – UIT-D. (2010). *Comisión de Estudio 1. Garantía de seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad*. Ginebra, Suiza: Publicación de la UIT.

[27] Pérez, J., & Olmos, A. (2009). Introducción. Gobernanza de Internet. *Revista TELOS No. 80*. Visto el 23 de diciembre del 2013 en: http://telos.fundaciontelefonica.com/telos/articulocuaderno.asp@idarticulo=1&rev=80.htm

[28] Foro de la Gobernanza de Internet en España. (2013). Obtenido de: http://www.igfspain.com/doc/archivos/Mensajes_del_Foro_de_la_Gobernanza_de_Internet_2013.pdf

[29] Ministerio de Industria, Energía y Turismo; Ministerio de Hacienda y Administraciones Públicas. (2013). *Agenda Digital para España*. Publicado por: Gobierno de España. Obtenido de: http://www.agendadigital.gob.es/agenda-digital/recursos/Recursos/1.%20Versi%C3%B3n%20definitiva/Agenda_Digital_para_Espana.pdf

[30] Ministerio de Industria, Energía y Turismo; Ministerio de Hacienda y Administraciones Públicas. (2013). *Agenda Digital para España: Plan de confianza en el ámbito digital.* Publicado por: Gobierno de España. Obtenido de: http://www.agendadigital.gob.es/planes-actuaciones/Bibliotecaconfianza/Plan/Plan-ADpE-5_Confianza.pdf

[31] ICANN aprueba el dominio .cat para la comunidad lingüístico–cultural catalana. (2005). Diario *El Mundo.* Visto el 20 de diciembre del 2013 en: http://www.elmundo.es/navegante/2005/09/16/esociedad/1126854203.html

[32] Aprobado el dominio .gal para el gallego en Internet. (2013). Diario *La Voz de Galicia.* Visto el 20 de diciembre del 2013 en: http://www.lavozdegalicia.es/noticia/vidadigital/2013/06/14/autorizado-dominio-gal-gallego-internet/0003137123951875674285 7.htm

[33] Comisión Europea. (2013, Octubre 17). *100% de cobertura lograda en Europa.* Obtenido de: http://europa.eu/rapid/press-release_IP-13-968_en.htm

[34] Iván Sánchez Medina. (Mayo 6, 2013). *Estado de la Gobernanza de Internet en Colombia*. Medellín, Colombia: Publicaciones de la Comisión Regulación Comunicaciones – CRC. Visto el 05 de enero del 2014 en: http://prezi.com/bbswpnw6l4-q/estado-de-la-gobernanza-de-internet-en-colombia/

[35] Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC (2012). *Colombia, sede de la escuela de Gobernanza en Internet.* Visto el 05 de enero del 2014 en: http://www.mintic.gov.co/index.php/mn-news/859-colombia-sede-de-la-escuela-de-gobernanza-en-internet

[36] Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC (2010). *Estrategia Internet Sano*. Visto el 05 de enero del 2014 en: http://archivo.mintic.gov.co/mincom/faces/?id=2954

[37] Certicámara S.A. (2013). *ABC para proteger los datos personales.* Bogotá, Colombia: Publicación CCD (Corporación Colombia Digital). Obtenido de: http://colombiadigital.net/publicaciones_ccd/anexos/certicamara_proteccion_datos_ago28.pdf

[38] Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC (2011). *Vive Digital Colombia (Versión 1.0/Febrero 2011)* Bogotá, Colombia: Publicación del MinTIC. Obtenido de: http://www.mintic.gov.co/images/MS_VIVE_DIGITAL/archivos/Vivo_Vive_Digital.pdf

[39] Secretaría Nacional de Planificación y Desarrollo – SENPLADES. (2013). *Plan Nacional para el Buen Vivir 2013 - 2017*. Quito, Ecuador: Publicación del SENPLADES.

[40] Secretaría Nacional de Telecomunicaciones – SENATEL. (2013). *Infraestructura del sector.* Obtenido de*:* http://www.regulaciontelecomunicaciones.gob.ec/biblioteca/

[41] Gobierno destina $90.3 millones para la estrategia Ecuador Digital 2.0. (2012, Mayo 24). Diario *Hoy*. Visto el 18 de diciembre del 2014 en: http://www.hoy.com.ec/noticias-ecuador/gobierno-destina-90-3-millones-para-la-estrategia-ecuador-digital-2-0-547986.html

[42] Ministerio de Telecomunicaciones y Sociedad de la Información – MINTEL. (2012). *Ecuador Digital 2.0*. Quito, Ecuador: Publicación del MINTEL.

[43] Aulas Móviles. (2013). *Ministerio de Telecomunicaciones y Sociedad de la Información – MINTEL.* Obtenido de: http://www.telecomunicaciones.gob.ec/aulas-moviles-y-alistamiento-digital/

[44] Infocentros Comunitarios. (2012). *Ministerio de Telecomunicaciones y Sociedad de la Información – MINTEL.* Obtenido de: http://www.telecomunicaciones.gob.ec/infocentros-comunitarios/

[45] Ministerio de Telecomunicaciones y Sociedad de la Información – MINTEL. (2012). *Plan Nacional de Alistamiento Digital*. Quito, Ecuador: Publicación del MINTEL.

[46] Ministerio Coordinador de Sectores Estratégicos – MCSE. (2014). *Rendición de Cuentas 2013*. Quito, Ecuador: Publicación del MCSE.

[47] Programa Conectividad Escolar. (2012). *Ministerio de Telecomunicaciones y Sociedad de la Información – MINTEL.* Obtenido de: http://www.telecomunicaciones.gob.ec/conectividad-escolar/

[48] Secretaria Nacional de Telecomunicaciones – SENATEL. (Julio, 2007). *Plan Nacional de Desarrollo de las Telecomunicaciones*. Quito, Ecuador: Publicación del CONATEL.

[49] Consejo de Europa - CdE. (2001). *Convenio sobre la Ciberdelincuencia. Serie de Tratados Europeos No. 185*. Budapest, Hungría: Publicación de la Secretaría del CdE

[50] Las técnicas que más utilizan los antisociales para robar en la red. (2012, Agosto 26). Diario *El Universo*. Visto el 27 de enero del 2014 en: http://www.eluniverso.com/2012/08/26/1/1422/las-tecnicas-mas-utilizan-antisociales-robar-red.html

[51] Cibercrimen: cuatro ataques por segundo. (2013, Noviembre 18). Diario *Expreso*. Visto el 27 de enero del 2014 en: http://expreso.ec/expreso/plantillas/nota_print.aspx?idArt=5305625&tipo=2

[52] Rodríguez, L. (2013). *La libertad de expresión en la Sociedad de la Información como derecho fundamental para la divulgación de la Ciencia y Tecnología: Entorno mundial y situación en el Ecuador* (Tesis de Maestría, ESPOL, Guayaquil, Ecuador).

[53] Superintendencia de Telecomunicaciones 2012, Revista SUPERTEL No. 13.

[54] Acurio, S. (2009). *Perfil sobre los delitos informáticos en el Ecuador*. Quito, Ecuador: Publicación de la Fiscalía General del Estado.

[55] La entrega del IP puede ser mal utilizada. (2012, Julio 27). Diario *Hoy*. Visto el 28 de enero del 2014 en: http://www.hoy.com.ec/noticias-ecuador/la-entrega-del-ip-puede-ser-mal-utilizada-557051.html

[56] Fundación Andina para la Observación y el Estudio de Medios – Fundamedios. (2014, Enero 27). *Corte en Ecuador admitió acción de inconstitucionalidad contra ley de comunicación*. Visto el 28 de enero del 2014 en: http://www.ifex.org/ecuador/2014/01/27/ley_comunicacion_demanda/es/

[57] El 'bullying' se viraliza en la Internet. (2013, Junio 30). Diario El Comercio. Visto el 28 de enero del 2014 en: http://www.elcomercio.com.ec/tecnologia/Bullying-internet-ciberbullying-ciberacoso-acoso-tecnologia-chantaje-plataformas_0_947305326.html.

[58] Superintendencia de Telecomunicaciones 2012, Revista SUPERTEL No. 14.