ANÁLISIS DE LOS MECANISMOS DE CONTROL DEL GROOMING EN COLOMBIA

AYDA GRACIELA CASTRO SUAREZ
JINETH MERCEDES CAMARGO THOMAS

TRABAJO DE GRADO

ASESOR

ALFONSO VALENCIA RODRIGUEZ
Director Especialización Seguridad Informática

UNIVERSIDAD PILOTO DE COLOMBIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2012

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, Febrero de 2013

AGRADECIMIENTOS

Te doy gracias a ti Amado Dios, porque a pesar de las circunstancias y de los momentos difíciles tu mano poderosa, tu amor, tu Palabra recordándome que todo lo puedo en Ti quien me fortalece y tu fidelidad siempre estuvo presente, sin ti no hubiera podido culminar esta gran etapa en mi vida, porque tú eres mi prioridad y mi motor.

Gracias le doy a mis Padres, Isabel y Manuel, quienes han sido siempre un gran ejemplo y un enorme apoyo en mi vida, y nunca han perdido la fe, ni la confianza, y quienes juntos con una palabra de ánimo, de amor me impulsan a seguir adelante para culminar todo lo que me propongo.

A mi hermana Lyda, que con sus consejos, su experiencia siempre ha estado guiándome a hacer lo mejor y a lograrlo sin temerle a las circunstancias y con los ojos puestos en Dios.

A todas las otras personas que estuvieron animándome, que estuvieron apoyándome para llegar a lograr cada uno de los logros y los propósitos y metas en mi vida.

Jineth Camargo Thomas

"Agradezco a Dios por la oportunidad que me dio de cumplir mi sueño de seguir estudiando, por las personas que se cruzaron en mi camino para enriquecer mi conocimiento, mi personalidad y mi vida.

A mis padres, Pedro José y Nubia, que a pesar de haber pasado por momentos muy difíciles en nuestras vidas, me han enseñado que no se puede desfallecer y que se debe seguir luchando… por su comprensión, amor y cuidados.

A mi hija, María José, por haberme esperado todo este tiempo, por las noches que no pasamos juntas y por los abrazos y besos que me dio para reconfortarme cuando creí que no podría seguir adelante.

A todos aquellos que siempre estuvieron ahí, alentándome para seguir luchando por llegar a donde tanto he querido."

Ayda Graciela Castro S.

GLOSARIO

1. **Menor de Edad:** Se entiende por menor de edad la persona que no ha cumplido los dieciocho años.

2. **Pornografía Infantil:** Se entiende por pornografía infantil, toda representación, por cualquier medio, de un menor de edad dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales.

3. **Spamming:** El uso de los servicios de correo electrónico para difundir mensajes no solicitados de manera indiscriminada a una gran cantidad de destinatarios.

4. **Servicio de Alojamiento:** Servicio de hospedaje a través del cual se le brinda a un cliente un espacio dentro de su servidor para la operación de un sitio.

5. **Sitio:** Conjunto de elementos computacionales que permiten el almacenamiento, intercambio y/o distribución de contenidos en formato electrónico a los que se puede acceder a través de Internet o de cualquier otra red de comunicaciones y que s e disponen con el objeto de permitir el acceso al público o a un grupo determinado de usuarios. Incluye elementos computacionales que permiten, entre otros servicios, la distribución o intercambio de textos, imágenes, sonidos o video.

6. **ISP:** (Internet Service Provider) - Proveedor de acceso a Internet.

7. ***Grooming*.** Problema relativo a la seguridad de los menores de edad en Internet, que consiste en las actividades previamente meditadas por un adulto con el objetivo de establecer y estrechar lazos de amistad con un niño o niña en Internet, buscando obtener satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como acontecimiento previo a un encuentro sexual abusivo.

8. ***Firmware***. El firmware es un bloque de instrucciones de máquina para propósitos específicos, grabado en una memoria de tipo de solo lectura (ROM, EEPROM, flash, etc.), que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. Está fuertemente integrado con la electrónica del dispositivo siendo el software que tiene directa interacción con el hardware: es el encargado de controlarlo para ejecutar correctamente las instrucciones externas.

   El programa BIOS de una computadora es un firmware cuyo propósito es activar una máquina desde su encendido y preparar el entorno para cargar un sistema operativo en la memoria RAM.[1]

[1] **WIKIPEDIA.** La Enciclopedia Libre. [En Línea], 2012, actualizado el 29 Diciembre 2012 [Publicado en 13 Agosto 2009]. Firmware. Disponible en Internet: <http://es.wikipedia.org/wiki/Firmware>.

RESUMEN

El Grooming o pornografía infantil en internet es un problema que a medida que la tecnología ha avanzado también ha incrementado éste tipo de delito. El Grooming es una acción que daña al menor sicológicamente, puesto que es un tipo de presión o chantaje, es una actividad que va en contra de la voluntad de un menor de edad. Donde primero el delincuente se gana la confianza del menor, consiguiendo datos personales del menor, secretos y a partir de esto comienza el chantaje, donde el menor por evitar que sea difundida su información accede a participar en esta actividad.

En Colombia, existen leyes contempladas en la Constitución política de 1991, la ley de infancia y adolescencia, la ley 1098 de 2006, la ley 679 de 2001, el decreto 1524 de 2002, la ley 1336 de 2009 y ley 599 de 2000, donde tocan temas de protección contra el abuso realizado a un menor de edad, estableciendo también estrategias y medidas de control.

También en Colombia el Grooming es considerado un delito informático, conocido por las entidades de control, donde ellas han creado un canal de denuncia, entre ellos en convenio el Ministerio de la información y la comunicación, el ICBF, Red Papaz.

El Ministerio de la información y la comunicación tiene como tal un programa llamado en Tic confío, como objetivo de brindar un buen uso de las TICS en los jóvenes; también puso en marcha un proyecto nacional llamado Internet sano para evitar la explotación sexual con menores de edad y hacer que se denuncien los casos en cuanto esta actividad.

El objetivo es analizar los mecanismos de control del Grooming en Colombia.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

INTRODUCCIÓN

El avance de las tecnologías, la aparición de nuevas formas de comunicación y el crecimiento global que ha tenido internet ha abierto grandes puertas y en ellas muchas oportunidades para crecer y mejorar; pero también junto con éstas han aumentado los peligros que afectan a los menores de edad.

Con el presente estudio se buscan analizar los mecanismos de control y medidas que han tomado en contra del *Grooming* o Ciber acoso sexual; donde el trabajo del acosador es atacar directamente de forma sexual a la víctima en éste caso a un menor de edad, por medio de las redes sociales, chats, foros o conversaciones, entre otros.

Muchas veces los menores, pese a su habilidad de navegar por el Internet, no tienen la conciencia del peligro que este representa. El internet por sí solo no es bueno o malo, lo malo es el uso inadecuado que se da al mismo, razón por la cual es importante conocer las formas de propagación de este delito, así como los mecanismos de control en Colombia, con el fin de prevenir este tipo de acto delictivo y darlo a conocer a Padres de familia y adultos a cargo.

OBJETIVOS

General

Establecer un análisis de los mecanismos de control del *Grooming* en Colombia.

Específicos

1. Recolectar información de fuentes bibliográficas y estudios referentes al control del *Grooming* en Colombia.

2. Aplicar un instrumento estadístico que permita evaluar el impacto de los controles del *Grooming* en Colombia.

3. Hacer recomendaciones sobre los controles que existen del *Grooming* en Colombia

1. MARCO TEÓRICO

1.1 INTRODUCCIÓN

Internet es una red que se ha convertido en una de las herramientas más grandes, utilizadas, con muchas ventajas hoy en día para prácticamente todo el mundo; pero, también con desventajas puesto que es peligroso, por la información libre que ofrece, peligroso más que todo para los menores, más porque ellos no tienen en la actualidad tanto control como antes.

La llegada de Internet abrió las puertas a la comunicación instantánea, a la creación de redes sociales, foros, lugares de intercambio en la Red. Con sus pros y sus contras. Siempre se pone el acento en las facilidades que han traído las tres W pero, ¿qué consecuencias negativas ha podido tener?

El término proviene del inglés "groom" que significa acicalar o cepillar en caso de animales. Sin embargo, el "Grooming" es "un nuevo tipo de problema relativo a la seguridad de los menores en Internet, consistente en acciones deliberadas por parte de un adulto de cara a establecer lazos de amistad con un niño o niña en Internet, con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual".[2]

1.2 TEORÍA Y CONCEPTOS BÁSICOS

1.2.1 Grooming o Ciber acoso sexual. El Grooming de niños es una actividad malvada realizada por un adulto vía internet con fines pedófilos por medio de abusos sexuales a menores de edad y obtención de material pornográfico. En los

[2] **EXPLOTACIÓN SEXUAL COMERCIAL DE NIÑOS, NIÑAS Y ADOLESCENTES E INTERNET**. X Informe al Secretario General de la OEA sobre las medidas emprendidas por los Estados Miembros para prevenir y erradicar la Explotación Sexual Comercial de niñas, niños y adolescentes en las Américas. Montevideo, Febrero, Vol. 1, 2011. 10 Ed. 31 p.

últimos años, este delito se ha convertido en uno de los más comunes entre los denominados delitos informáticos.[3]

En el lenguaje de seguridad informática, se conoce como Grooming a cualquier acción que tenga por objetivo minar y socavar moral y psicológicamente a una persona, a fin de conseguir su control a nivel emocional. Si bien esta actividad puede producirse en cualquier instancia, es particularmente grave en los casos en los que una persona lleva a cabo este tipo de coacciones y presiones emocionales en contra de un menor, con el objeto de obtener algún tipo de favor sexual.

Este tipo de chantajes suelen producirse habitualmente a través de servicios de chat y mensajería instantánea, y deben ser denunciados de forma inmediata.[4]

El Ciber Grooming es un método formado por un conjunto de estrategias que una persona adulta desarrolla para ganarse la confianza de un menor de edad a través de Internet y las nuevas tecnologías (TIC), para conseguir su control a nivel emocional, con el fin último de obtener concesiones de índole sexual.

Esta forma de abuso procede del Grooming, el cual se da sin intermediarios como las redes sociales, es decir, el adulto se gana la confianza del menor en directo, mediante encuentros físicos, para luego desembocar en los mismos actos.[5]

1.2.2 Métodos del *Groomer*. El acosador puede elegir a su víctima a través de Internet o en persona. Una vez fijado el objetivo, se dan las siguientes fases:

1. Puesta en contacto y amistad: El acosador (haciéndose pasar por un adolescente) inicia una relación por medio de Internet con el menor.

- Lentamente comienza a surgir una **"amistad"**.

2. Confesión: Gracias a la confianza, el acosador consigue sin forzar la situación, información y datos básicos sobre la víctima. Finalmente, el menor le acaba por confesar determinados secretos e intimidades.

---

[3] **Grooming o Ciber acoso.** [En Línea] Villa Rica, Chile. Informática y Rock & Roll. [Publicado el 23 Mayo 2009] Disponible en Internet: <http://javierzg.wordpress.com/2009/05/23/grooming-ciberacoso>.

[4] **INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN.** Enciclopedia Jurídica [En Línea], 2012, León, España, actualizado el 08 Febrero 2012 [Publicado en Noviembre 2007]. Observatorio de Seguridad de la Información. Grooming. Disponible en Internet: <http://www.inteco.es/wikiAction/Seguridad/Observatorio/area_juridica_seguridad/Enciclopedia/Articulos_1/Grooming>.

[5] **INSTITUCIÓN EDUCATIVA CAMPOS Y TOROZOS.** Principales riesgos en las Redes Sociales [En Línea], 2010, León y Castilla, España, [Publicado en Agosto 2010]. Disponible en Internet: <https://sites.google.com/site/riesgosredessociales2011/grooming/2-1---definicion >.

3. Desenmascaramiento: Con los datos obtenidos, se pide al menor su participación en actos de naturaleza sexual (envíos de imágenes, vídeos,...) a cambio de mantener los secretos en silencio. Así, el delincuente se hace con un verdadero arsenal de material con el que continuar chantajeando.

4. Componente sexual: Esta fase sólo se da en los casos más graves de Grooming. En ella, el pederasta obliga mediante chantajes al menor, a tener encuentros presenciales donde se producen abusos físicos.

1.2.3 Cómo evitarlo. Para Evitar el Grooming, es importante tener en cuenta las siguientes recomendaciones:

1. Colocar el PC en lugares de tránsito o visible y evitar que los niños chateen a puerta cerrada.

2. Evitar que los niños chateen después de las 22 horas en adelante, ya que a partir de esta hora se incrementa el número de usuarios y potencialmente aumenta el riesgo.

3. Preguntar permanentemente a los hijos quiénes son sus contactos o nuevos amigos del chat y quién está detrás de cada correo electrónico.

1.2.4 Tres fases y diez claves para luchar contra el acoso sexual en la red. Si se evita que el depredador obtenga el elemento de fuerza con el que iniciar el chantaje, el acoso es inviable. Para ello es recomendable:

1. **No proporcionar imágenes o informaciones comprometedoras** (elemento de fuerza) a nadie ni situar las mismas accesibles a terceros. Se ha de pensar que algo sin importancia en un determinado ámbito o momento puede cobrarla en otro contexto.
2. **Evitar el robo de ese elemento de fuerza** para lo cual se debe preservar la seguridad del equipo informático y la confidencialidad de las contraseñas.
3. **Mantener una actitud proactiva respecto a la privacidad** lo que implica prestar atención permanente a este aspecto y, en especial, al manejo que las demás personas hacen de las imágenes e informaciones propias.

Afrontamiento: tomar conciencia de la realidad y magnitud de la situación.

Cuando se comienzan a recibir amenazas e intimidaciones es importante:

4. **No ceder al chantaje** en ningún caso puesto que ello supone aumentar la posición de fuerza del chantajista dotándole de un mayor número de elementos como pueden ser nuevas imágenes o vídeos eróticos o pornográficos.

5. **Pedir ayuda**. Se trata de una situación nueva y delicada que conlleva gran estrés emocional. Contar con el apoyo de una persona adulta de confianza es fundamental. Aportará serenidad y una perspectiva distinta.
6. **Evaluar la certeza de la posesión** por parte del depredador de los elementos con los que se formula la amenaza y las posibilidades reales de que ésta se lleve a término así como las consecuencias para las partes. Mantener la cabeza fría es tan difícil como importante.
7. **Limitar la capacidad de acción del acosador**. Puede que haya conseguido acceso al equipo o posea las claves personales. En previsión de ello:
    a. Realizar una revisión total para evitar el *malware* del equipo y cambiar luego las claves de acceso.
    b. Revisar y reducir las listas de contactos así como la configuración de las opciones de privacidad de las redes sociales.
    c. En ocasiones, puede ser acertado cambiar de perfil o incluso de ámbito de relación en la Red (bien sea una red social, un juego online multijugador...).

Intervención

Las situaciones de acecho sexual rara vez terminan por sí mismas, siendo habitual la reincidencia en el acoso incluso en momentos muy distantes en el tiempo. Es preciso no bajar la guardia y llegar hasta el final para lo cual es conveniente:

8. **Analizar en qué ilegalidades ha incurrido el acosador y cuáles pueden ser probadas.** Puede ser inviable probar que el depredador dispone de ciertas imágenes o informaciones o que las ha hecho públicas. También puede ocurrir que no se pueda demostrar que esas imágenes fueron obtenidas por la fuerza o mediante engaño o incluso que se han recibido amenazas. Por todo ello conviene saber en qué ilícitos ha incurrido o incurre el depredador porque ello habilita la vía legal.
9. **Buscar y recopilar las pruebas de la actividad delictiva:** capturas de pantalla, conversaciones, mensajes... todo aquello que pueda demostrar las acciones del depredador o dar pistas sobre su paradero o modo de actuar será de gran utilidad tanto a efectos de investigación como probatorios. Se debe tener presente no vulnerar la Ley en este recorrido.
10. **Formular una denuncia**. Con un adecuado análisis de la situación y elementos de prueba que ayuden a la investigación el hecho ha de ser puesto en conocimiento de las Fuerzas y Cuerpos de Seguridad del Estado con independencia de que el acecho hubiera o no remitido.

Cada caso es diferente y la manera de abordarlo también. En determinadas circunstancias, incluso puede ser recomendable seguir la corriente del acosador para tratar de identificarle. En otras, la denuncia inmediata a la policía es la opción más razonable. No obstante, las anteriores son orientaciones que pueden

funcionar bien en la mayoría de los casos y mientras la policía ofrece su asistencia. [6]

1.3 GROOMING EN COLOMBIA Y EL MUNDO

1.3.1 Colombia. La Constitución política de 1991, la ley de infancia y adolescencia, la ley 1098 de 2006, la ley 679 de 2001, el decreto 1524 de 2002, la ley 1336 de 2009 y ley 599 de 2000, legislan temas de protección contra toda forma de abuso realizado en la persona de cualquier menor de edad, igualmente establece la adopción de medidas tanto técnicas como administrativas destinadas a prevenir el acceso de los menores de edad a cualquier información de carácter pornográfico, así mismo se realizan las exigencias a los proveedores de servicio de internet para que sean los encargados de brindar las herramientas de denuncia en pro de la prevención de la pornografía infantil en internet. De acuerdo a lo anteriormente expuesto, se pudo establecer que el término "Grooming" no se encuentra consagrado en ninguna de estas disposiciones legales vigentes en el país.

1.3.2 El Resto del mundo. En el informe del Consejo de Europa para la Convención sobre Cibercriminalidad[7] - Protection of Children Against Abuse Through New Technologies, este se ocupó de los temas emergentes de violencia contra los niños por medio de las nuevas tecnologías, haciendo énfasis en el Grooming tanto a través de Internet como de telefonía móvil.

El Grooming es una conducta delictiva previa a otra de carácter sexual más grave. En dicho informe el consejo índico que existen países que ya ha incluido dentro de sus legislaciones el Grooming como delito, a pesar de esto hay países en los cuales aún no se tiene en cuenta.

Alemania. En este país está prohibido extralimitarse autoritariamente sobre un menor de edad a través de exhibición o conversaciones con sentido pornográfico.[8]

---

[6] **FLOREZ HERNÁNDEZ**, Jorge. Decálogo para combatir el Grooming y el acoso sexual infantil. Internet Grooming [En Línea], 1994 – 2009. Disponible en Internet: <http://www.internet-grooming.net/decalogo-grooming-acoso-sexual-menores-online.html>

[7] **INTERNET LAW FORUM - PROTECTION OF CHILDREN AGAINST ABUSE THROUGH NEW TECHNOLOGIES - CYBERCRIME CONVENTION COMMITTEE** [En Línea]. Estados Unidos: **COUNCIL OF EUROPE** (ETS no. 185) [Citado en 06 Julio de 2011] Disponible en Internet: <http://socialnetwork.ibls.com/forums/topic/271/cyber-bullying>

[8] **BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE.** Grooming: nueva táctica de contacto de pedófilos [En Línea], 2008, Chile [Publicado el 21 Junio 2008]. El Grooming en otras legislaciones.

Australia. La Criminal Code Act de 1995, secciones 474.26 y 474.27, establece la prohibición sobre el uso de servicios de telecomunicaciones para encontrar menores de edad (16 años), o exponerlas a material indecente, con propósito de realizar Grooming. En el territorio australiano, algunos estados difieren en la edad en la que se encuentra cualificada una persona como menor de edad.

Canadá. El castigo por comunicarse con un menor de edad con el propósito de cometer abuso sexual haciendo uso de sistemas informáticos se encuentra legislado en el Criminal Code, sección 172.1.

España. Con el propósito de castigar el engaño con fines sexuales a través de internet a menores de edad, así como determinar cómo agresión sexual aquellas actividades que atenten contra la intimidad o libertad sexual del atacado, entro en vigencia en diciembre de 2010 la reforma del Código Penal.[9]

Estados Unidos. Si con el objetivo de abusar sexualmente de un menor de 18 años se transmite información, se prohíbe dicha transmisión; en algunos Estados se tiene disposiciones adicionales cuando se trata de seducción de niños vía online.

Reino Unido. Según las secciones 14 y 15 del Sexual Offences Act de 2003, tanto Inglaterra como Gales, penan la disposición de encuentros con menores de edad, para uno mismo o terceras personas, con la intención de abusar sexualmente de este menor.[10]

Escocia. Se implantan conceptos similares haciendo uso de la Protection of Children and Prevention of Sexual Offences Act de 2005.[11]

Disponible en Internet: <http://www.bcn.cl/carpeta_temas_profundidad/grooming-acoso-sexual-ninos/#el-grooming-en-otras-legislaciones >.

[9] **COLLI, Nieves.** Tribunal Nacional Argentino. Luz verde a un Código Penal consensuado que sube las penas a terroristas y pederastas [En Línea]. 2008. no. 11870 [Publicado el 14 Noviembre 2008] Disponible en: http://www.abc.es/20081114/nacional-tribunales/verde-codigo-penal-consensuado-20081114.html

[10]**INGLATERRA. U.K. PARLIAMENT.** Act of the U.K. Parliament; Sexual Offences Act, section 15. 2003.

[11]**INGLATERRA. U.K. PARLIAMENT.** Act of the Scottish Parliament; Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005, 2005 asp 9.

1.4 Estrategias implementadas para el Control de Grooming en Colombia

El Grooming o Cyberacoso en Colombia es uno de los delitos informáticos conocidos por las entidades de control, existe una línea virtual de denuncia de grooming, ciberbulling, sexting, etc, que en el país fue creada por la Fundación Telefónica, en convenio con el Ministerio de Tecnologías de la Información y la Comunicación, el Instituto Colombiano de Bienestar Familiar, el Foro de Generaciones Interactivas y la red PaPaz.[12]

A la iniciativa están asociados la Policía Nacional, la Empresa de Telecomunicaciones de Bogotá ETB, y Microsoft Colombia. Además cuenta con el apoyo de **Inhope** (Asociación internacional de líneas directas de Internet. Coordina una red de líneas directas de Internet en todo el mundo, apoyándolos en respuesta a los informes de contenido ilegal para que Internet sea más segura.), organismo que lidera y regula las líneas de denuncia de pornografía infantil a nivel mundial.

El portal lleva por nombre "Te Protejo – www.teprotejo.org" (primera línea virtual de denuncia en Latinoamérica para la protección de la infancia y la adolescencia colombiana.) es una iniciativa para la efectiva protección, a través de internet, de la infancia y la adolescencia en Colombia, además es un canal de denuncia de contenidos ilegales como son el abuso sexual, la explotación comercial y pornografía infantil y adolescente. En Te Protejo también se puede informar sobre el uso agresivo de TIC, la promoción de consumo de sustancias psicoactivas y otras situaciones de riesgo en menores de 18 años; la información allí suministrada será tratada de forma completamente anónima

El Ministerio de Tecnologías de la Información y las Comunicaciones contribuye al proyecto con el programa "en TIC confío", como estrategia del buen uso de las TIC en los jóvenes, incluso ya se han hecho visitas por el país para promover la iniciativa de "Cero tolerancia" con la pornografía infantil y adolescente, además de brindar información en el sitio web www.enticconfio.gov.co de interés para niños, jóvenes y adultos.

En Colombia el Ministerio de Tecnologías de la Información y las Comunicaciones puso en marcha el proyecto nacional "Internet Sano". En el marco de este proyecto se diseñó una estrategia de comunicación multimediática para prevenir y contrarrestar la explotación sexual y el turismo sexual con personas menores de edad en Internet. Esta campaña busca, de manera informativa y educativa,

[12] **INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES.** Annual Report 2011 [En Línea], 2011, Amsterdam [Publicado el Diciembre 2011]. Sayin no to illegal content on the internet. Disponible en Internet: <http://inhope.org/Libraries/Annual_reports/INHOPE_2011_Annual_Report.sflb.ashx>

vincular a todos los colombianos en la prevención de este delito. En este sentido, apela a que toda la población denuncie casos.

Esta campaña habilitó la creación de una línea gratuita nacional dirigida a proveedores y usuarios de redes globales, donde se informa las implicaciones legales de su uso en relación con la Ley. Se creó la estrategia INTERNET SANO albergada en el sitio Web www.internetsano.gov.co, donde formular denuncias contra eventos de explotación sexual infantil y señalar páginas electrónicas que se ofrezcan servicios sexuales con niñas, niños y jóvenes (Es una estrategia nacional, con el fin de prevenir y contrarrestar la pornografía, la explotación sexual y el turismo sexual con menores).

1.5 ASPECTOS LEGALES

1.5.1 Convención sobre los Derechos del Niño. La Convención de las Naciones Unidas sobre los Derechos del Niño, promulgada en 1989, reafirma la dignidad intrínseca y los derechos iguales e inalienables de todos los niños y las niñas del mundo y conmina a los Estados parte a garantizarlos. En su Artículo 19 establece, de manera explícita, la obligatoriedad de proteger a cualquier niño o niña del maltrato, abuso y explotación (Cuadros, 2006).[13]

Todos los Estados que se acojan a ella deben tomar medidas integrales en beneficio y protección de los derechos de la infancia, tales como:

- ✓ Bienestar social.
- ✓ Protección y cuidados necesarios.
- ✓ Instituciones especializadas para el cuidado de la niñez.
- ✓ Obligaciones de los padres, madres y/o representantes legales en la crianza y desarrollo de niños y niñas.
- ✓ Asistencia apropiada a los padres, madres y/o representantes legales para el desempeño frente a la crianza.
- ✓ Protección de los niños y niñas contra todas las formas de explotación y abuso sexual (incitación o coacción a la actividad sexual ilegal, explotación en la prostitución, otras prácticas ilegales, explotación en espectáculos o materiales pornográficos).
- ✓ Medidas para la recuperación del menor, tanto físicas y psicológicas como de reintegración social

[13] **ORGANIZACIÓN DE NACIONES UNIDAS – ONU.** El Sistema de Tratados de Derechos Humanos de las Naciones Unidas. Introducción a los tratados fundamentales de derechos humanos y a los órganos creados en virtud de tratados. 30 Ed. Ginebra: Editorial Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. 2004. 90 p.

1.5.2 Constitución Política de 1991. La Constitución Política de Colombia, Artículos 44 y 45, dispone en cuanto a los derechos fundamentales de niños, niñas y adolescentes (vida, integridad física, salud y seguridad social, entre otros), la protección contra toda forma de abandono (violencia física o moral, secuestro, venta, abuso sexual, explotación laboral o económica y trabajos riesgosos) y la prevalencia de estos derechos sobre los de los demás.

1.5.3 Ley 679 de 2001. Artículo 5. Informe de la comisión. Reglamentado por el Decreto Nacional 1524 de 2002. Con base en el informe de que trata el artículo anterior, el Gobierno nacional, con el apoyo de la Comisión de Regulación de Telecomunicaciones, adoptará las medidas administrativas y técnicas destinadas a prevenir el acceso de menores de edad a cualquier modalidad de información pornográfica, y a impedir el aprovechamiento de redes globales de información con fines de explotación sexual infantil u ofrecimiento de servicios comerciales que impliquen abuso sexual con menores de edad.

Artículo 10. Sanciones Administrativas. Parágrafo (adicionado por el artículo 3 de la Ley 1336 de 2009). El Ministerio de Comunicaciones tendrá competencia para exigir, en el plazo que este determine, toda la información que considere necesaria a los proveedores de servicios de internet, relacionada con la aplicación de la Ley 679 y demás que la adicionen o modifiquen. En particular podrá:

> 1. Requerir a los proveedores de servicios de internet a fin de que informen en el plazo y forma que se les indique, qué mecanismos o filtros de control están utilizando para el bloqueo de páginas con contenido de pornografía con menores de edad en Internet.
>
> 2. Ordenar a los proveedores de servicios de internet incorporar cláusulas obligatorias en los contratos de portales de internet relativas a la prohibición y bloqueo consiguiente de páginas con contenido de pornografía con menores de edad.
>
> Los proveedores de servicios de internet otorgarán acceso a sus redes a las autoridades judiciales y de policía cuando se adelante el seguimiento a un número IP desde el cual se produzcan violaciones a la presente ley.

Artículo 12. Medidas de Sensibilización. Las autoridades de los distintos niveles territoriales y el Instituto Colombiano de Bienestar Familiar, implementarán acciones de sensibilización pública sobre el problema de la prostitución, la pornografía y el abuso sexual de menores de edad. El Gobierno Nacional, por intermedio del Ministerio de Educación, supervisará las medidas que a este respecto sean dictadas por las autoridades departamentales, distritales y municipales.

1.5.4 Decreto 1524 de 2002. Reglamenta el artículo 5° de la Ley 679 de 2001

Artículo 4. Prohibiciones. Los proveedores o servidores, administradores y usuarios de redes globales de información no podrán:

1. Alojar en su propio sitio imágenes, textos, documentos o archivos audiovisuales que impliquen directa o indirectamente actividades sexuales con menores de edad.

2. Alojar en su propio sitio material pornográfico, en especial en modo de imágenes o videos, cuando existan indicios de que las personas fotografiadas o filmadas son menores de edad.

3. Alojar en su propio sitio vínculos o "links", sobre sitios telemáticos que contengan o distribuyan material pornográfico relativo a menores de edad.

Artículo 6. Medidas Técnicas.

1. Los ISP, proveedores de servicio de alojamiento o usuarios corporativos deberán implementar sistemas internos de seguridad para su red, encaminados a evitar el acceso no autorizado a su red, la realización de spamming, o que desde sistemas públicos se tenga acceso a su red, con el fin de difundir en ella contenido relacionado con pornografía infantil.

2. Los ISP deben implementar en su propia infraestructura, técnicas de control, basadas en la clasificación de contenidos que tengan como objetivo fundamental evitar el acceso a sitios con contenidos de pornografía infantil.

   La clasificación de estos contenidos se sujetará a la que efectúen las diferentes entidades especializadas en la materia. Dichas entidades serán avaladas de manera concertada por el Ministerio de Comunicaciones y el Instituto Colombiano de Bienestar Familiar-ICBF.

3. Los prestadores de servicios de alojamiento podrán utilizar herramientas tecnológicas de monitoreo y control sobre contenidos alojados en sitios con acceso al público en general que se encuentran en su propia infraestructura.

4. Los ISP y proveedores de servicios de alojamiento deberán ofrecer o informar a sus usuarios, sobre la existencia de mecanismos de filtrado que puedan ser instalados en los equipos de estos, con el fin de prevenir y contrarrestar el acceso de menores de edad a la pornografía.

5. Así mismo los ISP deberán facilitar al usuario el acceso a la información de criterios de clasificación, los valores y principios que los sustentan, la

configuración de los sistemas de selección de contenido y la forma como estos se activan en los equipos del usuario.

6. Cuando una dirección es bloqueada por el ISP, se debe indicar que esta no es accesible debido a un bloqueo efectuado por una herramienta de selección de contenido.

7. Los ISP y proveedores de servicios de alojamiento deberán incluir en sus sitios, información expresa sobre la existencia y los alcances de la Ley 679 de 2001, y sus decretos reglamentarios.

8. Los ISP y proveedores de servicios de alojamiento deberán implementar vínculos o "links" claramente visibles en su propio sitio, con el fin de que el usuario pueda denunciar ante las autoridades competentes sitios en la red con presencia de contenidos de pornografía infantil.

Parágrafo. Para todos los efectos la información recolectada o conocida en desarrollo de los controles aquí descritos, será utilizada únicamente para los fines de la Ley 679 de 2001, y en ningún caso podrá ser suministrada a terceros o con detrimento de los derechos de que trata el artículo 15 de la Constitución Política.

Artículo 7. Medidas Administrativas. En los diferentes contratos de servicio entre los ISP y sus suscriptores, deberán incluirse las prohibiciones y deberes de que trata este decreto, advirtiendo a estos que su incumplimiento acarreará las sanciones administrativas y penales contempladas en la Ley 679 de 2001 y en este decreto.

En los contratos de prestación de servicios de alojamiento se deben estipular cláusulas donde se prohíba expresamente el alojamiento de contenidos de pornografía infantil. En caso que el prestador de servicio de alojamiento tenga conocimiento de la existencia de este tipo de contenidos en su propia infraestructura, deberá denunciarlos ante la autoridad competente, y una vez surtido el trámite y comprobada la responsabilidad por parte de esta se procederá a retirarlos y a terminar los contratos unilateralmente.

1.5.5 Ley 1336 de 2009. Artículo 4. Autorregulación de café internet. Todo establecimiento abierto al público que preste servicios de Internet o de café Internet deberá colocar en lugar visible un reglamento de uso público adecuado de la red, cuya violación genere la suspensión del servicio al usuario o visitante.

Ese reglamento, que se actualizará cuando se le requiera, incluirá un sistema de autorregulación y códigos de conducta eficaces que promuevan políticas de prevención de explotación sexual de niños, niñas y adolescentes, y que permitan proteger a los menores de edad de toda forma de acceso, consulta, visualización o exhibición de pornografía.

Un modelo de estos sistemas y códigos se elaborará con la participación de organismos representativos del sector. Para estos efectos, el Ministerio de Comunicaciones convocará a los interesados a que formulen por escrito sus propuestas de autorregulación y códigos de conducta. Tales códigos serán adoptados dentro del año siguiente a la vigencia de la presente ley, copia de los cuales se remitirá a la oficina que indique el Ministerio de Comunicaciones, de su propia estructura o por delegación a los municipios y distritos, y serán actualizados cada vez que el Ministerio de Comunicaciones lo considere necesario en función de nuevas leyes, nuevas políticas o nuevos estándares de protección de la niñez adoptados en el seno de organismos internacionales, gubernamentales o no.

Las autoridades distritales y municipales realizarán actividades periódicas de inspección y vigilancia de lo dispuesto en este artículo y sancionarán su incumplimiento de conformidad con los procedimientos contenidos en el Código Nacional de Policía y los códigos departamentales y distritales de policía que apliquen.

El incumplimiento de los deberes a que alude esta norma dará lugar a las mismas sanciones aplicables al caso de venta de licor a menores de edad.

Artículo 25. Vigilancia y Control. La Policía Nacional tendrá además de las funciones constitucionales y legales las siguientes:

Los comandantes de estación y subestación de acuerdo con su competencia, podrán ordenar el cierre temporal de los establecimientos abiertos al público de acuerdo con los procedimientos señalados en el Código Nacional de Policía, cuando el propietario o responsable de su explotación económica realice alguna de las siguientes conductas:

1. Alquile, distribuya, comercialice, exhiba, o publique textos, imágenes, documentos, o archivos audiovisuales de contenido pornográfico a menores de 14 años a través de internet, salas de video, juegos electrónicos o similares.

1.5.6 Ley 599 de 2000. Artículo 218. Pornografía con personas menores de 18 años. El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad, incurrirá en prisión de 10 a 20 años y multa de 150 a 1.500 salarios mínimos legales mensuales vigentes.

Igual pena se aplicará a quien alimente con pornografía infantil bases de datos de Internet, con o sin fines de lucro.

La pena se aumentará de una tercera parte a la mitad cuando el responsable sea integrante de la familia de la víctima.

2. CONTROLES DE GROOMING

2.1. CONTROLES TÉCNICOS

Dentro de las aplicaciones y herramientas que permiten controlar la exposición de los menores de edad al *Grooming* se encuentran:

2.1.1. Control Parental. Se llama Control Parental a cualquier herramienta que permita a los padres controlar y/o limitar el contenido que un menor puede utilizar en la computadora o accediendo en Internet.[14]

Estas herramientas pueden ser automatizadas o no. Las herramientas automatizadas son aplicaciones para la computadora que permiten trabajar en dos niveles de seguridad: la prevención y el control. Ninguna de estas herramientas es 100% efectiva por lo que debemos ser conscientes de la importancia de las herramientas no automatizadas: la educación y la concientización. El diálogo con los menores es la mejor herramienta de prevención para los riesgos que existen en la web.

Todas las herramientas indicadas en la presente sección deben ser aplicadas con el compromiso de la familia, siendo conscientes de cuáles son las configuraciones que se realizan y tomando la responsabilidad sobre cuáles son los contenidos a los que se podrá acceder y a cuáles no.

2.1.1.1. ¿Cómo funcionan las aplicaciones de control parental?. Existen diferentes controles que se pueden aplicar:

- ✓ Herramientas de control de navegación: permite controlar a qué sitios es posible acceder y a qué sitios no. Este es el principal control utilizado y para ello, se utilizan diferentes técnicas de prevención:

    - Listas blancas/negras: en estos casos se utiliza una lista de sitos a los que el menor tiene permitido acceder (lista blanca) o bien permitir la navegación exceptuando los sitios explícitamente denegados (listas negras).

[14] **SEGUKIDS**. Juntos en la Red. Control Parental [En línea], 2012. Disponible en Internet: <http://www.segu-kids.org/padres/control-parental.html>

- Bloqueo por palabras clave: en estos casos la aplicación verifica el contenido del sitio web y bloquea el acceso a aquellos que tengan ciertas palabras ("porno", "sexo", "drogas", "matar", "xxx", etc.). Muchas aplicaciones, permiten personalizar los criterios de severidad (¿cuántas veces debe aparecer una palabra para considerar el sitio como no apto?) e incluso seleccionar las palabras por categorías y agregando palabras específicamente indicadas por el usuario.

- ✓ Bloqueo de aplicaciones: son herramientas que permiten directamente bloquear ciertas aplicaciones como acceso web (www), mensajería instantánea o chat, o correo electrónico.
- ✓ Control de tiempo: estas herramientas limitan el tiempo que un menor puede estar utilizando computadora o conectado a Internet. En su mayoría también permiten controlar a qué horas es posible conectarse. Son útiles para controlar que los horarios y la cantidad de uso sea razonable, acorde a los criterios de cada familia.
- ✓ Navegadores infantiles: Son herramientas que dan acceso a páginas adecuadas para los niños y adolescentes. Tienen un diseño y características apropiadas al público menor y permiten el uso de diferentes perfiles, en función de la edad del usuario. También existen buscadores infantiles con características similares. Algunos navegadores infantiles son Kidsui, Kidrocket, MyKidBrowser y BuddyBrowser.
- ✓ Herramientas que bloquean la información que sale de la computadora: son aplicaciones que impiden revelar información personal. Esto es especialmente útil con respecto a llenar formularios y hojas de registro en línea o comprar a través de la tarjeta de crédito. Puede ser utilizado tanto para la red, como para el correo electrónico, como para los chats, etc.
- ✓ Monitorización: son herramientas que realizan un monitoreo del sistema. Por ejemplo, registran todas las páginas web visitadas para posteriormente poder supervisar los hábitos de navegación de los menores. No son las herramientas más óptimas ya que implican una mayor invasión a la privacidad de los menores y a la vez no son preventivas, sino solo de monitoreo.

2.1.1.2. Aplicaciones para Control Parental. Existen gran cantidad de herramientas que los padres pueden utilizar para control parental. A continuación se listan algunas de ellas, sus características y formas de adquisición.

Tabla 1. Aplicaciones para Control Parental

Aplicación	Características	Sistema Operativo	Tipo
Kidbox	Arranque a pantalla completa apenas se enciende la computadora Control de uso mediante cantidad de horas y franja horaria Historial con el registro de todos los videos, juegos y sitios que se han utilizado. Tambien utiliza "Favoritos" Seguimiento por día, semana o total de los contenidos que han utilizado los niños Buscador, juegos en línea, navegador web, etc.	Windows	Gratuito
Zoodles	Envío de informes semanales a los padres Control de uso mediante cantidad de horas Contenidos (juegos, sitios web, libros, videos) de a cuerdo a la edad y a la valoración de los padres Permite bloquear publicidad Buscador, juegos en línea, navegador web, etc.	Windows / Mac OS / Dispositivos móviles	Gratuito
Norton™ Online Family	Seguimiento de sitios web Control y asignación del tiempo de uso de Internet Supervisión de actividad en las redes sociales Rastreo de las palabras, los términos y las frases que se buscan en línea Envío de alertas por correo electrónico sobre actividades en línea específicas Aptos para niños previamente revisados por maestros y padres	Windows / Mac OS / Dispositivos móviles	Gratuito
Kido'Z	Navegador web Buscador, juegos en línea, videos, etc. Los padres pueden personalizar los sitios bloqueados	Windows / Mac OS	Gratuito
Parental Control Bar	No se instala como aplicación, sino como una barra de tareas complementaria en el navegador Trabaja en dos modos "Child Mode" y "Parental Mode". El cambio de modalidad está protegido por una contraseña. Parental Control Bar Filtrado de contenidos. Posee un botón para agregar rápidamente una dirección web a la lista de sitios bloqueados	Windows 98 /ME / 2000 / XP con Internet Explorer, Mozilla Firefox, Safari	Gratuito

Tabla 1. (Continuación)

Aplicación	Características	Sistema Operativo	Tipo
Cybersitter	Protección por contraseña Se ejecuta oculto al usuario Control de acceso a Internet por día y hora Bloqueo de más de 40.000 sitios fraudulentos Registro de los sitios visitados Registro de chats (Windows Messenger, Yahoo! Messenger y MSN Messenger) Prohibición opcional de redes sociales como Facebook o MySpace Envío de reportes por correo Fácil instalación Seguro. No puede ser deshabilitado por usuarios no autorizados Los padres pueden personalizar los sitios bloqueados	Windows 2000 / XP / Vista	Pago
Net Nanny	Filtrado de contenido ilícito, obsceno o no apto para niños Bloqueo de acceso a aplicaciones (MSN Messenger, Yahoo! Messenger, IRC) Control y asignación del tiempo de uso de Internet Registro de escritura por teclado ante el uso del chat Bloqueo opcional de mensajería instantánea Monitoreo de actividad y uso de Internet (optativo: envío de reportes diarios por correo electrónico)	Windows NT / ME / 2000 / XP	Pago
Control Kids	Filtrado de sitios web de contenido indeseable Anti pop-ups. Anti-spyware Registro de navegación histórico Registro del teclado (keylogger) Limita la descarga de archivos por extensión (MP3, ZIP, EXE, etc.)	Windows 95 / 98 /Me / 2000 / NT / XP	Pago (descarga gratuita por 30 días)
K9 Web Protection	Filtrado de sitios web de contenido indeseable Anti pop-ups. Anti-spyware Registro de navegación histórico Registro del teclado (keylogger) Limita la descarga de archivos por extensión (MP3, ZIP, EXE, etc.)	2000 / XP / Vista	Gratuito
MintNanny	Fácil instalación Solo permite filtrado de navegación por listas negras	Linux	Gratuito

Tabla 1. (Continuación)

Aplicación	Características	Sistema Operativo	Tipo
Gnome-Nanny	Límites de horarios de conexión Control de tiempo de uso de chat, correo electrónico, navegación. Listado de sitios webs permitidos de manera individual para cada usuario.	Linux	Gratuito
Qustodio	Fácil instalación Bloqueo de sitios peligrosos Reglas de navegación Reportes	Windows XP, Vista o 7	Gratuito
Pure Sight	Herramienta de control parental con configuración protegida por contraseña Protección contra el cyberbulling en mensajería instantánea y programas de chat Controla el intercambio de archivos en redes P2P Filtro de contenido web ofensivo Establecer un límite de tiempo para el uso específico de determinadas herramientas, por ejemplo: mensajería instantánea	Windows	Pago (descarga gratuita por 30 días)
FoxFilter	Filtro de Firefox (addons) para control parental que ayuda a bloquear contenido inapropiado: pornografía, otros	Mozilla Firefox	Gratuito
OpenDNS	Implica realizar una modificación en el sistema Filtro de contenido Bloqueo de páginas y contenido inapropiado Bloqueo de archivos dañinos	Windows / Mac OS / Linux	Gratuito
DNS Público de Google	Implica realizar una modificación en el sistema Filtro de contenido Bloqueo de páginas y contenido inapropiado Bloqueo de archivos dañinos	Windows / Mac OS / Linux	Gratuito

Fuente: SEGUKIDS. Juntos en la Red [15]

2.1.2. Modificación de archivo Host. El archivo hosts es solo un pequeño archivo de texto que Windows utiliza como un servidor DNS en el computador, cualquier petición de una dirección URL que se introduzca en el navegador, el sistema operativo comprobará primero si existe alguna referencia a ella en el archivo hosts, si es así utilizará la dirección IP registrada en el para realizar la conexión.

[15] **SEGUKIDS.** Juntos en la Red. Control Parental [En línea], 2012. Disponible en Internet: <http://www.segu-kids.org/padres/control-parental-aplicaciones.html>

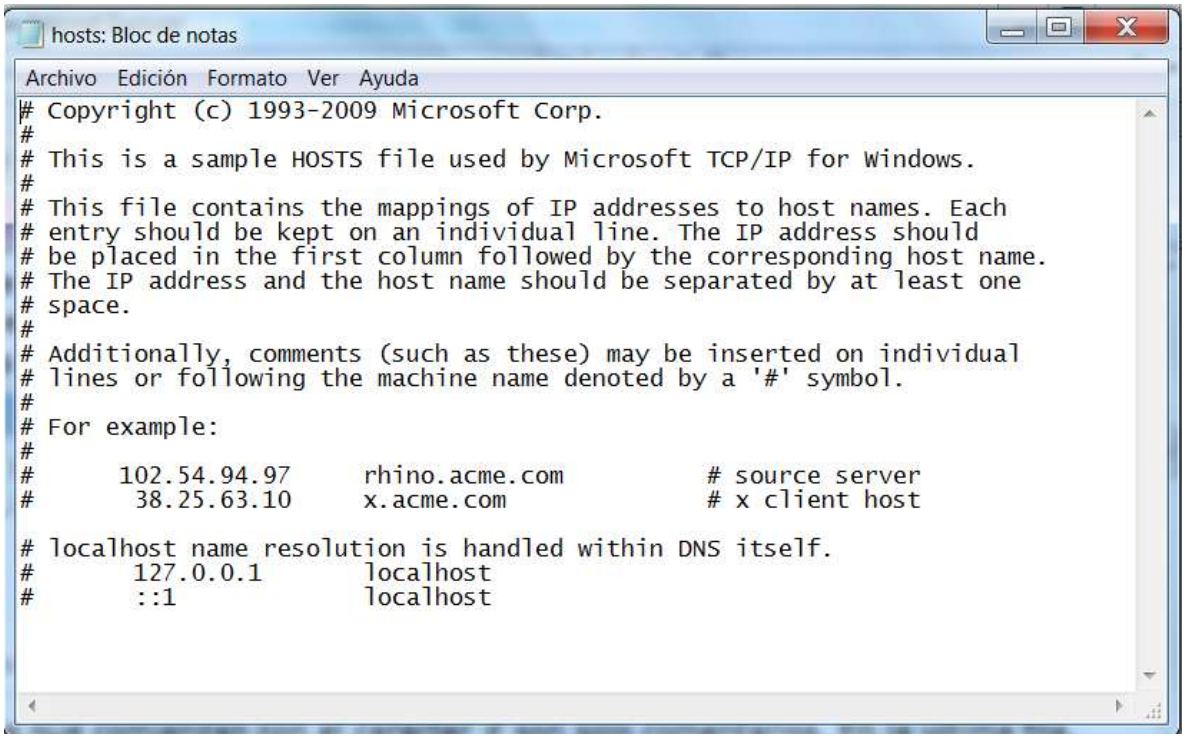
El archivo hosts se encuentra en la siguiente ruta en todos los equipos:

C:\Windows\System32\drivers\etc

Para editarlo se debe arrastrar y soltar encima del Bloc de notas, antes debe cerciorarse que no posee los atributos de solo lectura lo que puede ver y dando un clic derecho en el archivo y seleccionando en el menú la ficha Propiedades.

Al abrirlo podrá observar algo similar a la siguiente imagen:

Figura 1. Edición de archivo Host



Fuente: Propia de Autor

Todas las líneas que comienzan con el carácter # son solo comentarios. En la última fila, la combinación de números en la primera columna es la dirección IP donde Windows buscará el dominio que aparece a continuación.

Como editar el archivo hosts para impedir el acceso a una página web

Para impedir el acceso a una página web, solo es necesario incluir en el archivo host una dirección IP que no le corresponda o preferentemente no sea válida, es decir que no conduzca a ningún lado.

Por ejemplo para impedir el acceso a la página de ejemplo:

http://sitio.com/pagina.htm puede usar la IP 127.0.0.1 que es la del equipo local o la que se muestra en este caso que es una dirección IP inválida.

Se deben tener presentes dos cosas,

1. Debe existir un espacio entre la dirección IP y el nombre del dominio
2. No usar la dirección URL completa, sino solo el dominio del sitio, esto bloqueará todas las páginas contenidas en dicho sitio o dominio.

Dos ejemplos más, bloquear las siguientes páginas:

http://sitio.net/carpeta/pagina.php
https://sitio-lindo.info/cosas/pagina.html

Al terminar de introducir las líneas que se necesiten guarde los cambios hechos. Para desbloquear una página o sitio temporalmente sin eliminar la línea del archivo hosts, solo es necesario anteponer un carácter # que invalida completamente la instrucción de dicha línea.

2.1.3. DD-WRT. Firmware gratuito desarrollado para su uso con enrutadores inalámbricos. Éstos suelen venir con su propio firmware. Sin embargo, el DD-WRT se puede utilizar en lugar del firmware original del enrutador para proporcionar más funciones de servicios de gestión. Puedes establecer una serie de restricciones de acceso a Internet usando DD-WRT.[16]

Es muy común observarlo en equipos Linksys. Ejecuta un reducido sistema operativo basado en Linux. Está licenciado bajo la GNU General Public License versión 2.[17]

DD-WRT v23 Service Pack 1 (SP1) fue lanzado el 16 de mayo de 2006. Se revisó y reescribió gran parte del código durante el desarrollo, y se añadieron muchas características nuevas.

---

[16] **AUSTIN** , Sam n. Cómo bloquear el acceso a sitios web con DD-WRT [En línea], [Publicado el 15 Junio 2012]. Disponible en Internet: <http://www.ehowenespanol.com/bloquear-acceso-sitios-web-ddwrt-como_43837/>

[17]**WIKIPEDIA**. La enciclopedia libre [En Línea]. 2012, actualizado el 29 Diciembre 2012 [Publicado en 13 Agosto 2009]. DD-WRT. Disponible en Internet: <http://es.wikipedia.org/wiki/DD-WRT>

DD-WRT v23 Service Pack 2 (SP2) fue lanzado el 13 de septiembre de 2006. Se revisó la interfaz y se añadieron algunas características. Se soportan algunos modelos más de routers, y se planean aún más. Existe un soporte alfa para algunos routers basados en PowerPC e IXP425; incluyendo magicbox.

DD-WRT v24 lanzado el 18 de mayo de 2008. DD-WRT v24 permitirá hasta 16 interfaces virtuales con diferentes SSID, protocolos de cifrado, PPT Over Wan y una versión para redes de despliegue rápido (Red inalámbrica Mesh).

Con el uso de DD-WRT, se puede restringir el ingreso a un sitio web a determinado cliente, solamente haciendo uso de la dirección IP o MAC del mismo.

2.2. CONTROLES LEGALES

Dentro de la legislación colombiana se encuentran tipificados diferentes delitos que atentan contra la integridad de los menores de edad, para lo concerniente al presente análisis se van a destacar los siguientes:

- ✓ La explotación y abuso sexual (incitación o coacción a la actividad sexual ilegal, explotación en la prostitución, otras prácticas ilegales, explotación en espectáculos o materiales pornográficos).

Así mismo y en busca de preservar los derechos de los menores de edad, y el acceso de estos a cualquier modalidad de información pornográfica, y a impedir el aprovechamiento de redes globales de información con fines de explotación sexual infantil u ofrecimiento de servicios comerciales que impliquen abuso sexual con menores de edad, se establecieron las siguientes normas:

Tabla 2. Controles legales del Grooming en Colombia

LEY / DECRETO / RESOLUCIÓN	FECHA DE EXPEDICIÓN	OBJETO
Ley 679	3, agosto, 2001	Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.
Decreto 1524	24, julio, 2002	Por el cual se reglamenta el artículo 5 de la Ley 679 de 2001.
Ley 1336	21, julio, 2009	Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.
Ley 599	24, julio, 2000	Por la cual se expide el Código Penal.

Fuente: Propia de Autor

3. ANÁLISIS DE LA INFORMACIÓN SOBRE LOS CONTROLES DEL *GROOMING*

3.1. METODOLOGÍA

3.1.1. Recolección de información. Esta investigación consistió en analizar diferentes fuentes de información que permitieron posteriormente realizar unas recomendaciones y concluir frente al control del Grooming en Colombia. Se utilizaron las siguientes técnicas:

- ✓ Herramientas de recolección de información primaria (Encuesta)
- ✓ Inspección ocular a la población objetivo del estudio.
- ✓ Análisis de portales web de los proveedores de servicios de Internet – ISP.
- ✓ Análisis de bibliografías de diferentes autores y a través de medios diversos (impresos y online).

3.1.2. Análisis de los mecanismos de control de Grooming en Colombia. Dado que el fin de esta investigación es establecer un análisis de los mecanismos de control del Grooming en Colombia, fue necesario realizar una evaluación de los controles utilizando la recolección de datos primarios a través de la aplicación de encuestas a establecimientos comerciales (café internet) y determinar las recomendaciones sobre los mismos.

3.1.2.1. Encuesta para el análisis de los mecanismos de control del Grooming en Colombia. Como herramienta de recolección de información se aplicó una encuesta dirigida a la siguiente población:

- ✓ Establecimientos comerciales (café internet) (10)

OBJETIVO. Conocer el nivel de información de los dueños de establecimientos que ofrecen servicios de internet sobre el Grooming en Colombia.

INFORMACION PERSONAL:

Sea tan amable de responder de forma sincera las preguntas que se plantean a continuación:

1. ¿Sabe que es un delito informático?

Sí ___ No ___ Defínalo: _____

_____

_____

_____

_____

2. ¿Conoce del Grooming o Acoso Sexual por Internet?

Sí ___ No ___

3. ¿Conoce entidades de control en Colombia que ayuden a combatir los delitos informáticos, entre ellos el Grooming en Internet?

Sí ___ No ___

4. ¿Conoce la Ley 1336 de 2009?

Sí ___ No ___

5. ¿Sabe que existe una ley que exige la publicación de un reglamento donde se establezcan controles de buen uso del servicio de internet?

Sí ___ No ___

6. ¿Sabe que es un control parental?

Sí ___ No ___

7. ¿Utiliza técnicas que permitan controlar, filtrar o evitar el acceso a sitios web con contenidos de Grooming?

Sí ___ No ___ ¿Cuál? _____

8. Que métodos conoce, que sirvan para evitar el acceso a sitios web restringidos.

_____

_____

_____

_____

9. ¿Cuál es su proveedor de Servicio de Internet?

_____

10. ¿Su proveedor de servicio de internet le ha informado sobre los mecanismos de filtrado que pueden utilizar en sus equipos para evitar y/o controlar el Grooming?

Sí ___ No ___ ¿Cuáles?: _____

_____

_____

11. ¿Conoce campañas, métodos o estrategias que utilice su proveedor de servicio de internet para contrarrestar el Grooming?

Sí ___ No ___ ¿Cuáles?: _____

_____

_____

12. ¿Conoce el enlace de su proveedor de internet a través de cual se puede denunciar el Grooming?

Sí ___ No ___

¡Agradecemos la atención dada a la presente y la sinceridad en cada una de sus respuestas!

3.1.2.2. Análisis de los Portales Web de los Proveedores de Internet – ISP. De igual forma se estableció cuáles son los controles que están utilizando los Proveedores del Servicio de Internet (ISP) en busca de controlar el Grooming, a través de sus portales web.

Dicho análisis se aplicó a los siguientes ISP:

- Claro
- Movistar
- EmCali
- Epm
- Etb
- Media Commerce Telecomunicaciones
- Une
- Telebucaramanga
- Metrotel

Aplicando los siguientes cuestionamientos:

a. ¿Tiene habilitado el link que permita dirigirse a una entidad de Control para realizar la respectiva denuncia en caso de ser necesaria según lo establecido en **artículo 6 del decreto 1524 de 2002?**

b. Implementación de campañas que permitan dar a conocer el Grooming como delito, sus formas de propagación y mitigación.

c. Ofrece el ISP a sus suscriptores un control que permita bloquear el acceso a contenido de Grooming

d. Se encuentra publicada en el portal web del ISP la normatividad que legisla el control del Grooming.

4. ANALISIS ESTADISTICO

4.1. POBLACIÓN Y ANÁLISIS ESTADÍSTICO

4.1.1. Tamaño poblacional. Para la aplicación del instrumento estadístico se determinó el número de establecimientos comerciales que prestan el servicio de internet al público en la ciudad, información obtenida a través de la Cámara de Comercio de Bogotá (Ver Tabla 1. Café internet registrados en la cámara de comercio de Bogotá).

Tabla 3. Café internet registrados en la cámara de comercio de Bogotá

AÑO MATRICULAS	2011	2012
Establecimientos	222	288
Persona Jurídica	19	52
Persona Natural	206	311
TOTAL EST.	**447**	**651**

Fuente: Propia de Autor

4.1.2. Análisis Estadístico. El análisis estadístico se realizó teniendo como soporte la tabla 2, presentada a continuación, que permite establecer el nivel de confianza obtenido al aplicar la encuesta.

Tabla 4. Tabla de apoyo al cálculo del tamaño de una muestra por niveles de confianza

TABLA DE APOYO AL CALCULO DEL TAMAÑO DE UNA MUESTRA POR NIVELES DE CONFIANZA									
Certeza	**95%**	**94%**	**93%**	**92%**	**91%**	**90%**	**80%**	**62,27%**	**50%**
Z	1,96	1,88	1,81	1,75	1,69	1,65	1,28	1	0,6745
Z^2	3,84	3,53	3,28	3,06	2,86	2,72	1,64	1	0,45
E	0,05	0,06	0,07	0,08	0,09	0,1	0,2	0,37	0,5
e^2	0,0025	0,0036	0,0049	0,0064	0,0081	0,01	0,04	0,1369	0,25

Fuente: HERNÁNDEZ LERMA, Onésimo[18]

[18] **HERNÁNDEZ LERMA**, Onésimo. Elementos de probabilidad y estadística, México, Fondo de cultura Económica, 1979, 355 p.

Con el fin de determinar una muestra poblacional se utilizó la siguiente formula estadística:

$$n = \frac{Z^2 pqN}{Ne^2 + (pq)\, Z^2}$$

En donde:

Z = nivel de confianza

N = universo

p = probabilidad a favor

e = error de estimación

q = probabilidad en contra

n = tamaño de la muestra

De acuerdo a lo anterior, se determinó el nivel de confianza con que se deseaba trabajar (Z), donde z= 1.65 para el 90% de confianza o *z* = 1.28 para un 80% de confianza.

Además se debe considerar la probabilidad de que ocurra el evento (p) y la de que no se realice (q); siempre tomando en consideración que la suma de ambos valores p + q será invariablemente siempre igual a 1, se asignó p = 0,50 q = 0,50

Por lo cual:

N = 651; p = 0,5; q = 0,5

$$n = \frac{Z^2 pqN}{Ne^2 + (pq)\, Z^2}$$

$$n = \frac{1{,}64 * 0{,}5 * 0{,}5 * 651}{((651) * (0{,}2)^2) + (0{,}5 * 0{,}5) * 1{,}64}$$

$$n = \frac{266{,}91}{26{,}04 + 0{,}41}$$

$$n = \frac{266{,}91}{26{,}45}$$

$$n = 10{,}091$$

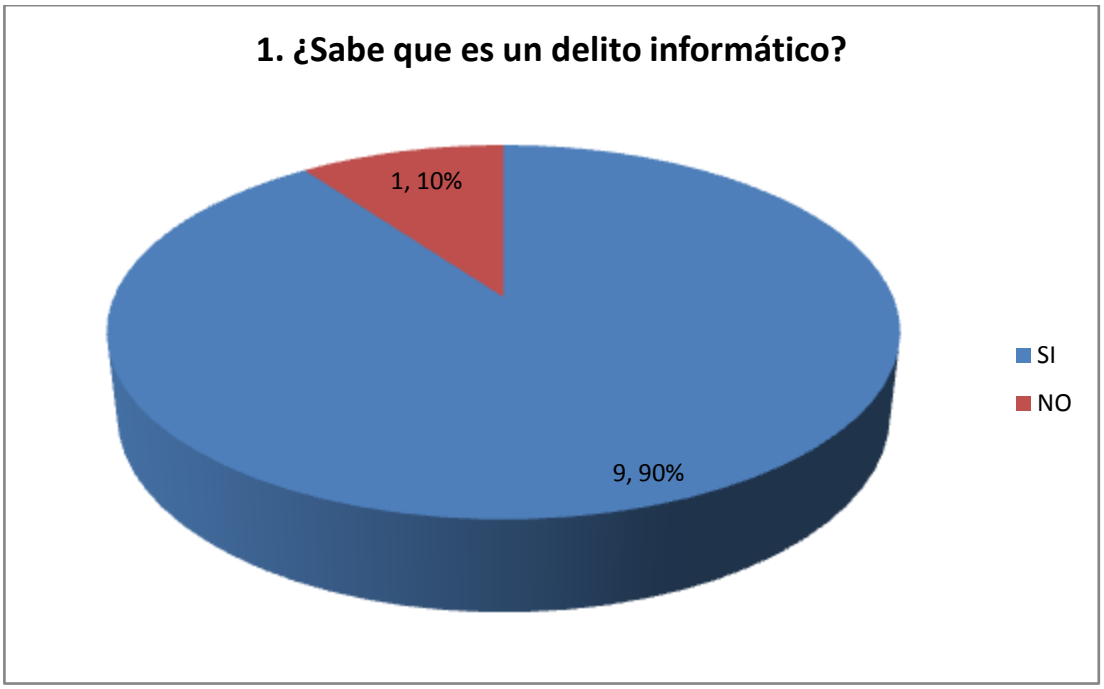
Como conclusión de lo anterior se pudo establecer que el número de encuestas a aplicar fue 10.

4.1.3. Interpretación estadística de la información recolectada.

4.1.3.1. Encuesta Aplicada. Para la recolección de información se aplicó una encuesta de 12 preguntas a los propietarios de 10 café internet, obteniendo los siguientes resultados:

Pregunta No. 1. ¿Sabe que es un delito informático?

Figura 2. Respuesta a la Pregunta No. 1

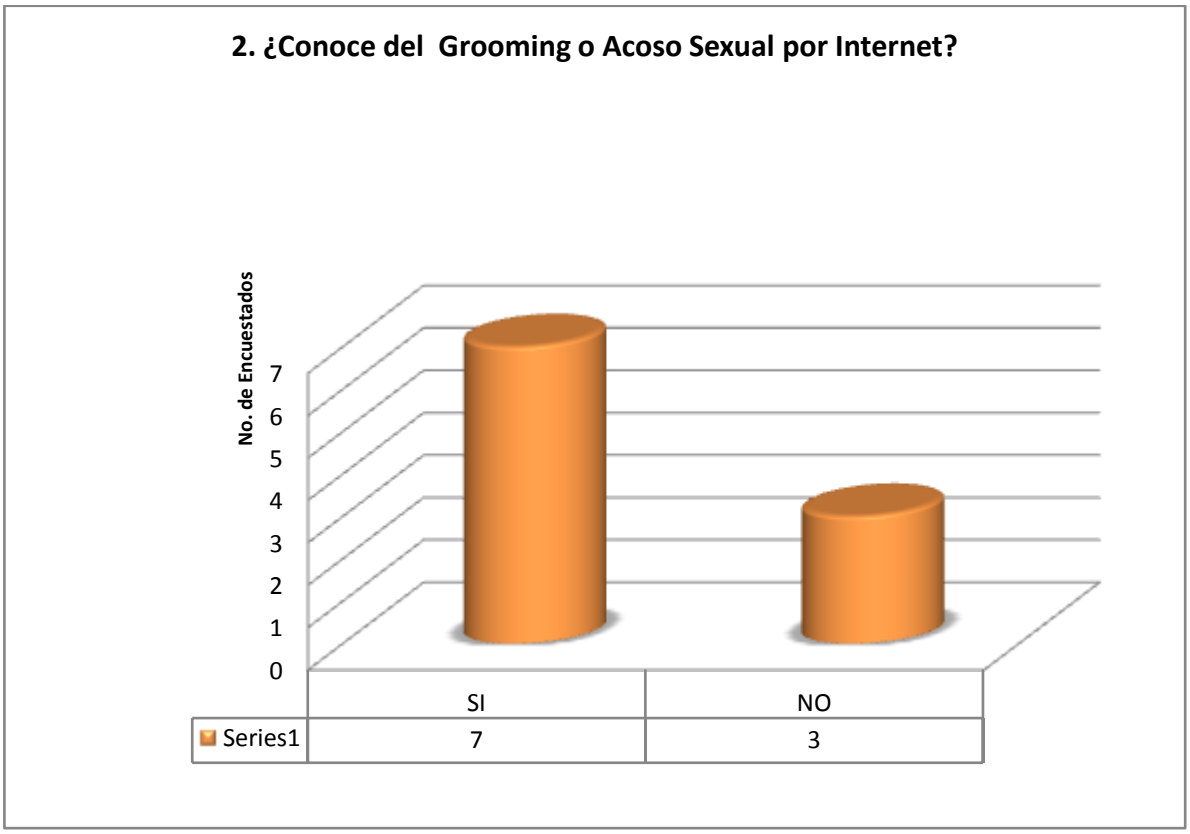


Fuente: Propia de Autor

A la pregunta ¿Sabe que es un delito informático?, el 90% de los encuestados respondió afirmativamente, a pesar de ello, se pudo establecer que el 78% (una población de 7 encuestados) de estos tienen una idea aceptable de lo que es un delito informático. El 12% restante no conocen lo que es un delito informático, lo cual se convierte en un riesgo para quienes hacen uso del servicio ofrecido, principalmente los menores de edad que lo utilizan sin la supervisión de un adulto.

Pregunta No. 2. ¿Conoce del *Grooming* o Acoso Sexual por Internet?

Figura 3. Respuesta a la Pregunta No. 2

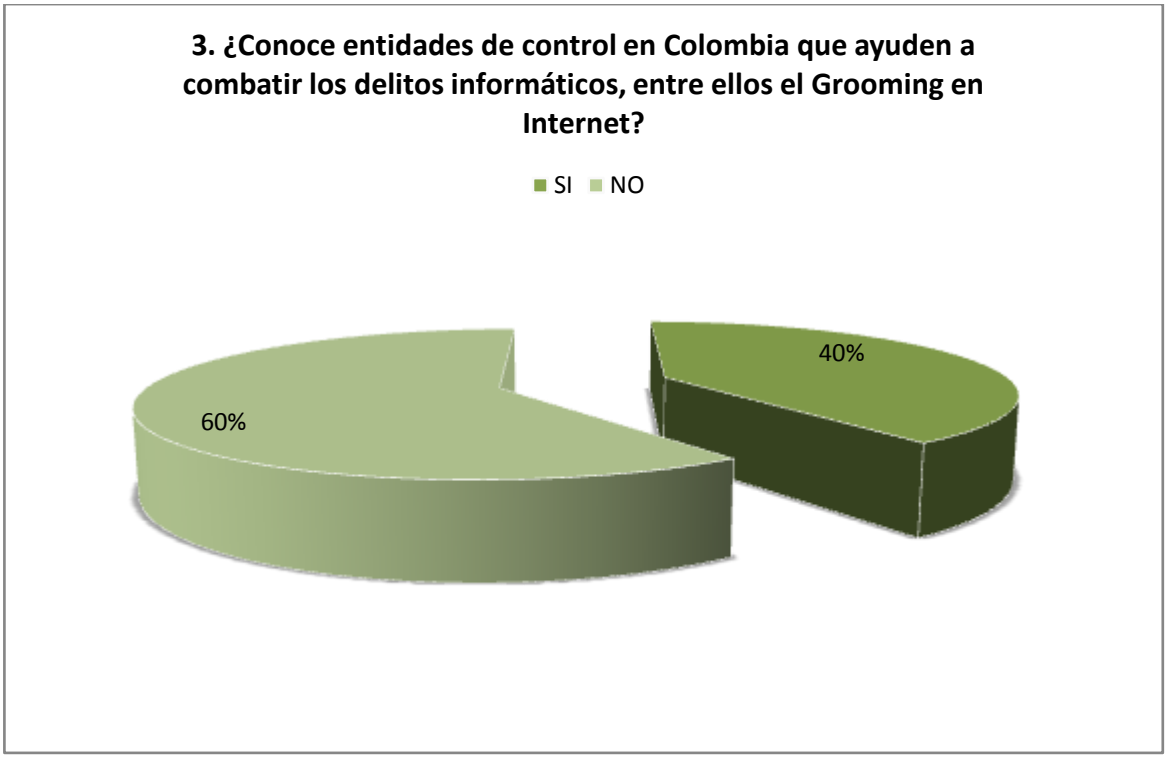


Fuente: Propia de Autor

De las personas encuestadas, el 30% no conoce del Grooming o acoso sexual por internet. Pero el 70% restante no tiene una definición clara del mismo, es preocupante cuando se desconoce lo que es un delito informático con mucha más razón desconocen lo que el Grooming o Acoso Sexual.

Pregunta No. 3. ¿Conoce entidades de control en Colombia que ayuden a combatir los delitos informáticos, entre ellos el Grooming en Internet?

Figura 4. Respuesta a la Pregunta No. 3

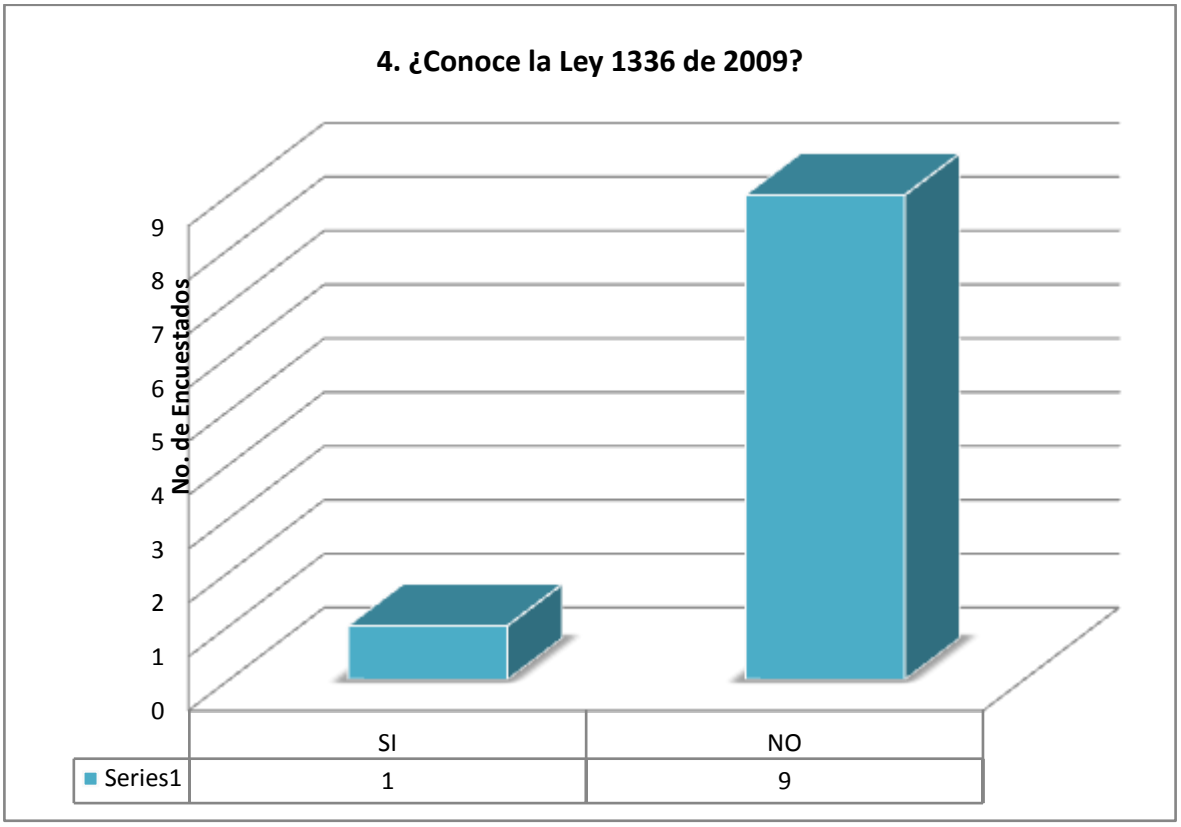


Fuente: Propia de Autor

Con el objetivo de determinar si la población encuestada tiene conocimiento sobre cuáles son las entidades de control que se encargan de regular el acceso de los menores de edad a información con contenidos de *Grooming*, se realizó la siguiente pregunta: ¿Conoce entidades de control en Colombia que ayuden a combatir los delitos informáticos, entre ellos el *Grooming* en Internet?, a lo cual el 60% respondió de forma negativa, mientras que el restante, 40%, aseguró conocer al menos una entidad de control de *Grooming*.

Pregunta No. 4. ¿Conoce la Ley 1336 de 2009?

Figura 5. Respuesta a la Pregunta No. 4



Fuente: Propia de Autor

De la población encuestada el 90% aseguró no tener conocimiento de la Ley 1336 de 2009, que determina la Autorregulación de café internet; teniendo en cuenta que el desconocimiento de las normas no le exime de la culpabilidad, los encuestados se encuentran expuestos a las sanciones a que hace referencia la dicha norma.

Pregunta No. 5. ¿Sabe que existe una ley que exige la publicación de un reglamento donde se establezcan controles de buen uso del servicio de internet?

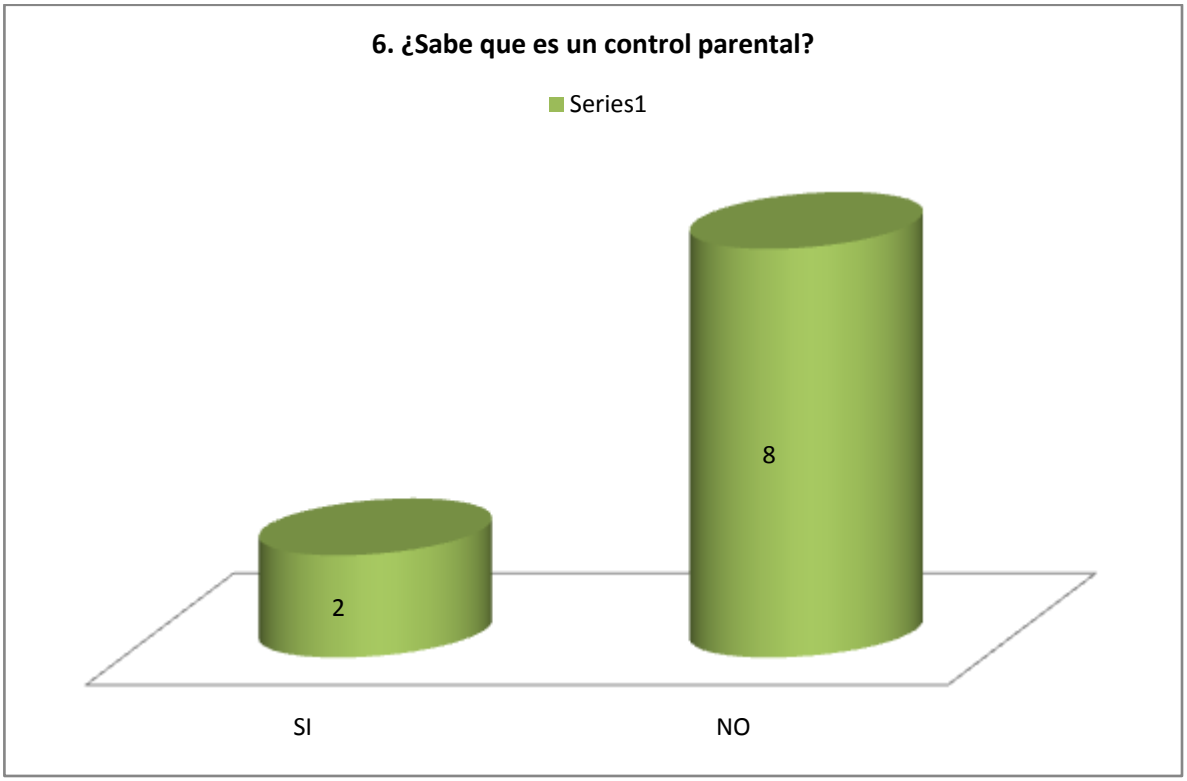
Figura 6. Respuesta a la Pregunta No. 5

Fuente: Propia de Autor

Tan solo el 10% de la población encuestada sabe que existe una regulación que exige a los café internet, la publicación de un reglamento sobre el buen uso que debe darse al internet, lo que permite determinar que no se está cumpliendo con lo establecido en dicha norma, con el objetivo de controlar el acceso a Grooming por parte de los menores de edad.

Pregunta No. 6. ¿Sabe que es un Control Parental?

Figura 7. Respuesta a la Pregunta No. 6

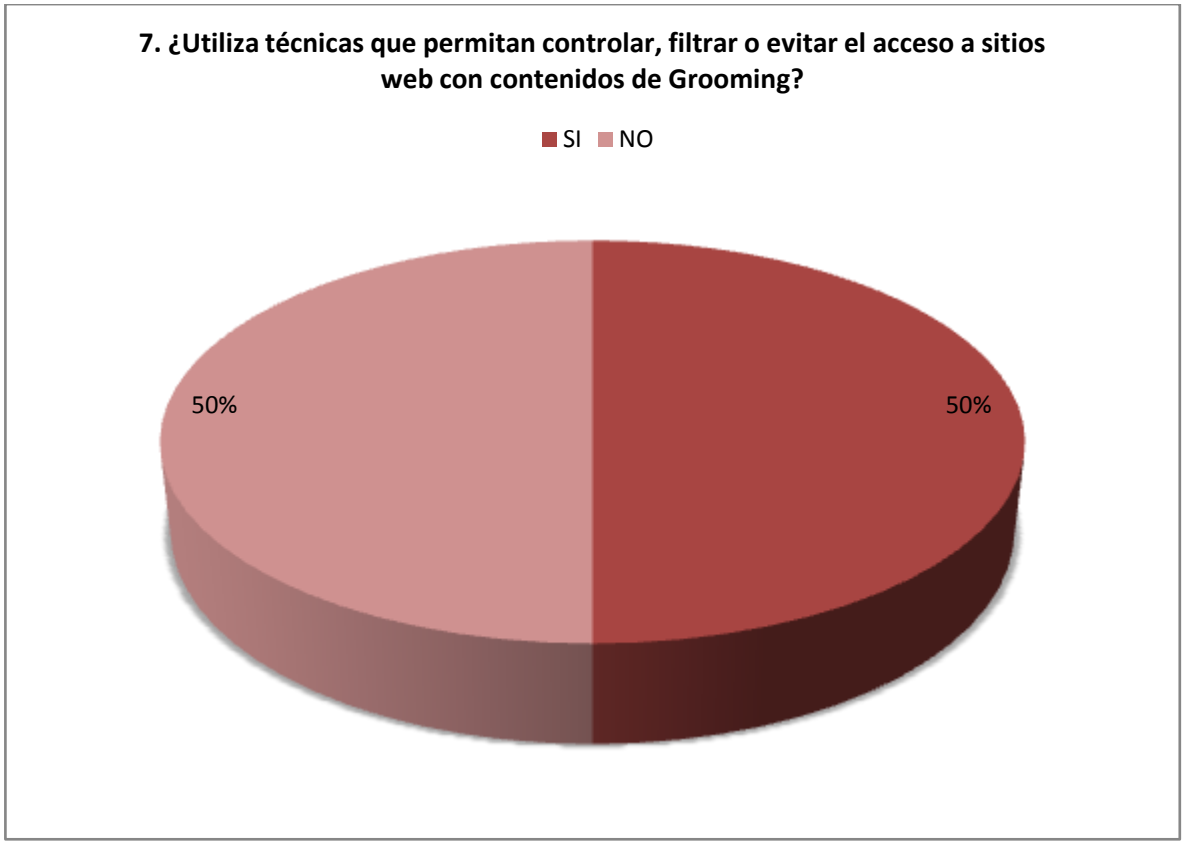


Fuente: Propia de Autor

A pesar del contenido existente en internet que define lo que es un Control parental el 80% de los encuestados contestaron negativamente a la pregunta de si sabían que es Control Parental, esto evidencia además el poco compromiso existente por parte de las entidades encargadas de controlar y regular el Grooming.

Pregunta No. 7. ¿Utiliza técnicas que permitan controlar, filtrar o evitar el acceso a sitios web con contenidos de *Grooming*?

Figura 8. Respuesta a la Pregunta No. 7

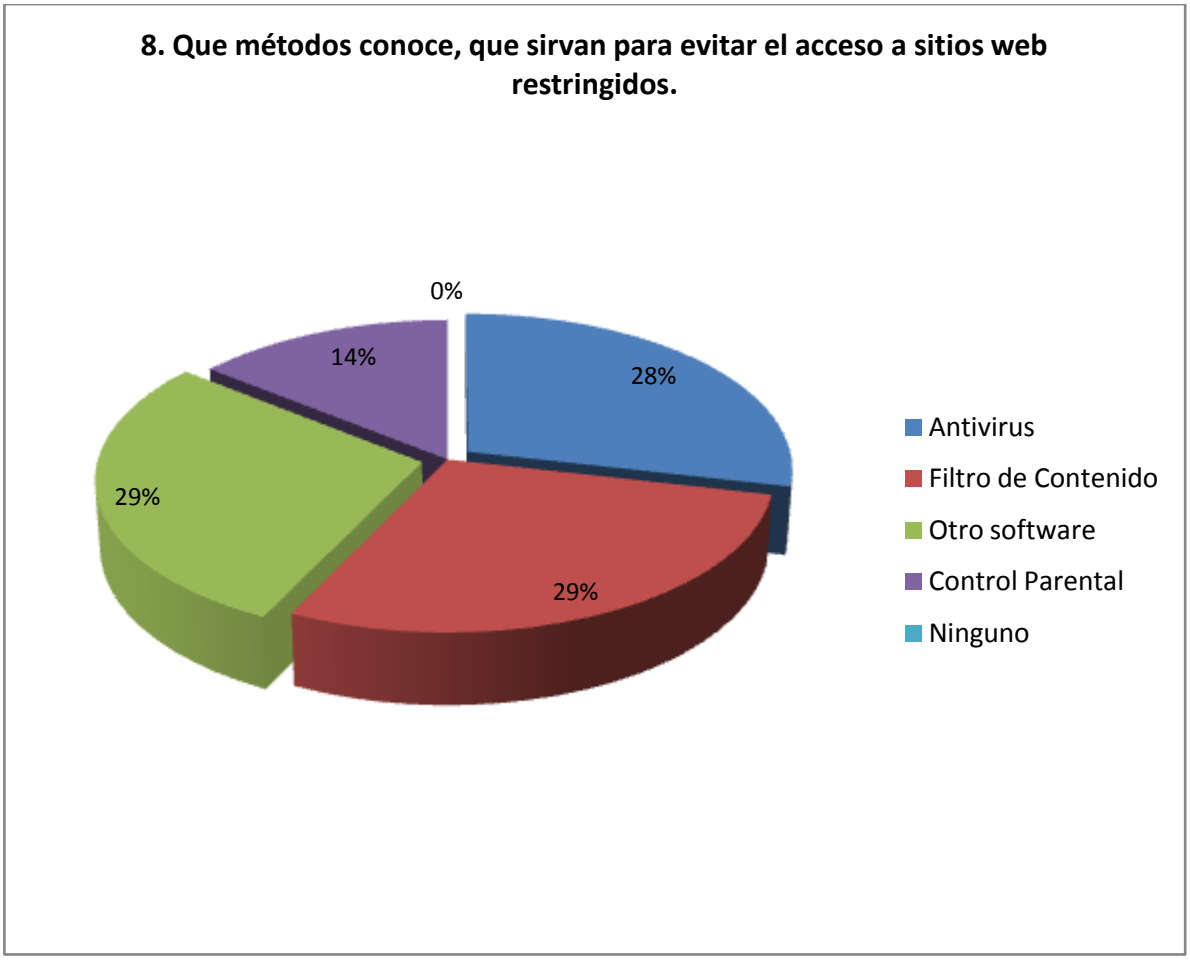


Fuente: Propia de Autor

De la población encuestada el 50% utiliza técnicas que permiten controlar, filtrar o evitar el acceso a sitios web con contenidos de *Grooming*, la más utilizada por quienes afirmaron el uso de dichas técnicas es el Filtro de Contenido, con un 80% de uso. Sin embargo y de acuerdo al análisis realizado en el que se pudo determinar que existen herramientas que se encuentran disponibles en internet y que son de obtención gratuita, para controlar el acceso al Grooming y a información inadecuada, el 50% restante no hace uso de ellas.

Pregunta No. 8. Qué métodos conoce, que sirvan para evitar el acceso a sitios web restringidos.

Figura 9. Respuesta a la Pregunta No. 8

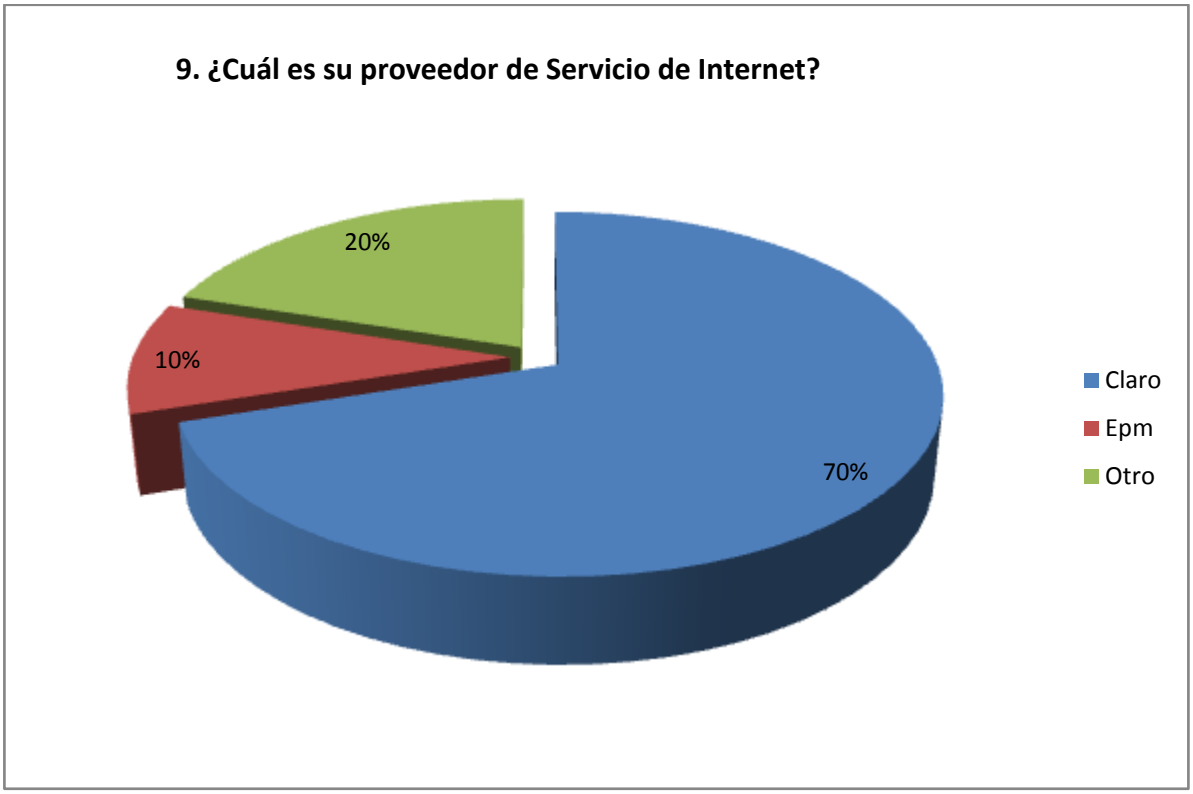


Fuente: Propia de Autor

De los métodos que conocen las personas (70% del total encuestado) que contestaron esta pregunta, se tienen los siguientes: Filtro de contenidos (29%), otro software o aplicación (29%), Antivirus (28%) y Control Parental (14%).

Pregunta No. 9. ¿Cuál es su proveedor de Servicio de Internet?

Figura 10. Respuesta a la Pregunta No. 9

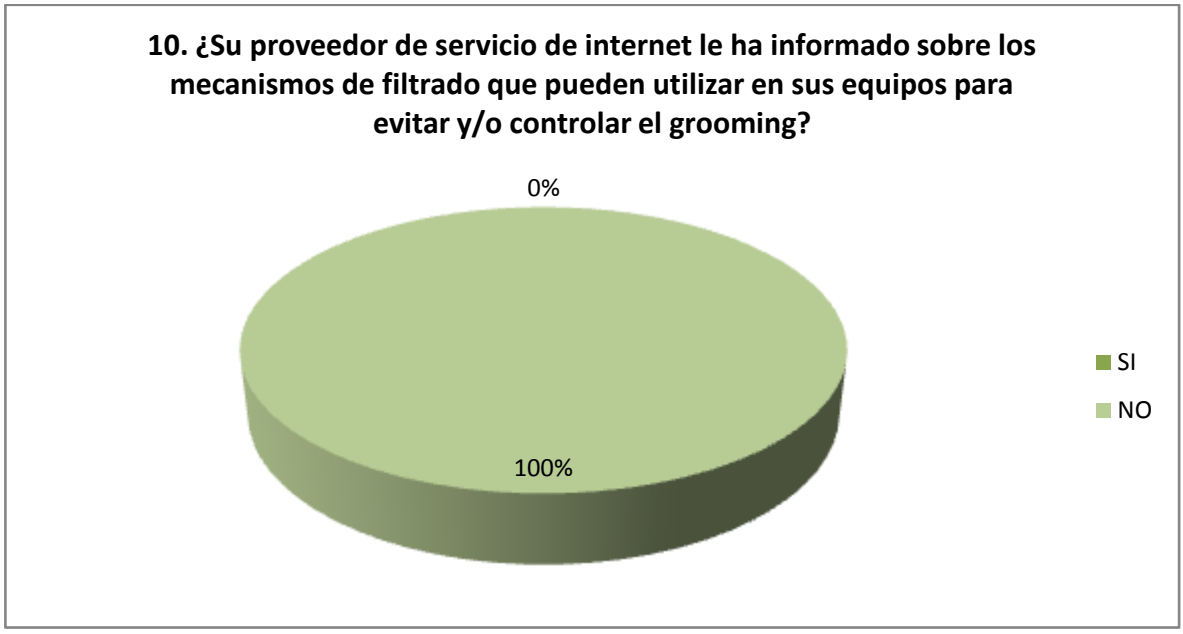


Fuente: Propia de Autor

Se pudo determinar que el ISP más utilizado es CLARO, con un 70% de contratación según la población encuestada, y el menos contratado es EPM con un 10%.

Pregunta No. 10. ¿Su proveedor de servicio de internet le ha informado sobre los mecanismos de filtrado que pueden utilizar en sus equipos para evitar y/o controlar el Grooming?

Figura 11. Respuesta a la Pregunta No. 10

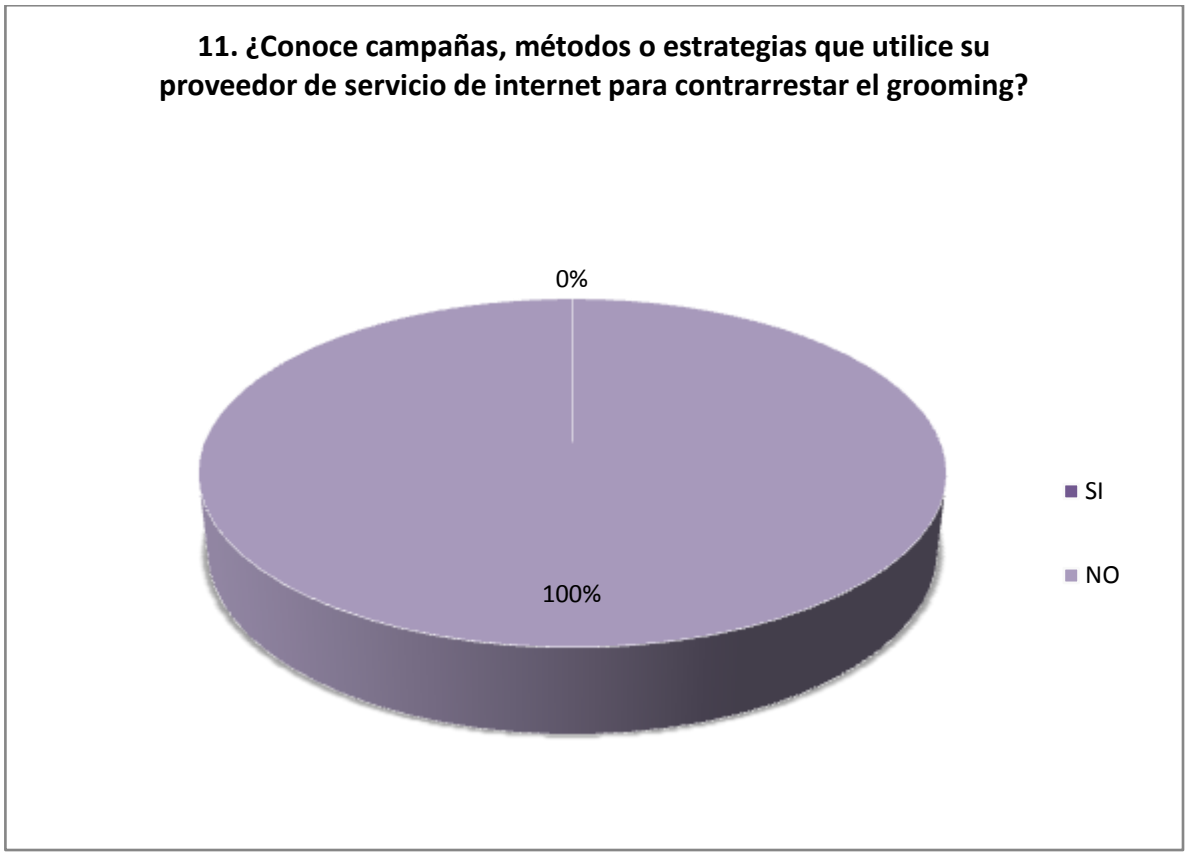


Fuente: Propia de Autor

De acuerdo a la respuesta dada por los encuestados, el total de Proveedores de Servicio de internet – ISP, no informa a sus suscriptores sobre mecanismos de filtrado que permita evitar y/o controlar el Grooming, incumpliendo de esta forma la aplicación del Decreto 1524 de 2002 que determina la obligación de los mismos de ofrecer o informar a sus usuarios sobre la existencia de mecanismos de filtrado que puedan ser instalados en los equipos de estos.

Pregunta No. 11. ¿Conoce campañas, métodos o estrategias que utilice su proveedor de servicio de internet para contrarrestar el *Grooming*?

Figura 12. Respuesta a la Pregunta No. 11

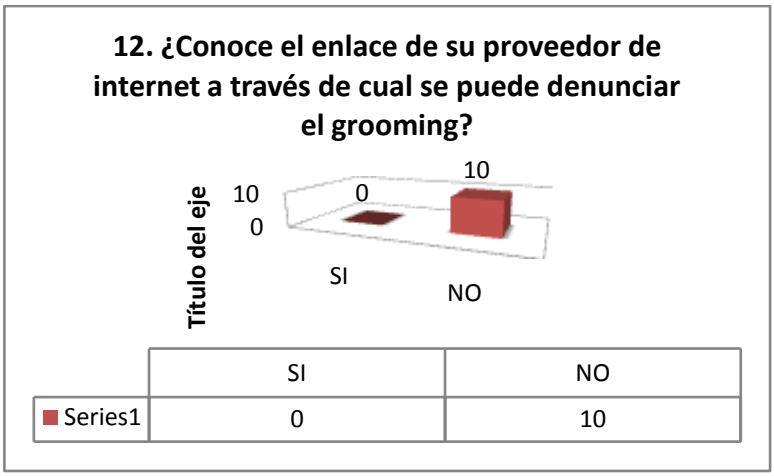


Fuente: Propia de Autor

Teniendo en cuenta que la pregunta No. 11 indaga sobre el conocimiento que existe en los encuestados sobre campañas, métodos o estrategias utilizadas por su Proveedor de Servicio de Internet con el fin de mitigar o contrarrestar el Grooming, se pudo establecer que el 100% de estos no conoce ninguna que esté desarrollando dicho proveedor.

Pregunta No. 12. ¿Conoce el enlace de su proveedor de internet a través de cual se puede denunciar el *Grooming*?

Figura 13. Respuesta a la Pregunta No. 12



Fuente: Propia de Autor

Según el conocimiento que los encuestados tienen sobre su ISP, el 100% desconoce si este tiene un link en su portal web que permita denunciar el Grooming.

4.1.3.2. Análisis de portales Web. Con el fin de determinar si los Proveedores de Servicio de Internet, promueven el control del Grooming según lo establece la legislación nacional, se realizó un análisis en sus portales web, del cual se obtuvieron los resultados que se describen a continuación.

Pregunta No. 1. ¿Tiene habilitado el link que permita dirigirse a una entidad de Control para realizar la respectiva denuncia en caso de ser necesaria según lo establecido en artículo 6 del decreto 1524 de 2002?

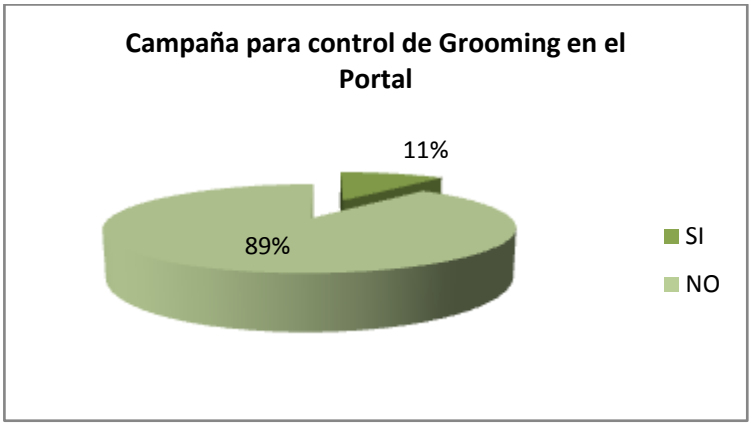
Figura 14. Respuesta a la Pregunta No. 1

Fuente: Propia de Autor

La totalidad de portales analizados (9), no tienen un link habilitado que se relacione con la denuncia del *Grooming* en caso de necesidad.

Pregunta No. 2. Implementación de campañas que permitan dar a conocer el Grooming como delito, sus formas de propagación y mitigación.

Figura 15. Respuesta a la Pregunta No. 2

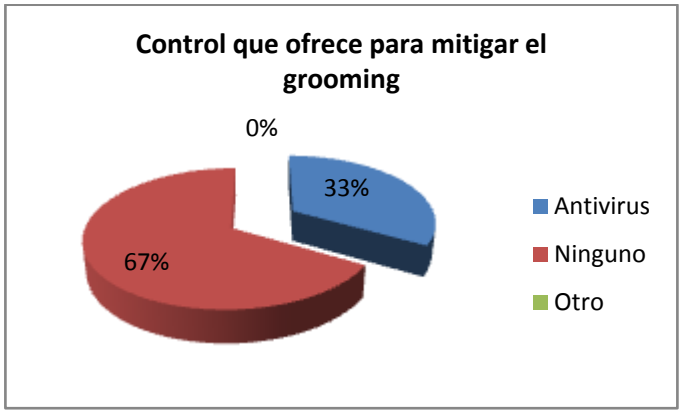


Fuente: Propia de Autor

De los 9 ISP (100%) analizados, tan solo 1 tiene publicada en su portal web una campaña para la mitigación del Grooming, este es ISP es ETB y la campaña se denomina: Estrategia - Zona Segura Guardián de Contenidos.

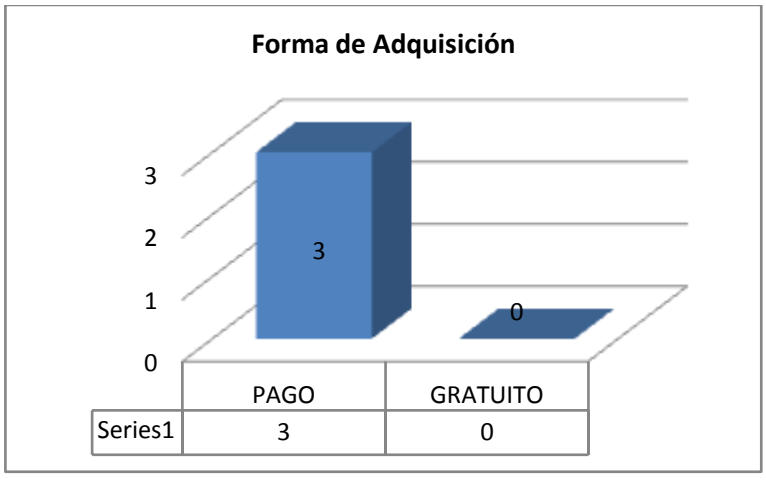
Pregunta No. 3. Ofrece el ISP a sus suscriptores un control que permita bloquear el acceso a contenido de Grooming

Figura 16. Respuesta a la Pregunta No. 3



Fuente: Propia de Autor

Figura 17. Respuesta a la Pregunta No. 3.1



Fuente: Propia de Autor

Del 100% de los ISP analizados, tan solo el 33% (3 ISP) ofrece a los suscriptores una alternativa que permite bloquear la información con contenido de *Grooming*, dicha alternativa es un antivirus y su adquisición con pago.

Pregunta No. 4. Se encuentra publicada en el portal web del ISP la normatividad que legisla el control del Grooming.

Figura 18. Respuesta a la Pregunta No. 4

Fuente: **Propia de Autor**

De los ISP analizados, el 56% tiene publicada la normatividad referente al Grooming, precisamente la estrategia INTERNET SANO, mientras que el 44% restante no hace mención a esta.

RECOMENDACIONES

Como resultado del análisis realizado a los controles aplicados en pro de la prevención del Grooming, se determinaron las siguientes recomendaciones para los diferentes actores responsables del control del mismo:

Los padres y comunidad en general

Hoy en día, Internet se ha convertido en una herramienta imprescindible en la vida de los adultos, y lo mismo sucede con los jóvenes. Por eso, lo padres deben comprender que sus hijos quieran y deban usar el computador con conexión a Internet tanto para hacer tareas escolares como para divertirse durante ratos de ocio y estar en contacto con sus amigos.

Es muy importante que los padres comprendan lo positivo que es para sus hijos el uso de Internet, pero a la vez deben ser muy conscientes de los peligros que conlleva y deben ayudarles a mitigarlos para conseguir una navegación segura.

A continuación se describen algunas prácticas que se deben tener en cuenta para guiar a los hijos en el uso de la red.

- ✓ Hay que educar al menor sobre los posibles peligros que puede encontrar en la Red.

- ✓ Se debe acompañar al menor en la navegación cuando sea posible, sin invadir su intimidad.

- ✓ Es importante advertir al menor de los problemas que conlleva facilitar información personal (nombre, dirección, teléfono, contraseñas, fotografías, etc.) a través de cualquier canal.

- ✓ Hay que informarle de que no todo lo que sale en Internet es cierto, ya que pueden engañarle con facilidad.

- ✓ Se debe prestar la misma atención a sus «ciber amistades» que a sus amistades de la vida real.

- ✓ El menor debe informar a sus padres de cualquier conducta o contacto que le resulte incómodo o sospechoso.

- ✓ Hay que vigilar el tiempo de conexión del menor a Internet para evitar que desatienda otras actividades.

- ✓ Se debe crear una cuenta de usuario limitado para el acceso del menor al sistema.

- ✓ Deben primar las recomendaciones y normas antes que las prohibiciones y castigos por un uso incorrecto de Internet.

- ✓ Asegurar la red de datos en su hogar. Si no tiene conocimiento de cómo hacerlo, asesórese de un profesional en el área. Esto puede hacerlo instalando y actualizando continuamente software de seguridad (firewall, anti spyware, anti adware, antivirus) que le permita bloquear los intentos de intrusión y robo de información.

- ✓ Haga uso de contraseñas fuertes (las contraseñas fuertes son aquellas que contengan no menos de 8 caracteres compuestos por letras (mayúsculas y minúsculas), números y caracteres especiales (¡·$%&/()=?¿*+-_.:,;))

- ✓ Aprenda todo lo que sea necesario sobre tecnologías para saber que hacen sus hijos y cuáles son los riegos a los cuáles están expuestos.

- ✓ A continuación se nombran algunos controles tipo software que se pueden aplicar para prevenir el Grooming:

    - Herramientas de control de navegación: permite controlar a qué sitios es posible acceder y a qué sitios no. Este es el principal control utilizado y para ello, se utilizan diferentes técnicas de prevención:

        - Listas blancas/negras: en estos casos se utiliza una lista de sitos a los que el menor tiene permitido acceder (lista blanca) o bien

permitir la navegación exceptuando los sitios explícitamente denegados (listas negras).

- Bloqueo por palabras clave: en estos casos la aplicación verifica el contenido del sitio web y bloquea el acceso a aquellos que tengan ciertas palabras ("porno", "sexo", "drogas", "matar", "xxx", etc.). Muchas aplicaciones, permiten personalizar los criterios de severidad (¿cuántas veces debe aparecer una palabra para considerar el sitio como no apto?) e incluso seleccionar las palabras por categorías y agregando palabras específicamente indicadas por el usuario.

- ✓ Bloqueo de aplicaciones: son herramientas que permiten directamente bloquear ciertas aplicaciones como acceso web (www), mensajería instantánea o chat, o correo electrónico.

- ✓ Control de tiempo: estas herramientas limitan el tiempo que un menor puede estar utilizando computadora o conectado a Internet. En su mayoría también permiten controlar a qué horas es posible conectarse. Son útiles para controlar que los horarios y la cantidad de uso sea razonable, acorde a los criterios de cada familia.

- ✓ Navegadores infantiles: Son herramientas que dan acceso a páginas adecuadas para los niños y adolescentes. Tienen un diseño y características apropiadas al público menor y permiten el uso de diferentes perfiles, en función de la edad del usuario. También existen buscadores infantiles con características similares. Algunos navegadores infantiles son Kidsui, Kidrocket, MyKidBrowser y BuddyBrowser.

- ✓ Herramientas que bloquean la información que sale de la computadora: son aplicaciones que impiden revelar información personal. Esto es especialmente útil con respecto a llenar formularios y hojas de registro en línea o comprar a través de la tarjeta de crédito. Puede ser utilizado tanto para la red, como para el correo electrónico, como para los chats, etc.

- ✓ Monitorización: son herramientas que realizan un monitoreo del sistema. Por ejemplo, registran todas las páginas web visitadas para

posteriormente poder supervisar los hábitos de navegación de los menores. No son las herramientas más óptimas ya que implican una mayor invasión a la privacidad de los menores y a la vez no son preventivas, sino solo de monitoreo.

Dentro de las múltiples herramientas que pueden utilizarse se encuentran las siguientes:

Tabla 5. Herramientas de monitoreo

Kidbox	• Arranque a pantalla completa apenas se enciende la computadora • Control de uso mediante cantidad de horas y franja horaria • Historial con el registro de todos los videos, juegos y sitios que se han utilizado. Tambien utiliza "Favoritos" • Seguimiento por día, semana o total de los contenidos que han utilizado los niños • Buscador, juegos en línea, navegador web, etc.	Windows	Gratuito
Zoodles	• Envío de informes semanales a los padres • Control de uso mediante cantidad de horas • Contenidos (juegos, sitios web, libros, videos) de a cuerdo a la edad y a la valoración de los padres • Permite bloquear publicidad • Buscador, juegos en línea, navegador web, etc.	Windows / Mac OS / Dispositivos móviles	Gratuito
Norton™ Online Family	• Seguimiento de sitios web • Control y asignación del tiempo de uso de Internet • Supervisión de actividad en las redes sociales • Rastreo de las palabras, los términos y las frases que se buscan en línea • Envío de alertas por correo electrónico sobre actividades en línea específicas • aptos para niños previamente revisados por maestros y padres	Windows / Mac OS / Dispositivos móviles	Gratuito

Fuente: **Propia de Autor**

- ✓ Dé confianza a sus hijos para que cuenten que acostumbran a hacer en internet, con quien conversan, observe y esté pendiente de qué hacen sus hijos cuando van a la casa de sus amigos, cuáles son sus páginas de preferencia.

- ✓ Identifique cuáles son las entidades de control, las estrategias para prevenir el grooming, los link de denuncias, entre las páginas que utilizan las entidades de control para prevenir el Grooming están:

  En Ticconfio
  Interne sano
  Cero tolerancia

  Estas campañas promovidas por el Ministerio de las tecnologías y las telecomunicaciones, donde se unen el ICBF, la Policía Nacional. Los porveedores de internet, habilitando la creación de una línea gratuita nacional dirigida a proveedores y usuarios de redes globales, donde se informa las implicaciones legales de su uso en relación con la Ley. Se creó un sitio Web www.internetsano.gov.co, donde formular denuncias contra eventos de explotación sexual infantil y señalar páginas electrónicas que se ofrezcan servicios sexuales con niñas, niños y jóvenes.

- ✓ Los padres de familia deben ser los mayores responsables de la seguridad de los menores y mantenerse al tanto de los peligros del internet como es el grooming, denunciar si notan que observen cualquier conversación o actitud extraña de sus hijos, asegurar los equipos para evitar que sus hijos se arriesguen.

- ✓ Los padres deben aprender y conocer las leyes en cuanto a la seguridad de la información que hay vigentes, entre ellas están:

  - o la ley 679 del 2001: tiene por objeto dictar medidas de protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad, mediante el establecimiento de normas de carácter preventivo y sancionatorio, y la expedición de otras disposiciones en desarrollo del artículo 44 de la Constitución.

  - o La constitución de 1991, Art. 44 y 45: Protección de los menores de edad.

Propietarios de los establecimientos comerciales (cafés internet)

1. Exigir a los Proveedores de Internet que programas de filtrado tienen para el control de programas de contenido obsceno gratuitos tienen.

2. Conocer y aprender los delitos informáticos que se encuentran y que son un riesgo para las personas que utilizan sus servicios, más importante aún si son menores de edad.

3. Poner las Políticas de Seguridad en un lugar visible, para cada persona que utilice los servicios.

4. No permitir que los menores de edad utilicen internet sin ser acompañados de un adulto o del padre de familia, es un lugar para servicio de internet no para cuidar los niños.

5. Conocer y aprender las leyes en cuanto a la protección del gooming en los niños. Entre éstas leyes está:

Ley 1336 de 2009: Artículo 4. Autorregulación de café internet. Todo establecimiento abierto al público que preste servicios de Internet o de café Internet deberá colocar en lugar visible un reglamento de uso público adecuado de la red, cuya violación genere la suspensión del servicio al usuario o visitante.

Ese reglamento, que se actualizará cuando se le requiera, incluirá un sistema de autorregulación y códigos de conducta eficaces que promuevan políticas de prevención de explotación sexual de niños, niñas y adolescentes, y que permitan proteger a los menores de edad de toda forma de acceso, consulta, visualización o exhibición de pornografía.

Un modelo de estos sistemas y códigos se elaborará con la participación de organismos representativos del sector. Para estos efectos, el Ministerio de Comunicaciones convocará a los interesados a que formulen por escrito sus propuestas de autorregulación y códigos de conducta. Tales códigos serán adoptados dentro del año siguiente a la vigencia de la presente ley, copia de los cuales se remitirá a la oficina que indique el Ministerio de Comunicaciones, de su propia estructura o por delegación a los municipios y distritos, y serán actualizados cada vez que el Ministerio de Comunicaciones lo considere necesario en función de nuevas leyes, nuevas políticas o nuevos estándares de protección de la niñez adoptados en el seno de organismos internacionales, gubernamentales o no.

Las autoridades distritales y municipales realizarán actividades periódicas de inspección y vigilancia de lo dispuesto en este artículo y sancionarán su incumplimiento de conformidad con los procedimientos contenidos en el Código Nacional de Policía y los códigos departamentales y distritales de policía que apliquen.

El incumplimiento de los deberes a que alude esta norma dará lugar a las mismas sanciones aplicables al caso de venta de licor a menores de edad.

Proveedores de servicio de internet - ISP

1. Promulgar y dar a conocer a quien utilice el Servicio de internet que existen riesgos en la red y que hay programas de filtrado para controlarlos. (Padres, Establecimientos comerciales, Instituciones educativas, etc.).

2. Capacitar a sus asesores para brindar información sobre el uso correcto de las redes, los riesgos que existen entre ellos el Grooming, las estrategias de control.

3. cumplir puntualmente la legislación vigente en Colombia que busca controlar el Grooming.

CONCLUSIONES

De acuerdo al análisis realizado por medio de las encuestas aplicadas, inspección ocular a los café internet, observación de los portarles web de los proveedores de Servicios de Internet - ISP, lecturas y análisis de información sobre control del Grooming, la legislación colombiana vigente que busca imponer el control al acceso de menores de edad a material pornográfico, a través del uso de las redes globales, obtenemos las siguientes conclusiones:

1. La mayoría de la población cree saber que es un delito informático, cada quien le da su propia interpretación. Igualmente, el conocimiento de lo que es Grooming o Acoso Sexual en la red a menores de edad, es deficiente o ambiguo; facilitando la materialización del riesgo a la exposición de información con contenidos pornográficos a menores de edad a través de internet.

2. De acuerdo a lo establecido en las normas legales vigentes, el Estado representado por los entes de control (en este caso Policía Nacional), se encuentra obligado a verificar que los prestadores de Servicio de Internet (ISP y Café Internet) cumplan con unas condiciones mínimas para la prestación del servicio, obligación que hasta el momento no se está cumpliendo.

3. Los establecimientos que prestan el servicio a los usuarios finales utilizan herramientas tecnológicas – Antivirus y/o filtros de contenidos – tratando de evitar el acceso menores de edad a sitios web con contenido pornográfico, siendo insuficiente para el control del Grooming, puesto que hace falta cultura o educación en el tema. Además de proveer herramientas que restrinjan el acceso a esta información deben tener exhibido un reglamento de normas de uso adecuado del servicio, algo que no se encuentra en los establecimientos visitados.

4. Dentro de las obligaciones de los ISP se encuentra el ofrecer a los suscriptores del servicio herramientas tecnológicas que les permitan a estos controlar los contenidos de Grooming en sus propios equipos, a pesar de ello y de estar legislado, se evidencia su incumplimiento, aumentando el riesgo para la población objetivo de los delincuentes que cometen este delito.

5. Existe el número suficiente de normas que permitan controlar el Grooming, la literatura sobre el mismo es abundante tanto en medios impresos como

en las redes, pero su puesta en práctica es insuficiente, permitiendo el aumento del delito. Las estrategias publicitarias en pro del control del Grooming por parte de los responsables son escasas, casi nulas. Está claro que existen las herramientas técnicas y los controles legales, pero la mayoría inutilizados.

La mayoría de las personas, disponen de un teléfono móvil, que les permite: llamar, enviar mensajes, hacer fotos, consultar la agenda, etc. Ya que es un dispositivo muy personal y con mucha información privada, es un buen motivo para mantenerlo seguro.

Los dispositivos móviles inteligentes, más conocidos como smartphones, son una fusión (y evolución) de los ordenadores actuales y, por tanto, son muchos los riesgos que también les afectan. Además, el uso cada vez más generalizado de estos dispositivos, hace que los atacantes lo incluyan dentro de sus objetivos preferidos.

Por lo anterior surgen otros interrogantes: ¿cuáles son los controles técnicos y/o legales que aplican a los dispositivos móviles inteligentes? ¿Cuáles son los controles utilizados en los lugares de libre acceso a internet (centros comerciales, terminales de transporte – aéreo y terrestre – y algunos establecimientos comerciales)? ¿Existe legislación que puntualice controles en los dispositivos inteligentes?, los menores de edad tiene acceso ilimitado un sin número de elementos tecnológicos que permiten su acceso y libre navegación en internet, situación que incrementa los riesgos y las amenazas, situación que hace que éstas se materialicen; se puede concluir que con la diversificación de medios tecnológicos los controles deben ir en aumento, se deben plantear, promulgar y aplicar, situación que simplemente ha llegado hasta su planteamiento, siendo ineficiente para evitar el grooming.

BIBLIOGRAFÍA

WIKIPEDIA. La Enciclopedia Libre. [En Línea], 2012, actualizado el 29 Diciembre 2012 [Publicado en 13 Agosto 2009]. Firmware. Disponible en Internet: <http://es.wikipedia.org/wiki/Firmware>.

EXPLOTACIÓN SEXUAL COMERCIAL DE NIÑOS, NIÑAS Y ADOLESCENTES E INTERNET. X Informe al Secretario General de la OEA sobre las medidas emprendidas por los Estados Miembros para prevenir y erradicar la Explotación Sexual Comercial de niñas, niños y adolescentes en las Américas. Montevideo, Febrero, Vol. 1, 2011. 10 Ed. 31 p.

Grooming o Ciber acoso. [En Línea] Villa Rica, Chile. Informática y Rock & Roll. [Publicado el 23 Mayo 2009] Disponible en Internet: <http://javierzg.wordpress.com/2009/05/23/grooming-ciberacoso>.

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Enciclopedia Jurídica [En Línea], 2012, León, España, actualizado el 08 Febrero 2012 [Publicado en Noviembre 2007]. Observatorio de Seguridad de la Información. Grooming. Disponible en Internet: <http://www.inteco.es/wikiAction/Seguridad/Observatorio/area_juridica_seguridad/Enciclopedia/Articulos_1/Grooming>.

INSTITUCIÓN EDUCATIVA CAMPOS Y TOROZOS. Principales riesgos en las Redes Sociales [En Línea], 2010, León y Castilla, España, [Publicado el Agosto 2010]. Disponible en Internet: <https://sites.google.com/site/riesgosredessociales2011/grooming/2-1---definicion>.

FLOREZ HERNÁNDEZ, Jorge. Decálogo para combatir el Grooming y el acoso sexual infantil. Internet Grooming [En Línea], 1994 – 2009. Disponible en Internet: <http://www.internet-grooming.net/decalogo-grooming-acoso-sexual-menores-online.html>

INTERNET LAW FORUM - PROTECTION OF CHILDREN AGAINST ABUSE THROUGH NEW TECHNOLOGIES - CYBERCRIME CONVENTION COMMITTEE [En Línea]. Estados Unidos: **COUNCIL OF EUROPE** (ETS no. 185) [Publicado el 06 Julio de 2011] Disponible en Internet: <http://socialnetwork.ibls.com/forums/topic/271/cyber-bullying>

BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. Grooming: nueva táctica de contacto de pedófilos [En Línea], 2008, Chile [Publicado el 21 Junio 2008]. El Grooming en otras legislaciones. Disponible en Internet:

<http://www.bcn.cl/carpeta_temas_profundidad/grooming-acoso-sexual-ninos/#el-grooming-en-otras-legislaciones >.

COLLI, Nieves. Tribunal Nacional Argentino. Luz verde a un Código Penal consensuado que sube las penas a terroristas y pederastas [En Línea]. 2008. no. 11870 [Publicado el 14 Noviembre 2008] Disponible en: http://www.abc.es/20081114/nacional-tribunales/verde-codigo-penal-consensuado-20081114.html

INGLATERRA. U.K. PARLIAMENT. Act of the U.K. Parliament; Sexual Offences Act, section 15. 2003.

INGLATERRA. U.K. PARLIAMENT. Act of the Scottish Parliament; Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005, 2005 asp 9.

INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES. Annual Report 2011 [En Línea], 2011, Amsterdam [Publicado el Diciembre 2011]. Sayin no to illegal content on the internet. Disponible en Internet: <http://inhope.org/Libraries/Annual_reports/INHOPE_2011_Annual_Report.sflb.ashx>

ORGANIZACIÓN DE NACIONES UNIDAS – ONU. El Sistema de Tratados de Derechos Humanos de las Naciones Unidas. Introducción a los tratados fundamentales de derechos humanos y a los órganos creados en virtud de tratados. 30 Ed. Ginebra: Editorial Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. 2004. 90 p.

COLOMBIA. CONGESO DE LA REPUBLICA. Constitución Política de Colombia. El pueblo de Colombia en ejercicio de su poder soberano, representado por sus delegatarios a la Asamblea Nacional Constituyente, invocando la protección de Dios, y con el fin de fortalecer la unidad de la Nación y asegurar a sus integrantes la vida, la convivencia, el trabajo, la justicia, la igualdad, el conocimiento, la libertad y la paz, dentro de un marco jurídico, democrático y participativo que garantice un orden político, económico y social justo, y comprometido a impulsar la integración de la comunidad latinoamericana decreta, sanciona y promulga la siguiente Constitución Política De Colombia. Bogotá D.C., 1991. p. 7-8.

COLOMBIA. CONGESO DE LA REPUBLICA. Ley 679. (3, agosto, 2001). Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. Bogotá D.C., 2001. p. 2, 4, 14-15.

COLOMBIA. CONGESO DE LA REPUBLICA. Decreto 1524. (24, julio, 2002) Por el cual se reglamenta el artículo 5 de la Ley 679 de 2001 Bogotá D.C., 2002. p. 2-4.

COLOMBIA. CONGESO DE LA REPUBLICA. Ley 1336 (21, julio, 2009) Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Bogotá D.C., 2009. p. 3, 11.

COLOMBIA. CONGESO DE LA REPUBLICA. Ley 599 (24, julio, 2000) Por la cual se expide el Código Penal. Diario Oficial. Bogotá D.C., 2000. No. 44097 p. 69.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACION. Referencias Bibliográficas: Contenido, forma y estructura. NTC 5613. Bogotá, D.C.: El Instituto, 2008. 39 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACION. Referencias Documentales para Fuentes de Información Electrónica. NTC 4490. Bogotá, D.C.: El Instituto, 1998. 27 p.

HERNÁNDEZ LERMA, Onésimo. Elementos de probabilidad y estadística, México, Fondo de cultura Económica, 1979, 355 p.

SEGUKIDS. Juntos en la Red. Control Parental [En línea], 2012. Disponible en Internet: <http://www.segu-kids.org/padres/control-parental.html>

SEGUKIDS. Juntos en la Red. Control Parental [En línea], 2012. Disponible en Internet: <http://www.segu-kids.org/padres/control-parental-aplicaciones.html>

AUSTIN, Sam n. Cómo bloquear el acceso a sitios web con DD-WRT [En línea], [Publicado el 15 Junio 2012]. Disponible en Internet: http://www.ehowenespanol.com/bloquear-acceso-sitios-web-ddwrt-como_43837/

WIKIPEDIA. La enciclopedia libre [En Línea]. 2012, actualizado el 29 Diciembre 2012 [Publicado en 13 Agosto 2009]. DD-WRT. Disponible en Internet: <http://es.wikipedia.org/wiki/DD-WRT>