POLITICA DE INTERNET SANO TELEMATICA SAS

TELEMÁTICA SAS, En virtud de la legislación vigente da cumplimiento con la Ley 679 del 03 de Agosto de 2001, expedida por el congreso de la república, colaboramos en prevenir, bloquear, combatir y denunciar la explotación, alojamiento, uso, publicación, difusión de imágenes, textos, documentos, archivos audiovisuales, o cualquier material pornográfico relacionado con actividades sexuales de menores de edad o que pueda inducir a la misma.
Esta ley 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 política de Colombia.

También pretende dictar medidas preventivas y sanciones para quienes exploten y/o abusen sexualmente de los menores de edad, para así ayudar a que tengan un desarrollo integral y sano.

¿DONDE DENUNCIAR LA PORNOGRAFÍA INFANTIL?

Para formular denuncias contra contenidos de pornografía infantil o páginas electrónicas en las que se ofrezcan servicios sexuales con menores de edad, existen varias entidades:

- ✓ **MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (MINTIC)**

Teléfono: 01 8000 912667
Página Web Dignidad Infantil del Ministerio de Comunicaciones:
http://archivo.mintic.gov.co/mincom/faces

- ✓ **FISCALÍA GENERAL DE LA NACIÓN**

Teléfono: 01 8000 912280
www.fiscalia.gov.co
e-mail: contacto@fiscalia.gov.co

- ✓ **DIRECCIÓN CENTRAL DE POLICÍA JUDICIAL - DIJIN**

Grupo Investigativo Delitos Informáticos
Carrera 77A # 45-61 Barrio Modelia
Teléfonos: PBX: 426 6900 Ext. 6301-6302
Directo: (1) 4266300

- ✓ **INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR**

Teléfonos: 01 8000 918080 ó (1)6605520, (1)6605530, (1)6605540
Horario: 7am a 9pm de lunes a domingo
www.icbf.gov.co

También se puede Denunciar a través de estos link:

http://www.enticconfio.gov.co/

http://www.teprotejo.org/index.php/es/

DIANA CAROLINA MANAJRRES BOHADA
GERENTE

CONTROL DE CAMBIOS

Fecha Revisado	Modificación	VER.	Responsable revisión	Responsable aprobación
May 2017	Versión inicial del documento	00	Coordinador HSEQ	Gerente
Sep 2018	Revisión y actualización de documentación	00	Coordinador HSEQ	Gerente
Sep 2020	Revisión y actualización de documentación	00	Coordinador HSEQ	Gerente
Sep 2022	Revisión y actualización de documentación	00	Coordinador HSEQ	Gerente
Mar 2023	Se realiza actualización del documento por cambio de tipo de sociedad y logo	01	Coordinador HSEQ	Gerente Administrativo

¿QUÉ ES INTERNET SANO?

Es la campaña del Ministerio de Comunicaciones para que todos los colombianos comprendamos el significado de la prevención de la pornografía infantil y juvenil en Internet.

NORMATIVIDAD VIGENTE

Ley 679 del 03 de Agosto de 2001

Notas de Vigencia

- Modificada por la **Ley 1336 de 2009**, publicada en el Diario Oficial No. 47.417 de 21 de julio de 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'

- Modificado por la **Ley 1101 de 2006**, publicada en el Diario Oficial No. 46.461 de 23 de noviembre de 2006, 'Por la cual se modifica la Ley 300 de 1996 Ley General de Turismo y se dictan otras disposiciones'

- Modificada por el **Decreto 1524 de 2002,** Publicado en el diario oficial 44.883 del 30 de julio de 2002 ´Por medio del cual se reglamenta el artículo 5° de la Ley 679 de 2001´

LA DELGADA LINEA DE LA PORNOGRAFIA INFANTIL

Aunque es cotidiano compartir todo tipo de contenidos en redes sociales y sitios web, este hábito traspasa los parámetros de ocio o diversión al límite del peligro, a tal punto de revelar información sensible como direcciones, sitios de trabajo, datos familiares.
Esta práctica, que puede generarse por el orgullo que los padres sienten por sus hijos, expone a los niños a extorsiones y a consumidores de pornografía infantil, sin ser conscientes de ello.
En primer lugar, piense que las fotos públicas son 100% susceptibles de copiar, manipular y editar. Con programas de dominio público, especializados en manejo de imágenes y bajo la técnica morphing, pueden realizarse montajes perfectos, para crear la ilusión de transformación, herramienta práctica para convertir una imagen de un niño usando vestido de baño en fotos pornográficas.

Ahora bien, si usted se empeña en realizar esta práctica, tenga en cuenta las siguientes sugerencias de Adalid:

- Piense que si quiere compartir las fotos con alguien en especial, el correo electrónico o las aplicaciones de mensajería instantánea son una forma privada de hacerlo. Snapchat o WickrMe proporcionan mayor seguridad de hacerlo pues borran la imagen que se envió en el dispositivo destinatario.

- Configure la privacidad de sus redes sociales, use los filtros de restricción para que no todos sus contactos puedan acceder a las fotografías. Aun siendo un perfil privado, sea muy cuidadoso y autorice el acceso a su información solamente a personas de plena confianza, no a todos sus agregados o “amigos”.

- Lea la letra chica e infórmese acerca de las normas, las condiciones de uso y las autorizaciones automáticas que usted cede al usar dicha red y al subir todo tipo de contenido.

- No etiquete las fotos de los niños con sus nombres propios. Estas pueden ser indexadas automáticamente por los buscadores.

- No publique fotos en sitios que revelen la ubicación del niño. Nunca lo haga frente a su casa, frente al colegio, o a un sitio reconocido que visite frecuentemente.

- Cuídese de tomar fotos de los menores frente a su automóvil familiar en donde se vea la placa del vehículo. Esta es una forma rápida de ubicar a los niños.

- Al tomar fotos asegúrese que la funcionalidad GPS de su dispositivo móvil esté desactivada. Estos datos siempre van integrados de manera invisible a las imágenes y es muy simple ubicar el lugar.

- En paseos, fiestas o reuniones esté atento de quién le toma fotos a sus hijos o sobrinos y exíjale a sus familiares que pidan autorización para publicar estas imágenes.

- Siempre informe a su pareja cuando publique fotos de los menores, es mejor que los dos estén al tanto.

- Finalmente, recuerde que al subir fotos a entornos digitales, éstas se convierten en material de dominio público y la única forma para eliminarlas es recurrir a expertos. Eso sí, el proceso puede ser muy demorado y tedioso.

SEGURIDAD DE LA INFORMACION

Debido a que el uso de Internet se encuentra en aumento, cada vez más compañías permiten a sus empleados, socios y proveedores acceder a sus sistemas de información. Por lo tanto, es fundamental saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema.
Internet y sus elementos asociados son mecanismos ágiles que proveen una alta gama de posibilidades de comunicación, interacción y entretenimiento, tales como elementos de multimedia, foros, chat, correo, comunidades, bibliotecas virtuales entre otros que pueden ser accedidos por todo tipo de público. Sin embargo estos elementos deben contener mecanismos que protejan y reduzcan los riesgos de seguridad alojados, distribuidos y potencializados a través del mismo servicio de Internet.

Telemática SAS. como proveedor del servicio de conectividad está convencida de que las relaciones con nuestros clientes se deben fortalecer desde una comunicación asertiva, sana y orientada a proporcionar las herramientas y concejos prácticos necesarios para la protección adecuada de los elementos de cómputo y los servicios asociados a la Internet. Por esta razón ponemos a disposición de todos nuestros clientes y de la comunidad en general, conceptos teórico - prácticos que pueden evitar o reducir los riesgos a que se está expuesto cuando se interactúa con la Internet y sus elementos asociados.

SEGURIDAD INFORMATICA

Son aquellas **reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño**, ya sea de manera personal, grupal o empresarial.

CARACTERISTICAS DE LA SEGURIDAD INFORMATICA

Integridad: Granizar que los datos sean los que se supone que son, La verificación de la integridad de los datos consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente).

Confidencialidad: Asegurar que sólo los individuos autorizados tengan acceso a los recursos, la cual consiste en hacer que la información sea ininteligible para aquellos individuos que no estén involucrados o autorizados.

Disponibilidad: Garantizar el correcto funcionamiento de los sistemas de información para el acceso a un servicio o a los recursos.

Irrefutabilidad: **(No-Rechazo o No Repudio) Que no se pueda negar la autoría de quien provee de dicha información.**

Autenticación: Garantizar que sólo los individuos autorizados tengan acceso a los recursos o información.

ALGUNOS TERMINOS DE SEGURIDAD

Seguridad de la Información: Son aquellas acciones que están encaminadas al establecimiento de directrices que permitan alcanzar la confidencialidad, integridad y disponibilidad de la información, así como la continuidad de las operaciones ante un evento que las interrumpa.

Activo: Recursos con los que cuenta la empresa y que tiene valor, pueden ser tangibles (servidores, desktop, equipos de comunicación) o intangibles (Información, políticas, normas, procedimientos).

Vulnerabilidad: Exposición a un riesgo, fallo o hueco de seguridad detectado en algún programa o sistema informático.

Amenaza: Cualquier situación o evento posible con potencial de daño, que pueda presentarse en un sistema.

Riesgo: Es un hecho potencial, que en el evento de ocurrir puede impactar negativamente la seguridad, los costos, la programación o el alcance de un proceso de negocio o de un proyecto.

Gestión de seguridad: Proceso de establecer y mantener la seguridad en un sistema o red de sistemas informáticos.

Parche: En seguridad informática, código que corrige un fallo (agujero) de seguridad.

Advertencia: Mensaje que comunica al usuario que una acción puede ocasionar u ocasionara la perdida de datos del sistema del usuario.

ELEMENTOS DE PROTECCION

Firewall: Elemento de protección que sirve para filtrar paquetes (entrada o salida) de un sistema conectado a una red, que puede ser Internet o una Intranet. Existen

firewall de software o hardware. Este filtrado se hace a través de reglas, donde es posible bloquear direcciones (URL), puertos, protocolos, entre otros.

Anti-virus: Programa capaz de detectar, controlar y eliminar virus informáticos y algunos códigos maliciosos (Troyanos, Works, Rootkits, Adware, Backdoor, entre otros).

Anti-Spam: Aplicación o herramienta informática que se encarga de detectar y eliminar el spam y los correos no deseados.

Criptografía: Es el arte de cifrar y descifrar información con claves secretas, donde los mensajes o archivos sólo puedan ser leídos por las personas a quienes van dirigidos.

AMENAZAS DE SEGURIDAD

Spam: Envío de cualquier correo electrónico, masivo o no, a personas a través de este medio que incluyen temas tales como pornografía, bromas, publicidad, venta de productos, entre otros, los cuales no han sido solicitados por el(los) destinatario(s).

Ingeniería social: Es la manipulación de las personas para convencerlas de que ejecuten acciones, actos o divulguen información que normalmente no realizan, entregando al atacante la información necesaria para superar las barreras de seguridad.

Código Malicioso: Hardware, software o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Ejemplo: Troyanos, Works, Spyware, etc.

Hoax: Es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena, aparte de ser molesto, congestiona las redes y los servidores de correo, pueden ser intencionales para la obtención de direcciones de correo para posteriormente ser utilizadas como spam.

Suplantación: Hacerse pasar por algo o alguien, técnicamente el atacante se hace pasar por un servicio o correo original.

TIPOS DE FRAUDES

1. Phishing

Viene a significar "pescar, pescando incautos". Es una técnica que se basa en intentar engañar al usuario (ingeniería social), normalmente mediante un correo electrónico, diciéndole que pulse en un determinado enlace, para validar sus claves por tal motivo o tal otro.
El cuerpo del mensaje es lo de menos, lo importante es que la víctima haga click en el enlace, para así llevarle a una página web que él se cree que es la página

original (ya sea de su banco, de su red social,....), de esta forma los delincuentes logran nuestras claves personales.
Se tienen dos variantes de esta amenaza:

- **Vishing:** Utilización de técnicas de phishing pero para servicios asociados con voz sobre IP (VoIP).
- **Smishing:** Utilización de técnicas de phishing en los mensajes de texto de teléfonos móviles.

¿Cómo funciona?
A través de Sitio Web, Ejemplo:
- Sitio oficial: www.sitioReal.com
- Sitios falsos: www.sitioReal.com.sitio.com

Adicional a esto, fijan una imagen simulando ser un sitio seguro (con certificados digitales) que a simple vista, da mucha confianza pero son FALSOS.

¿Cómo llegan a las personas?

- ***Utilizando mecanismos masivos de comunicación como el spam:*** Mediante engaños Invocando la posibilidad de dar obsequios o premios si hacen esta acción.
- ***A través de Correo electrónico:*** Con el envío de Correos masivos solicitando datos personales o informando fallas técnicas que requieren de restablecer contraseñas.

¿A quién le puede pasar?

A cualquier usuario que tenga un correo electrónico y acceso a Internet que haga consultas y/o actualizaciones en portales que le presten servicios.

¿Dónde está el peligro y cómo podemos ser víctimas?

Al ser una página falsa, inducen a los usuarios a que ingresen los datos personales, como cuantas de correo, número de tarjetas de crédito, claves, etc.

¿Cuáles son las consecuencias?

Estafas, suplantaciones o robos de dinero, dado que éste atacante posee las claves de acceso a los sistemas y servicios.

¿Cómo se puede evitar?

- Siempre que llegue este tipo de mensajes, ingrese directamente al sitio oficial desde el browser o navegador, nunca desde el enlace l link enunciado en el correo, ni dando clic a dicho enlace.

- Evite el envío de mensajes cadena, pornografía, mensajes no solicitados, bromas a otros remitentes de correo.
- Cuando ingrese al sitio, valide que la seguridad que se indica a través de certificados digitales, si están respaldados, de doble clic el icono de seguridad, que debe estar ubicado en la parte inferior derecha del navegador (no dentro de la página).

Una modalidad más peligrosa de **Phishing** es el **Pharming,** el cual consiste en infectar un ordenador y editar el archivo hosts local, de forma que en dicho archivo asocian la dirección de las entidades bancarias con la IP del servidor de los ciberdelincientes, de forma que aunque pongamos a mano la dirección del sitio web al que queremos ir, el navegador no llevará a la IP del servidor de los estafadores.

2. Ingeniería Social:

La ingeniería social busca aprovecharse de la ingenuidad de la gente, realmente son los mismos timos que antes pero llevados a cabo en la red como es el caso de la estafa nigeriana, en este caso la víctima recibiría un correo de este tipo:

"*Soy una persona muy rica que reside en Nigeria y necesito trasladar una suma importante al extranjero con discreción. ¿Sería posible utilizar su cuenta bancaria?"* (Fuente: Wikipedia)

A cambio de acceder se supone que el usuario recibiría un 10 o el 20 por ciento de una suma que suele rondar alrededor de decenas de millones de euros.

3. Gusanos:

Son programas **"Malware"** que suelen acompañar a un correo electrónico como archivo adjunto o un enlace (aunque no siempre).

Entre otras cosas **se hacen con la libreta de direcciones de correo** de la víctima (las que tenemos en Outlook, MNS Messenger,....) y automáticamente mandan un mensaje de correo a todas estas direcciones **con el fin de infectar también a más equipos**. Por lo tanto es fácil picar ya que el correo que nos llega es de un conocido, con un asunto que puede decir "mira esto." o aprovechar acontecimientos de la actualidad.

Por lo tanto, uno de los mayores peligros de este tipo de Malware es que su **velocidad de propagación es enorme**, cuando se quiere lanzar la alerta de que ha aparecido un nuevo gusano y se incluye en las bases de datos de los antivirus ya puede ser demasiado tarde.

También puede conectarse a algún servidor de Internet y descargar cualquier otro tipo de software mal intencionado, por ejemplo, un virus o troyano. De esta forma, estaríamos uniendo la gran capacidad de reproducirse y propagarse de los gusanos con la enorme peligrosidad y poder de devastación de otros virus y troyanos.

4. Troyanos:

Son programas que toman el control de la máquina pero sin alterar su funcionamiento, es decir, intentan pasar desapercibidos con el fin de:

- **Robar información,** por ejemplo, cuando nos conectamos al banco pueden detectar las pulsaciones del teclado (keyloaders) de forma que obtienen nuestras credenciales, con lo que pueden realizar transferencias bancarias, estas transferencias se realizan a la cuenta de una persona que a su vez y a cambio de una comisión realiza otra trasferencia del dinero hasta el destinatario final (a través de medios de pago electrónico o Western Union) cuyo objetivo es que no se conozca quien el destinatario final.

- **Controlar los equipos con el fin de realizar otros delitos**, es decir, a través de su servidor los ciberdelincuentes controlan una serie de equipos a través de los cuales pueden enviar correo spam, difundir virus, realizar ataques masivos a servidores al conectarse todos a la vez a un mismo sitio Web,....., de esta forma mantienen su servidor en el anonimato. En este caso se habla de ordenadores Zombies los cuales forman "un ejército" al servicio de los ciberdelincuentes, a la red formada por estos ordenadores zombies se les denomina Botnet. Por lo tanto, si nuestro equipo contiene este tipo de malware podemos estar realizando delitos informáticos con repercusiones legales sin ser conscientes de ello.

5. Spyware:

El Spyware es un software que una vez introducido en el ordenador realiza un seguimiento de la información personal del usuario y la pasa a terceras entidades, generalmente con fines publicitarios. De hecho, el Spyware se suele ir acompañado de otro tipo de programas llamados "Adware" (software de anuncios) que se refiere a una categoría de software que, cuando está instalada en su computadora, puede enviarle pop-up's (ventanas emergentes) o anuncios para re-dirigir su Navegador a cierta página Web.

¿Qué efectos provocan en el ordenador?

- Al conectarse a Internet o abrir el navegador **se abren continuamente ventanas emergentes** ('pop-ups').
- **Insertar publicidad en páginas** en las que en principio no deberían tener dicha publicidad.
- Cambia la página de inicio y aparecen **nuevas barras de herramientas en el navegador**.
- La conexión a Internet, e incluso el **funcionamiento** general de la computadora, **se ralentiza** (el spyware utiliza memoria y ancho de banda).
- Hacen lo que se denomina **"Secuestro del Navegador"** que consiste en cambiar la página de inicio, no nos dejan acceder a páginas de seguridad, nos redireccionan a sus Webs.

TIPS DE SEGURIDAD

1. Pornografía Infantil

- Evite Alojar, publicar o trasmitir información, mensajes, gráficos, dibujos, archivos de sonido, imágenes, fotografías, grabaciones o software que en forma indirecta o directa se encuentren actividades sexuales con menores de edad, en los términos de la legislación internacional o nacional, tales como la Ley 679 de 2001 y el Decreto 1524 de 2002 o aquella que la aclare, modifique o adicione o todas las leyes que lo prohíban.

2. Control de virus y códigos maliciosos:

- Mantenga siempre un **antivirus actualizado** en su equipo(s), procure correr éste periódicamente, de la misma manera, tenga en su equipo elementos como anti-spyware y bloqueadores de pop-up (ventanas emergentes).
- Evite visitar **páginas no confiables** o instalar software de dudosa procedencia.
- Asegúrese que se aplican las **actualizaciones** en sistemas operativos y navegadores Web de manera regular.
- Si así lo requiere, obtenga y configure el **firewall personal**, esto reducirá el riesgo de exposición.
- Instalar un software **antiespia**.
- Tener activado un **cortafuego** que bloquee accesos no autorizados de aplicaciones a Internet, o viceversa.
- Mantener el **sistema operativo actualizado**, para ello debemos activar las actualizaciones automáticas del sistema, estas actualizaciones reparan vulnerabilidades del sistema que van siendo detectadas, y los ciberdelincuentes utilizan dichas vulnerabilidades para colarse en el ordenador.

3. Correo electrónico:

- No publique su cuenta de correo en sitios no confiables.
- No preste su cuenta de correo ya que cualquier acción será su responsabilidad.
- No divulgue información confidencial o personal a través del correo.
- Si un usuario recibe un correo con una advertencia sobre su cuenta bancaria, no debe contestarlo
- Nunca responda a un correo HTML con formularios embebidos.
- Si ingresa la clave en un sitio no confiable, procure cambiarla en forma inmediata para su seguridad y en cumplimiento del deber de diligencia que le asiste como titular de la misma.

4. Control de Spam y Hoax

- Nunca hacer click en enlaces dentro del correo electrónico aun si parecen legítimos. Digite directamente la URL del sitio en una nueva ventana del browser
- Para los sitios que indican ser seguros, revise su certificado SSL.

- No reenvié los correos cadenas, esto evita congestiones en las redes y el correo, además el robo de información contenidos en los encabezados.

5. Control de la Ingeniería social

- No divulgue información confidencial suya o de las personas que lo rodean.
- No hable con personas extrañas de asuntos laborales o personales que puedan comprometer información.
- Utilice los canales de comunicación adecuados para divulgar la información.

6. Control de phishing y sus modalidades

- Si un usuario recibe un correo, llamada o mensaje de texto con una advertencia sobre su cuenta bancaria, no debe contestarlo.
- Para los sitios que indican ser seguros, revise su certificado SSL.
- Valide con la entidad con quien posee un servicio, si el mensaje recibido por correo es válido.

7. Robo de contraseñas

- Cambie sus contraseñas frecuentemente, mínimo cada 30 días.
- Use contraseñas fuertes: Fácil de recordar y difícil de adivinar.
- Evite fijar contraseñas muy pequeñas, se recomienda que sea mínimo de una longitud de 10 caracteres, combinada con números y caracteres especiales.
- No envié información de claves a través del correo u otro medio que no esté encriptado.

MECANISMOS DE SEGURIDAD

TELÁMATICA LTDA, cuenta con sistemas de autenticación y autorización para controlar el acceso a los diferentes servicios de la red, al igual que controles de autenticación para los usuarios (equipos terminales de acceso del cliente). También cuenta con diferentes protecciones para controlar el acceso a los servicios de Internet

tales como los mecanismos de identificación y autorización respecto a los servicios. Para proteger las plataformas de los servicios de Internet.

Por otra parte, se han implementado configuraciones de seguridad base en los diferentes equipos de red, lo que comúnmente se llama líneas base de seguridad, además del establecimiento de medidas de seguridad a través de elementos de control y protección como:

Antivirus: Tanto las estaciones de trabajo como los servidores de procesamiento interno de información son protegidos a través de sistemas anti-códigos maliciosos.

Antispam: Todos los servidores de correo poseen antispam que reduce el nivel de correo basura o no solicitado hacia los clientes, descongestionando los buzones y el tráfico en la red.

Firewall: A través de éste elemento de red se hace la primera protección perimetral en las redes Telematica SAS y sus clientes, creando el primer control que reduce el nivel de impacto ante los riesgos de seguridad.

Filtrado de URLs: Los clientes pueden realizar filtrado de URL a través de sus navegadores Web, se sugiere instalar además sistemas parentales.

TELEMÁTICA SAS, cuenta con varios mecanismos capaces de realizar el bloqueo de URLs, entre ellos se encuentran los sistemas DNS y una herramienta para todo el tráfico hacia Internet, el objetivo principal de bloquear las que contengan o promuevan la pornografía infantil en Internet a través imágenes, textos, documentos y/o archivos audiovisuales.

Seguridad a nivel del CPE: Los dispositivos de conexión final ubicados en las premisas de los clientes cuentan con elementos bases para la autenticación y autorización, con ello permiten hacer una conexión a Internet de manera más segura.

LIMITACIONES DE ACCESO

Si bien **Telemática SAS,** cuenta con mecanismos de seguridad, filtrado y se hace un control de navegación acorde a los estipulado en la **Ley 679 de 2001** y sus decretos reglamentarios, en ningún caso bloquea o hace uso de software o programas que eviten la libre navegación y acceso a Internet (salvo lo estipulado en la ley), por consiguiente, **Telemática SAS** no tiene limitaciones en el acceso hacia Internet para sus clientes y usuarios, dando cumplimiento a lo estipulado por el Ministerio de las TIC.

FUENTES

http://www.mintic.gov.co/portal/604/articles-3685_documento.pdf
http://www.alegsa.com.ar/Dic/antispam.php
http://roble.pntic.mec.es/jprp0006/uso_responsable_tic/33_fraudes_por_internet.html
http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5551
http://wwwmantovaniseguridadinformatica.blogspot.com.co/2009/06/la-seguridad-informatica-consiste-en.html

http://www.bitcuantico.com/2011/01/26/seguridad-informatica-conceptos-y-caracteristicas/
http://www.enticconfio.gov.co/delgada-linea-pornografia-infantil