HIZ TELECOMUNICACIONES S.A.S.

POLITICA ANTIFRAUDE

HIZ TELECOMUNICACIONES S.A.S. promueve una cultura de no tolerancia al fraude.

OBLIGACIONES DEL USUARIO

I. Abstenerse de utilizar, permitir, propiciar, facilitar o patrocinar la comercialización de los servicios de telecomunicaciones ofrecidos por HIZ para obtener beneficio o lucro económico para sí o para terceras personas naturales o jurídicas sin autorización expresa y escrita de Colombia Telecomunicaciones.

II. Abstenerse de presentar documentación falsa respecto a su identidad como persona natural (cédula de ciudadanía) o jurídica e información tendiente a distorsionar la realidad (referencias, direcciones inexistentes, documentos presentados como prueba para algún trámite, entre otra).

III. Está expresamente prohibido que el cliente aloje contenidos de pornografía infantil, utilice o permita utilizar el servicio con fines de explotación, pornografía, turismo sexual y demás formas de abuso sexual contra menores de edad.

IV. El cliente contratante del servicio tiene como obligación realizar un uso adecuado del mismo de acuerdo a lo estipulado en este contrato y a lo expresado por las autoridades competentes como el Ministerio de Comunicaciones, la Comisión de Regulación de Comunicaciones, la Superintendencia de Industria y Comercio, y cualquier otra entidad de vigilancia y control que tenga incidencia en el uso del servicio.

V. En el caso de que el HIZ requiera realizar sin previo aviso visita para hacer la verificación de un presunto fraude detectado, el cliente deberá facilitar la inspección en sus instalaciones o en cualquier parte de la red y permitir la entrada a éstas a una persona plenamente identificada y autorizada para hacer las corroboraciones a que haya lugar. Para lo cual debe levantarse un informe en el que se deje constancia de lo sucedido en la visita.

El incumplimiento de alguno de los puntos anteriores faculta a HIZ TELECOMUNICACIONES SAS para terminar de manera inmediata y unilateral cualquier tipo de relación que tenga con el Usuario, sin perjuicio de las demás sanciones a que haya lugar.

HIZ TELECOMUNICACIONES .S.A.S.
Cl. Portobelo No. 37-26 Arjona, Bolívar
Línea gratuita nacional 018000911449
Email servicioalcliente@hiztel.co
Móvil 318 4043 274

HIZ TELECOMUNICACIONES S.A.S.

Reporte de manera inmediata irregularidades o actos sospechosos de personas con y/o sin identificación de la empresa que estén maniobrando las cajas, cables que estén en los postes; del mismo modo los casos de sustracción de trozos de cable o infraestructura, siniestros o daños en la infraestructura de telecomunicaciones; cajas abiertas sin ninguna seguridad o que atenten contra la seguridad de la comunidad.

El Usuario debe reportarlo a través de cualquiera de los siguientes canales establecidos por HIZ TELECOMUNICACIONES S.A.S.: líneas telefónicas 318 84043274, 6 291794; correo electrónico servicioalcliente@hiztel.co y oficina de servicio al cliente Cll. Portobelo No. 37-26 (Arjona, Bolívar).

HIZ TELECOMUNICACIONES S.A.S.

SEGURIDAD EN LA RED

Nuestro deber es mantener a nuestros clientes informados y aún más en materia de SEGURIDAD (Resolución 3502 de 2011, Artículo 6 Compilada por la Resolucion 5050 de 2016, articulo 2.9.2.3.)

HIZ Telecomunicaciones SAS tiene el deber de brindarles a sus clientes información sobre los riesgos relativos a la seguridad en la red, el Usuario debe tener en cuenta que coexisten riesgos sobre la seguridad de la red y el servicio contratado, entendiendo que la red de Internet es una conexión libre y sin censura.

Como mecanismos de prevención, lo invitamos a tener en cuenta los siguientes puntos:

- Le recomendamos conocer y mantener estrictos cuidados con la seguridad, mantenimiento y programación de estos equipos, asegurando que la configuración de los mismos no sea manipulada por terceros no autorizados. Recuerde que estos equipos son de su propiedad y entera responsabilidad.
- Establezca contraseñas aleatorias y como mínimo utilice 10 caracteres alfanuméricos combinados y con caracteres especiales, cámbielas periódicamente.
- No permita la manipulación de equipos o soporte técnico con personas o empresas diferentes a HIZ.
- Ten cuidado con los SMS que recibes de celulares, llamadas o correo electrónico informándote que ganaste premios o sobre promociones de parte de HIZ TELECOMUNICACIONES SAS, porque pueden ser engaños cometidas por entidades fraudulentas. No entregue información confidencial por ninguno de estos medios.
- Instala sistemas de antivirus y firewalls en tu equipo.
- No descargue información o programas de sitios web desconocidos, sin confirmar su procedencia y/o confiabilidad.
- Navegue seguro en internet, tenga en cuenta los siguientes conceptos:
- Hasta hace unos años, los virus eran considerados la principal amenaza para los equipos informáticos.
- En la actualidad existen otras amenazas derivadas de los virus. Están los gusanos informáticos, que son programas que, a diferencia de los virus, se propagan realizando

copias de si mismos con consecuencias similares y también los troyanos, que una vez se introducen en el sistema, capturan contraseñas, pulsaciones del teclado o permiten el acceso remoto al computador.

- En los últimos años, y debido principalmente al uso cotidiano de computadores y la masificación del acceso a Internet, han aparecido otras amenazas catalogadas bajo el término "malware", que es la forma abreviada para MALicious softWARE, es decir, programas maliciosos. Malware es cualquier programa, documento o mensaje que pueda resultar perjudicial para un computador, tanto por pérdida de datos como por disminución de su productividad. Bajo esta denominación encontramos los siguientes:
  - **Spyware (Software/ programa espía):** programa que monitorea, daña, espia o roba información sobre los hábitos del usuario e información personal al navegar en internet y los remite de forma secreta/sin autorización a otra red informática o hackers.
  - **Hoax**: Mensaje de correo electrónico advirtiendo sobre falsos virus
  - **Spam**: Envío indiscriminado de mensajes de correo no solicitados, con fines publicitarios o buscando saturar una red específica.
  - **Rootkits**: es un kit para hacerse root (administrador) de un equipo. Es un código malicioso realmente complejo que se introduce en una máquina y, a veces, en el núcleo mismo del sistema operativo. De este modo, es capaz de tomar el control total de un PC sin dejar rastros. El incremento de los rootkits se ve favorecido por el hecho de que la mayoría de usuarios de Windows trabajan con derechos de administrador, lo que facilita enormemente la instalación de rootkits en los PC.