CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINSTRACIÓN DE RED

El presente Código de Gestión de Tráfico y Administración de Red (el "Código"), es informar a los suscriptores del servicio de Acceso a Internet de **KBLEX, S.A. DE C.V.** ("**KBLEX**"), de los principios y políticas relevantes con base en los cuales se llevan estas actividades a efecto de asegurar la calidad, capacidad y velocidad del servicio de acceso a Internet contratado, al tiempo de preservar la integridad y seguridad de la red a través de la cual se brinda dicho servicio.

I. Derechos de los usuarios.

De conformidad con lo dispuesto en el artículo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión, nuestros usuarios gozan de los siguientes derechos:

a) Libre elección. Los usuarios de FFT pueden acceder e intercambiar contenido y tráfico de manera abierta por Internet, siempre que los dispositivos y/o aparatos que nuestros usuarios conecten a Internet más allá del punto de conexión terminal de la red se encuentren homologados por el Instituto Federal de Telecomunicaciones y en cumplimiento de la normatividad aplicable.

Los diferentes paquetes del servicio de acceso a Internet de FFT permiten a los usuarios el acceso total al contenido, aplicaciones o servicios disponibles en internet, salvo que algún usuario requiera aplicar ciertas pautas de filtrado, en cuyo caso deberá apegarse a las reglas económicas y operativas vigentes.

FFT no condiciona el acceso al usuario a aplicaciones, servicios o contenidos específicos disponibles en internet, siendo el proveedor de estos el único responsable de los criterios de acceso. El uso aceptable del servicio de internet supone riesgos y responsabilidades para la seguridad y privacidad de los usuarios cuando buscan, acceden y/o descargan, por ejemplo, contenidos, aplicaciones o servicios ilegales, ilícitos, dañinos con malware, virus informáticos, adware, spyware, phishing, etc.

FFT no establece ninguna limitante para el uso de dispositivos o aplicaciones externos al módem, pero el desempeño y/o calidad debe considerar la concurrencia comprometida, entre otros.

b) No discriminación. En la prestación del servicio de acceso a Internet, FFT no inspecciona, filtra o discrimina contenidos, así como tampoco obstruye, interfiere ni bloquea información, contenidos, aplicaciones o servicios.

c) Privacidad. El servicio de acceso a Internet se provee manteniendo la privacidad de los usuarios. En el Aviso de Privacidad de FFT, nuestros usuarios pueden conocer el procedimiento bajo el cual es tratada su información personal, de conformidad con la normatividad aplicable.

d) Seguridad. FFT podrá bloquear el acceso a determinados contenidos, aplicaciones o servicios con el fin de preservar la privacidad de sus usuarios, la seguridad de la red, así como para prevenir la comisión de delitos. Asimismo, FFT podrá bloquear el acceso a contenidos, aplicaciones o servicios ofrecidos en Internet, a petición expresa de sus usuarios, cuando exista orden de autoridad competente o sean contrarios a la normatividad aplicable.

e) Transparencia e información. En la página de internet de FFT, nuestros usuarios encontrarán la información relativa a las características del servicio ofrecido, por ejemplo, su velocidad por

paquete y alcance, con la finalidad de que tomen una decisión informada sobre las diferentes alternativas disponibles en el mercado.

f) Calidad. FFT preservará en beneficio de sus usuarios los índices de calidad establecidos en los Lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores del servicio fijo emitidos por el Instituto Federal de Telecomunicaciones.

II. Políticas de gestión de tráfico y administración de red.

El servicio de acceso a Internet por medio de enlaces inalámbricos tiene características muy particulares, tales como la conexión que se mantiene entre la radio base y el módem, la cual debe ser punto a punto sin algún obstáculo en la línea de vista, la imposibilidad de incrementar la capacidad definida en la radio base utilizada, los riesgos de seguridad latentes, entre otros, por lo cual FFT debe aplicar las políticas de gestión de tráfico y administración de la red que se describen a continuación:

A. Limitación de conexiones Peer-to-Peer con base a la tecnología

Las conexiones Peer to Peer –P2P– tienen una arquitectura destinada a la comunicación entre aplicaciones uno-a-uno, lo que permite a las personas o a los dispositivos compartir información y archivos de uno a otro sin necesidad de intermediarios. Esas conexiones se utilizan primordialmente para intercambiar contenidos o archivos que violan los derechos de propiedad intelectual y derechos de autor, por ejemplo, series, películas, música, videojuegos, además de que son una fuente importante de malware, razón por lo cual son bloqueadas en el Gateway de FFT dependiendo de la tecnología implementada, pues ello permite reducir el riesgo de comprometer la integridad de la información de los usuarios y de terceros, así como los reclamos legales de los tenedores de los referidos derechos.

En caso de tener activa la limitación, los usuarios NO tendrán acceso a conexiones P2P, excepto si el usuario presenta una solicitud de liberación por escrito a FFT con la debida argumentación para que esas conexiones sean habilitadas.

B. Regulación en la resolución de las aplicaciones Streaming

Esta política se aplica a todos los usuarios de FFT para que reciban una resolución adecuada y, por ende, para que la calidad de video sea razonable, sin alcanzar necesariamente la más alta disponible en el servidor origen. Dicha acción tiene como objetivo evitar una excesiva demanda de tráfico que pueda comprometer la disponibilidad de servicio para el resto de los usuarios de la plataforma.

III. Recomendaciones para el usuario.

Algunas de las medidas que pueden adoptar los usuarios para minimizar riesgos en sus conexiones y su privacidad en las comunicaciones son las siguientes:

- No abrir mensajes de correo electrónico de remitentes desconocidos.
- Utilizar herramientas para verificar la autenticidad de los correos electrónicos.
- Brindar tus datos personales solo en sitios de confianza.
- Verificar los enlaces antes de dar clic en ellos.

- Usar un navegador seguro y actualizarlo constantemente.
- Cerrar siempre las sesiones de cuentas personales y redes sociales.
- No aceptar en redes sociales invitaciones de desconocidos.
- Acceder directamente a los sitios de confianza para hacer búsquedas desde ellos.
- Verificar que, al navegar por internet, los sitios sean de confianza: la URL de esos sitios debe comenzar con “https”.
- No descargar archivos de fuentes no fiables.
- Leer y, en su caso, aceptar los acuerdos de licencia para el usuario final.
- Navegar en sitios seguros.
- Aprovechar las opciones de seguridad integradas en los dispositivos móviles.
- Conocer todos los detalles de nuestros dispositivos para prevenir ataques.
- No utilizar software sin licencia.
- Ocultar los datos de navegación haciendo uso de servidores proxy.
- Utiliza contraseñas seguras que no se repitan y que combinen letras, números y hasta símbolos.
- Usar un buen antivirus y protector de phishing.
- Actualizar constantemente las aplicaciones y/o el sistema operativo de tus dispositivos.
- No proporcionar datos sensibles en redes sociales o por correo electrónico.

IV. Referencias al marco legal aplicable y a los estándares internacionales que dan origen a la gestión de tráfico y administración de nuestras redes.

Este código se apega a los protocolos de TCP/IP estandarizados por la organización internacional IETF −Internet Engineering Task Force−, así como a lo dispuesto en la Ley Federal de Telecomunicaciones y Radiodifusión y en los Lineamientos para la gestión de tráfico y administración de red a que deberán sujetarse los concesionarios y autorizados que presten el servicio de acceso a Internet, emitidos por el Instituto Federal de Telecomunicaciones.