POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE RED

En atención a 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 Instituto Federal de Telecomunicaciones, CMC asegurará la calidad, capacidad y velocidad del servicio de acceso a Internet contratado por los usuarios mediante sistemas de administración, monitoreo y gestión, garantizando una ampliación de capacidad cuándo alcance una saturación de un 75% durante más de 4 horas continuas en tres días consecutivos. De esta manera preservaremos la calidad, capacidad y velocidad del servicio de acceso a Internet contratado por los usuarios finales de la red.

Las políticas de gestión de tráfico y administración que tiene implementada la red CMC, asegura la libre elección de los usuarios finales para acceder a los contenidos, aplicaciones y servicios en Internet, sin que CMC dificulte, limite, degrade, restrinjan o discrimine el acceso a los mismos, .

CMC garantiza un trato no discriminatorio a los usuarios finales, PACS, tipos de tráfico similares, así como al tráfico propio y el de terceros que curse por la red, asegurando la privacidad de los usuarios y la inviolabilidad de las comunicaciones privadas entre los mismos.

CMC por políticas de gestión de tráfico y administración de red, bajo ningún supuesto, inspeccionará, monitoreará o alterará el contenido específico del tráfico que curse por su red.

CMC no implementa políticas de gestión de tráfico y administración de red que resulten en la limitación, degradación, restricción, discriminación, obstrucción, interferencia, filtrado o bloqueo del acceso a contenidos, aplicaciones o servicios a los usuarios finales, salvo en aquellos casos emergentes que se realicen de manera temporal y que se presente alguna de las siguientes situaciones:

I. Riesgo, técnicamente comprobable, a la integridad y seguridad de la red, a la privacidad de los usuarios finales o a la inviolabilidad de sus comunicaciones privadas;

II. Congestión excepcional y temporal de la red, sujeto a que no exista discriminación entre tipos de tráfico similares, y

III. Situaciones de emergencia y desastres que pongan en riesgo la operación de la red.

IV.- Por orden de autoridad competente.

CMC respetará el derecho de los usuarios finales a incorporar o utilizar cualquier clase de instrumentos, dispositivos, aparatos o equipos terminales que se conecten más allá del punto de conexión terminal instalado, siempre y cuando estos se encuentren homologados, y en cumplimiento de la normatividad aplicable.

Adicionalmente, CMC no limitará cualesquiera de las funcionalidades o sistemas de operación de los referidos instrumentos, dispositivos, aparatos o equipos terminales.

CMC garantiza la libre elección de los usuarios finales para acceder a los contenidos, aplicaciones y servicios disponibles en Internet. CMC en ningún caso limita, degrada, restringe o discrimina el acceso a los mismos de forma arbitraria, así como de asignar características y recursos de red específicos a un contenido, aplicación o servicio en particular.

CMC hace a los usuarios finales las siguientes recomendaciones, para cuidar la privacidad de sus comunicaciones, así como la privacidad de sus datos.

1. Utilizar siempre los equipos homologados que le han sido recomendados.
2. Verificar que los mismos contengan las últimas actualizaciones de software, recordemos que cada momento surgen nuevas versiones que tienen como finalidad, protección de privacidad y mejoras en el desempeño de sus equipos y aplicaciones.
3. Construir contraseñas seguras y darles una actualización por lo menos cada 3 meses.
4. No abrir link de sitios que usted no requirió, la seguridad de sus equipos depende de ello.
5. Tener y mantener un sistema antivirus actualizado.
6. Evitar abrir correos sospechosos o de procedencia dudosa, de hecho, si se pretenden abrir estos, pasarlos antes de su apertura por un escaneo del sistema antivirus.
7. Cuidar no aceptar invitaciones de personas desconocidas, actualmente se ha convertido en el principal método de hackeo en las redes sociales.