CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN

DE RED PARA EL SERVICIO DE ACCESO A INTERNET.

El presente Código tiene como finalidad informar a los usuarios del servicio de Acceso a Internet provisto por C. Emmanuel Trejo Colindres Titular de una Autorización para la Operación y Explotación de una Autorización para la comercialización de servicios de Telecomunicaciones***, (en lo sucesivo, "CAPA 3 INTERNET"),***), así como sobre los principios de Neutralidad de Red establecidos el Articulo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión y se emite con base a lo establecido en el Artículo 12 de 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 (en lo subsecuente, "Lineamientos") emitidos por el Instituto Federal de Telecomunicaciones (en lo subsecuente , "IFT"), conforme a lo siguiente:

*CAPA 3 INTERNET**,*** manifiesta que, al implementar las políticas de gestión de tráfico y administración de red, puede situarse en casos fortuitos o de fuerza mayor que requieran de manera excepcional que se limite, degrade, restrinja, discrimine, obstruya, interfiera, filtre o bloqueé el acceso a los contenidos, aplicaciones o servicios, para asegurar con ello el funcionamiento, seguridad e integridad del tráfico de datos, así como la prestación del servicio de acceso a Internet a los usuarios. Al respecto, se considera razonable y justificado que políticas que resulten en tales afectaciones puedan ser implementadas únicamente de manera temporal en las siguientes situaciones:

a) Cuando exista un riesgo a la integridad y seguridad en el tráfico de datos o a las comunicaciones privadas de los usuarios. Por ejemplo, ante ataques o situaciones técnicamente comprobables que impliquen la interrupción de la capacidad de comunicación del servicio de acceso a Internet o pretendan obtener información de la comunicación de los usuarios.

b) Cuando exista congestión excepcional y temporal, entendida como aquella de corta duración y que implica un incremento repentino en el número de usuarios o en el tráfico que transita. Es relevante señalar que las congestiones temporales son distintas a aquellas que pueden presentarse en determinadas franjas horarias y de manera recurrente, las cuales pueden requerir de otros mecanismos de gestión e, incluso, ser un indicador de la necesidad de ampliar la capacidad del PSI para cumplir con la calidad contratada por los usuarios.

C) Cuando se presenten situaciones de emergencia y desastre, entendidas en términos de lo señalado en la Ley General de Protección Civil, que resulten en afectaciones al servicio provisto por ***CAPA 3 INTERNET*****.**

Lo anterior, como ya se ha explicado, sin perjuicio de las obligaciones que deban cumplir los PSI respecto a otras disposiciones. El usuario final podrá recibir asesoría y atención mediante el número telefónico **419 120 8519** asimismo podrá enviar sus preguntas al correo electrónico **soportecapa3@gmail.com,** Por otra parte, el domicilio de atención a clientes se ubica en **Calle Ocampo #12 Col. Centro Doctor Mora Guanajuato.**

1.- DERECHOS DE LOS USUARIOS FINALES DEL SERVICIO DE ACCESO A INTERNET.

El servicio de acceso de internet se sujetará a los siguientes principios señalados en el artículo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión:

I. Libre elección. Los usuarios de los servicios de internet prestados por el proveedor pueden acceder a cualquier contenido, aplicación o servicio ofrecido por los concesionarios o por los autorizados a comercializar, dentro del marco legal aplicable, sin limitar, degradar, restringir o discriminar el acceso a los mismos. El proveedor no limita el derecho de los usuarios del servicio de acceso a Internet a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos que se conecten a su red, siempre y cuando éstos se encuentren homologados, tomando en cuenta que no todos los dispositivos existentes en el mercado cuentan con las caracterizarías técnicas para poder ser conectados a su red.

II. No discriminación. El proveedor se abstiene de obstruir, interferir, inspeccionar, filtrar o discriminar contenidos, aplicaciones o servicio;

III. Privacidad. El proveedor preserva la privacidad de los usuarios y la seguridad de la red;

IV. Transparencia e información. Las características del servicio ofrecido, incluyendo las políticas de gestión de tráfico y administración de red autorizada por el Instituto, velocidad, calidad, la naturaleza y garantía del servicio, se pueden consultar en la página de internet y en el Código de prácticas comerciales del proveedor.

V. Gestión de tráfico. El proveedor podrá tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red conforme a las políticas autorizadas por el Instituto, a fin de garantizar la calidad o la velocidad de servicio contratada por el usuario, siempre que ello no constituya una práctica contraria a la sana competencia y libre concurrencia;

VI. Calidad. El proveedor debe preservar los niveles mínimos de calidad que al efecto se establezcan en los lineamientos respectivos.

2.- ACCESO A CONTENIDOS DE INTERNET

Los Usuarios podrán acceder de manera libre y sin restricciones a cualquier contenido, aplicación o servicio provisto por esta siempre y cuando no exista un mandamiento judicial que obligue al operador a suspender el servicio de forma parcial o total.

Los concesionarios y autorizados podrán tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red conforme a las políticas autorizadas por el Instituto, a fin de garantizar la calidad o la velocidad de servicio contratada por el usuario, siempre que ello no constituya una práctica contraria a la sana competencia y libre concurrencia.

3.- POLITICAS DE GESTIO Y ADMINISTRACION DE TRAFICO.

Las políticas de gestión de tráfico y administración de red son un conjunto de técnicas utilizadas por los proveedores del servicio de acceso a Internet para el manejo, tratamiento y procesamiento del flujo de tráfico cursado por una red pública de telecomunicaciones.

Las técnicas de gestión implementadas por CAPA 3 INTERNET, en todo momento se encaminan a asegurar la calidad, capacidad y velocidad del servicio de acceso a Internet provisto a los Usuarios, y al mismo tiempo preservar la integridad y la seguridad.

Las políticas utilizadas en ningún momento impedirán, limitarán, degradarán, restringirán o discriminarán el libre acceso a cualquier contenido, aplicación o servicio, y tampoco violarán la privacidad o intervendrán las comunicaciones de los Usuarios.

3.1.- Congestión en el tráfico:

Durante períodos de congestión, las aplicaciones que consumen mucho ancho de banda, como la transmisión de video y la descarga de archivos, pueden disminuir su velocidad más que otras aplicaciones. Como resultado, la calidad del flujo de video puede reducirse y / o puede producirse un almacenamiento en búfer. Además, las descargas de archivos pueden tardar más en completarse durante los períodos de congestión. En situaciones de congestión más severa, es posible que sea necesario disminuir la velocidad todas las aplicaciones y, en tales casos, la descarga de las páginas web puede llevar más tiempo. La reducción de velocidad aplica para todo el tráfico de datos, por lo que de no implementarla podría afectar la operación y a la calidad de los servicios ofrecidos en perjuicio de los usuarios finales.

3.2.- Bloqueo de contenido:

CAPA 3 INTERNET no lleva a cabo el bloqueo de tráfico de datos en los Servicios que tengan contratados los usuarios finales.

El bloqueo es la técnica que impide el acceso de los Usuarios a un sitio web determinado o la utilización de un tipo de contenido o servicio particular, ya sea de manera temporal o permanente.

CAPA 3 INTERNET podrá bloquear el acceso en caso de existir riesgo a la integridad del tráfico de datos y a las comunicaciones legítimas de los Usuarios dada a la existencia de máquinas que tienen gusanos, virus u otro malware que genere grandes cantidades de correo electrónico no deseado.

3.3.- Seguridad de la red:

Consiste en la protección e implementación de técnicas informáticas para la seguridad e integridad del tráfico de datos del proveedor del servicio de internet. Dicha protección es implementada mediante la implementación de políticas/reglas en el firewall(cortafuegos), esto con la finalidad de aislar a clientes dentro de la red de ataques externos e internos.

Se aplica en casos donde existen ataques de agentes externos e internos que buscan alterar, degradar, perturbar o corromper el funcionamiento eficiente y correcto del tráfico de datos (virus, malware, spyware y ransomware). Para estos casos, la implementación de técnicas informáticas por parte del proveedor del servicio de internet hará todo lo posible por anular, atacar y desaparecer el ataque.

3.4.-Beneficios a los Usuarios:

Las políticas de administración y gestión de tráfico enunciadas ofrecen como beneficio a los Usuarios finales:

- Reducción del tiempo de respuesta en la entrega de contenido hacia los usuarios.
- Optimización en consumo de ancho de banda del operador hacia la red de tránsito.
- Reducción de costos operativos en enlaces hacia red de tránsito.
- Mayor seguridad al navegar por la web.
- Disminución de la brecha digital.

Asimismo, no implementar tales políticas traería como consecuencia:

- Incremento del tiempo de respuesta en el envío y recepción de contenido.
- Aumento de los costos operativos en enlaces hacia red de tránsito.
- Degradación de la experiencia de usuario.
- Mayor inseguridad al navegar por la web.
- Aumento de la brecha digital.

4.- RECOMENDACIONES DE USO.

Para favorecer y fomentar la seguridad al navegar por Internet, así como minimizar riesgos a la privacidad de los Usuarios, **CAPA 3 INTERNET** hace las siguientes recomendaciones:

1. **Evita acceder a contenidos, aplicaciones o servicios no confiables o de dudosa reputación**: Los sitios web que se encuentran dentro de la red de internet son susceptibles de encontrarse infectados o controlados por agentes externos que buscan acceder, robar e inclusive eliminar datos de tus dispositivos. Para evitar ser objeto de pérdida o robo de información, utiliza contraseñas o bloqueos en tus dispositivos por medio de códigos alfanuméricos, no accedas a contenido publicitario que contengan promociones gratuitas y accede a sitios programados con seguridad (dominio y protocolo HTTPS).
2. **Mantener el sistema operativo actualizado**: Las actualizaciones del sistema operativo de tus dispositivos suelen implementar parches para solucionar problemas técnicos o brechas de seguridad, lo que brindará mayor protección en contra de nuevos malwares.
3. **Respalda tu información**: En caso de algún daño que impida el acceso a la información dentro de un dispositivo, se recomienda que previo a dicho suceso efectúe una copia de seguridad o respaldo de sus datos dentro de algún medio de almacenamiento como puede ser un disco duro o por medio de servicio de la nube ofrecido por algún sitio web confiable.
4. **Instalar un Antivirus**: Los antivirus son programas cuyo objetivo es detectar y eliminar virus informáticos o malwares al navegar por la web y descargar datos, además algunos de ellos son capaces de buscar y detectar virus para bloquearlos, así como desinfectar archivos y prevenir una infección de estos, por lo que contar con dicho programa

ofrecerá mayor protección y seguridad al utilizar el Internet; son fáciles de descargar e instalar y existen varias opciones para todos los sistemas operativos.

5. **No proporcionar información sensible en sitios inseguros**: Se recomienda no proporcionar datos personales, números de cuenta, tarjetas bancarias, números telefónicos, NIP's de seguridad, tokens, códigos de seguridad de tarjetas, contraseñas, pins, tokens, imágenes, fotografías, etc., a menos de que estés plenamente convencido de la autenticidad del sitio y que las finalidades de uso sean las pertinentes.
6. **Actualizar frecuentemente las contraseñas**: Se recomienda cambiar contraseñas frecuentemente haciendo uso de contraseñas seguras que tengan al menos 8 caracteres y que tengan una combinación de números, letras mayúsculas, minúsculas y símbolos. Además, se aconseja no establecer la misma contraseña para diversos perfiles y cuentas, sino utilizar una única para cada sitio.
7. **Configurar adecuadamente la privacidad en redes sociales**: Revisa la configuración de seguridad en las redes sociales que uses y evita compartir información personal y confidencial.
8. **Cuidar los permisos en las aplicaciones**: Al instalar aplicaciones en los dispositivos, algunas aplicaciones solicitar permisos para acceder a carpetas como la galería de fotos y vídeos, así como para acceder al hardware del dispositivo como la cámara y micrófono, por lo que es importante permitir dicho acceso sólo a aplicaciones de confianza y descargadas desde plataformas oficiales, y en su caso administrar las aplicaciones que tienen tales permisos desde la configuración del dispositivo.
9. **Realizar descargas de sitios oficiales y confiables**: Para descargar software, aplicaciones y archivos de forma segura se recomienda no modificar la configuración de fábrica de los equipos; descargar software y aplicaciones solo de sitios web y tiendas oficiales; verificar los permisos y accesos requeridos por el software o aplicación antes de otorgarlos.
10. **Evitar acceder desde puntos Wi-Fi inseguros**: Evitar conectarse desde conexiones Wi-Fi desconocidas o de red abierta, puesto que mediante éstas es sumamente fácil acceder a datos sensibles y confidenciales, por lo que se recomienda utilizar una conexión VPN para que la información que transmitas vaya cifrada de punto a punto.

5.- MARCO LEGAL APLICABLE.

El presente Código se apega a lo dispuesto en la Ley Federal de Telecomunicaciones y Radiodifusión, así como 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, publicados en el Diario Oficial de la Federación el 5 de julio de 2021 y expedidos por el Instituto Federal de Telecomunicaciones.