CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE RED.

MARTIN MONTERO TORRES

ÍNDICE

OBJETIVO..... 2

CONCESIONARIO PRESTADOR DEL SERVICIO..... 3

DERECHOS DE LOS USUARIOS FINALES DEL SERVICIO DE ACCESO A INTERNET 4

POLÍTICAS DE GESTIÓN Y ADMINISTRACIÓN DE TRÁFICO DEL PROVEEDOR DEL SERVICIO DE INTERNET 6

RECOMENDACIONES PARA LOS USUARIOS FINALES CON LA FINALIDAD DE MINIMIZAR RIESGOS DE PRIVACIDAD..... 10

MARCO LEGAL APLICABLE..... 13

OBJETIVO

El presente Código de Políticas de Gestión de Tráfico y Administración de Red tiene como objetivo principal poner a la disposición de los usuarios finales el conjunto de actividades, técnicas y procedimientos que el concesionario **Martin Montero Torres** con nombre comercial **Monteros Networks,** utiliza para la operación y aprovechamiento de su red pública de telecomunicaciones así como del manejo, tratamiento y procesamiento del flujo de tráfico que cursa dentro de la misma red, este tipo de acciones son necesarias para el manejo del tráfico de la red, dar cumplimiento a las condiciones de contratación de los servicios con el usuario final y hacer frente a problemas de congestión, seguridad de la red y de la privacidad, entre otros.

Martin Montero Torres tiene como objetivo mantener la permanencia de los servicios, asegurar la libre elección de los suscriptores, trato no discriminatorio, privacidad e inviolabilidad de las comunicaciones; de igual forma, mantener la calidad, capacidad y velocidad de los servicios contratados con base a estándares nacionales e internacionales, buenas prácticas en la industria de telecomunicaciones y normatividad aplicable.

Asimismo, la implementación continua de gestión de tráfico y administración conlleva beneficios respecto al funcionamiento continuo y eficiente de la red, pues permite a salvaguardar la seguridad e integridad de su red pública de telecomunicaciones (por ej., ante ataques maliciosos que puedan en consecuencia vulnerar a **Martin Montero Torres** y a la gama de servicios que ofrecen tanto a nivel mayorista como minorista), ofrecer distintas gamas de servicio dependiendo de las necesidades de los usuarios, así como garantizar los niveles de calidad de servicio que le son contratados.

Lo anterior con apego a lo señalado en los artículos 1, 2 fracción VII y 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* correlativo con el artículo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión.

CONCESIONARIO PRESTADOR DEL SERVICIO.

Martin Montero Torres es titular de una concesión única para uso comercial emitido por el Instituto Federal de Telecomunicaciones para proveer servicios de telecomunicaciones y radiodifusión específicamente el servicio de acceso a internet, ofreciendo a los usuarios finales distintos paquetes de datos. Los servicios que brinda están debidamente autorizados por el Instituto Federal de Telecomunicaciones (en adelante IFT).

Martin Montero Torres 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 de la red, 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 de la red 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 por la red. 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 de las redes para cumplir con la calidad contratada por los usuarios. Al respecto, es relevante reiterar que las acciones que tome **Martin Montero**

Torres ante una congestión temporal o excepcional no podrán implicar que exista discriminación entre tipos de tráfico similares.

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 a la red de **Martin Montero Torres.** Al respecto, se enfatiza que la aplicación de políticas que resulten en afectaciones al servicio de acceso a Internet podrá realizarse en tanto resulte indispensable para atender la situación.

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 ***924-152-0016,*** así mismo podrá enviar sus preguntas al correo electrónico **monterosnetwork@gmail.com o soporte@monteros.network** con atención las 24 horas del día los 365 días del año además de la información pública de los servicios que puede ser consultada en la página web **www.monteros.network .**Por otra parte, el domicilio de atención a clientes se ubica en ***calle Miguel Alemán #44 , colonia Cruz del Milagro, Sayula de Áleman, Veracruz de Ignacio de la Llave, C.P. 96151.***

DERECHOS DE LOS USUARIOS FINALES DEL SERVICIO DE ACCESO A INTERNET

Martin Montero Torres respetará en todo momento los derechos de los usuarios finales que consumen el servicio de acceso a internet dentro de su red pública de telecomunicaciones. Dichos derechos son aquellos que se enlistan a continuación:

I. **LIBRE ELECCIÓN.** El usuario final podrá acceder a cualquier contenido, aplicación o servicio ofrecido por el proveedor del servicio de internet dentro del marco legal aplicable, sin limitar, degradar, restringir o discriminar el acceso a los mismos. Los usuarios pueden acceder e intercambiar contenido y tráfico de manera abierta por internet, haciendo uso de dispositivos homologados en el país.

II. **NO DISCRIMINACIÓN.** El proveedor del servicio de internet se abstendrá de obstruir, interferir, inspeccionar, filtrar o discriminar contenidos, aplicaciones o servicio al usuario final, salvo en el caso que el mismo usuario solicite un servicio

adicional que provea dichas características (ej. bloqueo de contenidos, servicios y mecanismos de control parental, entre otros).

III. **PRIVACIDAD.** El proveedor del servicio de internet deberá preservar la privacidad del usuario final y la seguridad de la red. El proveedor cuenta con un Aviso de Privacidad donde el cliente puede conocer el procedimiento bajo el cual es tratada su información, conforme a la normatividad aplicable.

IV. **TRANSPARENCIA E INFORMACIÓN**. El proveedor del servicio de internet deberá publicar en su página de internet la información relativa a las características del servicio ofrecido como es la velocidad, calidad, la naturaleza y garantía del servicio así de indicar las políticas de administración de la red y gestión de tráfico.

V. **GESTIÓN DE TRÁFICO**. El proveedor del servicio de internet podrá tomar las medidas o acciones necesarias para la adecuada gestión de tráfico y administración de la red a fin de garantizar la calidad o la velocidad de servicio contratada por el usuario final, siempre que ello no constituya una práctica contraria a la sana competencia y libre concurrencia;

VI. **CALIDAD.** El proveedor del servicio de internet deberá preservar los niveles mínimos de calidad que al efecto se establecen dentro de los *Lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores del servicio fijo* emitidos por el IFT y publicados el día veinticinco de febrero de dos mil veinte así de las demás disposiciones administrativas y técnicas aplicables que emita o haya emitido la autoridad competente.

VII. **DESARROLLO SOSTENIDO DE LA INFRAESTRUCTURA**. En los lineamientos respectivos, el IFT fomentará el crecimiento sostenido de la infraestructura de telecomunicaciones, por lo tanto, el proveedor del servicio de internet se compromete a desarrollar, mantener vigente y operativa su red, basándose en la estrategia del negocio y en la disponibilidad física y técnica de dicha red, manteniendo en todo momento el objetivo de la satisfacción de sus clientes.

POLÍTICAS DE GESTIÓN Y ADMINISTRACIÓN DE TRÁFICO DEL PROVEEDOR DEL SERVICIO DE INTERNET

A continuación, se explicarán cada una de las políticas de gestión y administración de tráfico que **Martin Montero Torres** aplica dentro de su red pública de telecomunicaciones con la finalidad de proveer un servicio eficiente y de calidad, siendo dicha explicación de fácil entendimiento para los usuarios finales.

GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE LA RED	
CONCEPTO	Consiste en la implementación de técnicas para optimizar el tráfico el cual, son acciones que realizan con el objeto de mejorar la experiencia de navegación al usuario, en la que se administrará el tráfico de datos en casos de congestión.
CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.	Consiste en llevar a cabo las acciones para optimizar el tráfico en caso de la saturación de la red. Haciendo uso adecuado de los recursos disponibles en un momento y ubicación determinados. Se utiliza para preservar la operación y calidad de la red, de tal manera que se garantice la mejor experiencia del conjunto de usuarios finales en la red, únicamente ante situaciones que podrían comprometer la calidad del servicio. Los casos más comunes donde se aplicará los controles de congestión serían los siguientes: • Fallas técnicas en la red • Fluctuaciones imprevisibles en el flujo de tráfico de la red (demasiado consumo de datos por los usuarios finales) • Cualquier otra situación donde exista un funcionamiento incorrecto en la red o en posibles apariciones de los casos enlistados, tratando de evitar en todo momento su origen.
IMPACTO EN EL SERVICIO DE INTERNET AL USUARIO FINAL.	Posible reducción a la velocidad del servicio de acceso a internet contratado por el usuario final, aunque dicho impacto será de manera temporal e inmediato.
POSIBLES AFECTACIONES EN CASO DE NO APLICARSE	**A LA RED.** De no aplicarse, la red colapsaría debido a la expansión de la congestión de datos, intermitencia y altas latencias.

	AL USUARIO FINAL O EN SU SUS COMUNICACIONES. Puede verse afectada directamente presentando lentitud o intermitencias en la navegación de la red.

BLOQUEO DE CONTENIDO	
CONCEPTO	Es la técnica que impide el acceso de los usuarios no registrados o equipos que generen afectaciones en la red, en los servicios, o en las condiciones de seguridad en la red.
CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.	Está técnica no se lleva acabo el bloqueo del tráfico de datos en los servicios del usuario final, solo se establece un filtro en la entrega del servicio de acceso a internet en equipos no autorizados por el prestador del servicio.
IMPACTO EN EL SERVICIO DE INTERNET AL USUARIO FINAL.	No tendrá acceso al contenido, aplicación o servicio bloqueado dentro del plazo que persista el supuesto que lo originó.
POSIBLES AFECTACIONES EN CASO DE NO APLICARSE	**A LA RED.** De no bloquearse contenido que afecten la integridad y seguridad de la red o que sean señalados como ilícitos, se perturbaría y se comprometería el tráfico que exista dentro de la misma red, infectándose de posibles virus o amenazas de terceros. En el caso de bloqueo de contenido a petición del usuario final, no tendría afectación alguna en la red. **AL USUARIO FINAL O EN SU SUS COMUNICACIONES.** De no bloquearse contenido que afecten la integridad y seguridad de la red o que sean señalados como ilícitos, existe una gran posibilidad de fuga de datos privados de los usuarios finales así de una evidente interceptación de las comunicaciones por parte de terceros.

PRIORIZACIÓN DE DATOS	
CONCEPTO	Consiste en dar prioridad a la transmisión de ciertos tipos de datos frente a otros. Dichas prioridades atienden a consideraciones técnicas que usualmente recae en la decisión del proveedor del servicio de internet.
CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.	Se aplica en todo momento de la provisión del servicio de internet al usuario final. Se utiliza para una mejor transmisión de datos sin la necesidad de degradar la calidad del resto del

	tráfico y permite establecer funciones de balanceo, eficiencia en el funcionamiento de la red y soluciones de seguridad.
IMPACTO EN EL SERVICIO DE INTERNET AL USUARIO FINAL.	La percepción del usuario derivado de la implementación de la priorización de datos es generar que los tiempos de respuesta en el acceso de la red y/o descargas de contenidos se mantenga o disminuya, y con ello, los usuarios pudieran experimentar una mejora en la navegación, Al realizar esta técnica se obtiene mejores tiempos de respuesta latencia.
POSIBLES AFECTACIONES EN CASO DE NO APLICARSE	**A LA RED.** Generaría altos costos operativos en la red del prestador del servicio. **AL USUARIO FINAL O EN SU SUS COMUNICACIONES.** Aumentaría la posibilidad de escenarios de congestión de tráfico, altas latencias y problemas en la navegación en la red para el usuario final.

SEGURIDAD DE LA RED	
CONCEPTO	Consiste en la protección e implementación de técnicas informáticas para la seguridad e integridad de la red del proveedor del servicio de internet. Dicha protección es implementada mediante la creación de políticas/reglas en el firewall, esto con la finalidad de aislar a clientes dentro de la red de ataques externos e internos.
CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.	Se aplicarán protocolos de seguridad para el acceso a los diferentes equipos de la red, 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, implementando las siguientes medidas en la red: • **Autentificación de comunicación Prestador de servicio a usuario final:** Se encapsula la comunicación desde prestador de servicio hacia el usuario final, otorgando un acceso único e intransferible, donde identifica y clasifica cada usuario final. • **Sustitución de equipo alterado/modificado:** En caso de manipulación no autorizada del equipo terminal del usuario final, se reestablecerá a los

	valores iniciales o sustituirá el equipo terminal para evitar problemas de seguridad. • **Solo personal Autorizado:** La instalación y/o soporte debe ser otorgado por personal autorizado por el prestador de servicio. • **Firewall:** Sistema diseñado para proteger las redes privadas del acceso no autorizado y no verificado en una conexión a Internet, evitando posibles ataques.
IMPACTO EN EL SERVICIO DE INTERNET AL USUARIO FINAL.	Puede que la velocidad de navegación del usuario final baje o no tenga acceso a contenido, aplicación o servicio por causas originadas del ataque. El proveedor del servicio de internet se comprometerá en realizar todas las acciones posibles que tenga a su alcance para combatir cualquier ataque en la red detectándose a través de lo siguiente: • **Firewall (Filtrado de paquetes):** Sistema que es capaz de controlar el acceso a la red y, por lo tanto, protege su red. Actúa como un filtro para bloquear el tráfico entrante no legítimo antes de que pueda ingresar a la red y causar daños. • **Limite el número de puertos accesibles:** Se realiza una limitación de puertos específicos para evitar posibles ataques; solo si el usuario final solicita la liberación de dichos puertos, este será otorgado. • **Monitoreo de registros de red:** Ayuda a recopilar y analizar datos de registro de diferentes tipos de dispositivos de red y dar prevención de intrusiones no legitimas.
POSIBLES AFECTACIONES EN CASO DE NO APLICARSE	**A LA RED.** Puede comprometerse el tráfico de datos que se encuentre en la red, infectándose de posibles virus y en consecuencia dañando la estabilidad del servicio de internet. **AL USUARIO FINAL O EN SU SUS COMUNICACIONES.** Posible afectación en la velocidad de navegación además de acceso no autorizado a terceros causantes del ataque a datos privados además de las comunicaciones del usuario final.

RECOMENDACIONES PARA LOS USUARIOS FINALES CON LA FINALIDAD DE MINIMIZAR RIESGOS DE PRIVACIDAD

Martin Montero Torres recomienda a sus usuarios finales, así como al público en general, a seguir las siguientes indicaciones para navegar dentro del internet con mayor seguridad y así obtener una protección más adecuada y amplia de nuestros datos personales.

Las recomendaciones son las que se detallarán a continuación:

1. **Utiliza contraseñas robustas:** Se sugiere que sea en todos los dispositivos o aplicaciones, en caso de que sospeches de robo, cámbiala inmediatamente. Procura utilizar diferentes contraseñas para tus cuentas de redes sociales, sitios financieros, sitios de compras y trabajo. Cuando crees una contraseña hazlo utilizando al menos 8 caracteres, combina letras mayúsculas, minúsculas, números y caracteres especiales.
2. **Actualización frecuente de contraseñas**: Cambia tu contraseña de manera frecuente.
3. **Visitar sitios seguros:** Asegurándote que los sitios que visitas sean oficiales y que la dirección contenga “HTTPS”, ya que es un protocolo de comunicación de internet que protege la integridad y la confidencialidad de los datos intercambiados.
4. **Programa de Seguridad en Internet:** Es valioso asegurarse que los equipos a través de los que accede al Servicio cuenten con un programa llamado “navegadores” que brinde protección a l navegar en Internet, el cual incluya un antivirus actualizado a fin de prevenir ataques de programas maliciosos
5. **Utiliza Herramientas:** para prevenir programas maliciosos, anuncios no deseados (Adware); seguimiento y almacenamiento de contraseñas, tecleo o información de tarjetas de crédito (Keylogger); obtención de información personal y/o confidencial (Phishing), entre otros.
6. **Evitar navegación en sitios no conocidos**: Al navegar en Internet asegúrate de validar que el sitio, servicio, contenido o aplicación navegado cuente con

certificados de seguridad y sellos de confianza emitidos por auditores y certificadores reconocidos.

7. **Proporciona información solo cuando estés seguro:** Cuida la información que compartes. Recomendamos no proporcionar datos personales, números telefónicos, números de cuenta, tarjetas bancarias, códigos de seguridad de tarjetas, entre otros, a menos de que estés plenamente convencido de la autenticidad del sitio y que las finalidades de uso sean las pertinentes.
8. **Descarga programas informáticos (software) y aplicaciones de sitios oficiales y confiables:** Para descargar software y aplicaciones de forma segura, se recomiendo solo descargarlos solo en los sitios web oficiales y corroborar los permisos y accesos requeridos por el software antes de adquirirlo.
9. **Evita abrir correos de remitentes desconocidos**: Si recibes un correo electrónico con algún archivo adjunto que no estabas esperando evita abrir archivos ejecutables y/o link de páginas web.
10. **Asegura tus dispositivos**: Instala y mantén un programa de antivirus reconocido en tus dispositivos, Computadora de escritorio, Computadora portátil, celulares, tabletas, entre otros.
11. **Protege la información en dispositivos móviles**: Utiliza mecanismos de desbloqueo seguros como contraseñas biométricas, robustas o patrones. Mantén actualizados tus dispositivos con la versión más reciente de software. Realiza copias de seguridad, ya que te ayudarán a recuperar tu información en caso de pérdida o daño de tu dispositivo.
12. **Configuración de privacidad en redes sociales:** Revisa la configuración de seguridad en las redes sociales que uses y evita compartir información personal y/o confidencial. Recomendamos activar verificación en dos pasos.

13. **Control parental:** Instala herramientas de control parental para monitorear, restringir y controlar las actividades de los menores de edad cuando hagan uso de Internet.

Martin Montero Torres preserva la privacidad de los usuarios, así como la seguridad de la red y la inviolabilidad de sus comunicaciones privadas, por lo que de ninguna manera podrá monitorear, rastrear, inspeccionar o alterar el contenido específico del tráfico que transita por su red ni hacerse de información de los suscriptores que no sea necesaria para proveerles el servicio. Excepción a casos de solicitud expresa por parte de la autoridad competente/federal.

Para más información, consulta el Aviso de Privacidad en www.monteros.network

MARCO LEGAL APLICABLE

- Constitución Política de los Estados Unidos Mexicanos, artículos 1,6,7,28 y demás aplicables.
- Ley Federal de Telecomunicaciones y Radiodifusión artículos 145, 146 y demás aplicables.
- 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.
- Lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores del servicio fijo

VERSIÓN Y FECHA ÚLTIMA DE ACTUALIZACIÓN

Última actualización	**11 de agosto de 2022**
Versión	**1.0**
Elaboró	**Martin Montero Torres**