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

NETPACIFIC
JUAN CARLOS
LOPEZ VELASCO

ÍNDICE

OBJETIVO

El presente Código de Políticas de Gestión de Tráfico y Administración de Red tiene como objetivo principal poner a disposición de los usuarios finales el conjunto de actividades, técnicas y procedimientos que **JUAN CARLOS LÓPEZ VELASCO** cuenta con TÍTULO DE CONCESIÓN ÚNICA PARA USO COMERCIAL OTORGADO POR EL INSTITUTO FEDERAL DE TELECOMUNICACIONES CON NÚMERO DE FOLIO ELECTRÓNICO **FET102304CO-521068** y en lo sucesivo se denominará **"EL PROVEEDOR"** 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.

"EL PROVEEDOR" tiene como objetivo mantener la permanencia de nuestros 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 ejemplo, ante ataques maliciosos que puedan en consecuencia vulnerar a **"EL PROVEEDOR"** 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.

“EL PROVEEDOR” es titular de un TÍTULO DE 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).

“EL PROVEEDOR” 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 **“EL PROVEEDOR”** 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 **“EL PROVEEDOR”**. 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 **954 163 27 12**; asimismo podrá enviar sus preguntas al correo electrónico contacto@netpacific.mx 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 netpacific.mx.

Por otra parte, el domicilio de atención a clientes se ubica Calle 7A Norte, Número 308, Colonia Sector Juárez, C.P. 71980, Municipio San Pedro Mixtepec, Juquila, Estado de Oaxaca.

DERECHOS DE LOS USUARIOS FINALES DEL SERVICIO DE ACCESO A INTERNET

"EL PROVEEDOR" 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 **“EL PROVEEDOR”** 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.

TOPE DE DATOS	
CONCEPTO	Consiste en la supervisión de volumen de tráfico y el estrangulamiento de los datos una vez alcanzado el tope de consumo de datos que tiene el usuario final en su paquete.
CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.	Se aplica en el caso en el que el usuario final rebasa el límite de los datos ofrecidos por el proveedor del servicio de internet, quien procederá a impedir el acceso del servicio ya sea bajando la velocidad de transferencia o suspender el acceso a internet.
IMPACTO EN EL SERVICIO DE INTERNET AL USUARIO FINAL.	El usuario final no tendrá acceso al servicio de internet llegando al máximo contratado en su paquete, teniendo la opción de contratar un nuevo paquete que se ajuste a sus necesidades una vez alcanzado este límite.

POSIBLES AFECTACIONES EN CASO DE NO APLICARSE	**A LA RED.** Afectación al tráfico fluido dentro de la red, debido a una posible congestión y/o saturación de tráfico de datos, propiciando así la reducción de velocidad en la navegación de los demás usuarios finales en las horas pico debido a esto. **AL USUARIO FINAL O EN SUS COMUNICACIONES.** No tendría afectación en su servicio, sin embargo, sí pudiese repercutir a terceros usuarios que se encuentren consumiendo sus datos disponibles y, de aparecer 6 congestiones en la red, recientan disminución en su velocidad de datos contratados.

GESTIÓN DE CONGESTIÓN / OPTIMIZACIÓN DE TRÁFICO	
CONCEPTO	Para optimizar el tráfico, utilizamos diferentes técnicas para gestionar la red, especialmente en periodos de congestión en la red para mejorar la experiencia la navegación del usuario.
CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.	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. Su utilidad radica en balancear el tráfico en ciertas secciones de la red para descongestionar la parte donde existen anomalías, logrando estabilizar el flujo de datos eficiente en la red. Es importante señalar que su implementación no repercute al bloqueo o discriminación de contenido, aplicación o servicio de internet.
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 a la totalidad de las secciones de dicha red. **AL USUARIO FINAL O EN SUS COMUNICACIONES.** Bajaría considerablemente la velocidad de acceso a internet contratada del usuario final, siendo inclusive hasta totalmente nulo el servicio ante la saturación de datos en la red.

PRIORIZACION 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.	El usuario podrá percibir que existe cierta mayor fluidez de tráfico de datos en ciertas características del contenido, aplicación o servicio que quiera acceder a internet.
POSIBLES AFECTACIONES EN CASO DE NO APLICARSE	**A LA RED.** Posibles acontecimientos de congestionamiento en partes de la red así de la deficiencia en el tráfico de datos. **AL USUARIO FINAL O EN SUS COMUNICACIONES.** Si bien no impactaría en un primer momento la velocidad o calidad del servicio contratado por el usuario final, podría limitarse tanto la calidad del servicio que no se sacaría el mayor grado de aprovechamiento para una mejor experiencia del usuario final en los servicios proveídos por el concesionario.

BLOQUEO DE CONTENIDO	
CONCEPTO	Consiste en impedir el acceso al usuario final a un sitio web determinado o utilizar cierto tipo de contenido o servicio particular en cierto plazo.
CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.	Los casos en los que se aplicaría esta técnica serían los siguientes: • A petición expresa y consentida del usuario final. En este supuesto, su utilización radicaría más a intereses propios del usuario final quien señalará de manera específica el contenido que desea restringir al proveedor del servicio de internet; • Cuando cierto contenido, aplicación o servicio dentro de internet sea un riesgo técnicamente comprobable y pueda repercutir a la integridad y seguridad de la red, así como la privacidad e inviolabilidad de las comunicaciones de los usuarios finales. Se utilizaría con la finalidad de garantizar la continuidad del funcionamiento de la red así de la seguridad de los usuarios finales y sus equipos. • Contenido, aplicación o servicio determinado como ilícitos por la autoridad competente por medio de ordenamiento jurídico aplicable y obligatorio para el proveedor del servicio de internet.
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 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

¿QUÉ MEDIDAS IMPLEMENTA PARA GARANTIZAR LA SEGURIDAD DE LA RED?	Consiste en la protección e implementación de técnicas informáticas para la seguridad e integridad de la red del proveedor del servicio de internet. Si llegara a presentarse un ataque a la red de internet, Juan Carlos López Velasco se reserva el derecho de utilizar técnicas de administración, para preservar la seguridad, estabilidad y funcionabilidad de la red de internet. Se aplica en casos donde existen ataques de agentes externos e internos que buscan alterar, degradar, perturbar o corromper el funcionamiento eficiente y correcto de la red (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.
¿CÓMO DETECTA INVASIONES EN SU RED?	**Denegación de servicio (DoS, por sus siglas en inglés):** Este tipo de ataque puede causar la sobrecarga de un enrutador. Lo que significa que el uso de la CPU llega al 100% y el enrutador puede volverse inaccesible con tiempos de espera. Todas las operaciones en paquetes que pueden consumir un procesamiento significativo de la CPU, como el firewall (filtro, NAT, mangle), el registro y las colas, pueden provocar una sobrecarga si llegan demasiados paquetes por segundo al router. **Protocolo de mensajes de control de Internet (ICMP, por sus siglas en inglés):** Este protocolo ayuda a las redes a resolver problema de comunicación, los hackers pueden hacer uso de ICMP para poder buscar hosts activos en la red. El ataque más común es: ICMP Smurf: Este ataque es una versión más sofisticada de un ataque DDos, donde el atacante genera una gran cantidad

	de paquetes ICMP de origen falsificados y tienen como destino la IP del servidor victima. Generalmente, proviene de la red LAN, debido a que es un tipo de tráfico ICMP, pero se genera tráfico hacia la red broadcast, dado que una única dirección de broadcast admite 255 host, entonces este ataque amplifica un solo paquete ping 255 veces a nivel de peticiones. **Fuerza Bruta:** Es un método de prueba y error, donde el atacante utiliza herramientas que permite probar todas las combinaciones posibles hasta encontrar el texto que fue cifrado
¿CUÁLES SON LAS RECOMENDACIONES LE DA A SUS CLIENTES PARA MANTENER LA PRIVACIDAD DE SUS DATOS?	• Utilizar navegadores que cuenten con identificadores para ataques de phishing. continuamente la instalación de parches de seguridad en sistemas operativos y aplicaciones. • Contar con antivirus en los equipos con los que se acceda a la red global de internet. • Observar los enlaces y páginas que se pretenden abrir de tal forma que, se evite acceder a sitios inseguros o donde se solicite información confidencial, personal o sensible. • Cerciorarse de que se está navegando en sitios web seguros. • No hacer clic en correos electrónicos no solicitados o que provengan de fuentes desconocidas. • Evitar hacer caso de mensajes cuyo contenido sea atractivo, por ejemplo, adjudicación de premios provenientes de concursos donde el usuario no participó. • Evitar relevar contraseñas de los sitios web que se frecuentan, por ejemplo, de correos electrónicos, banca electrónica, servicios públicos o cualquier otro. • Utilizar herramientas de borrado seguro de información en los equipos de cómputo que sean desechados por el usuario. • Actualizar periódicamente las contraseñas de sistemas y/o aplicaciones para prevenir que usuarios no autorizados tengan acceso a la información de los usuarios. • Utilizar contraseñas seguras y robustas para proteger el acceso al sistema operativo, aplicaciones y cuentas personales de los usuarios. • Habilitar doble factor de autenticación en aquellos sitios en donde sea posible.

¿CÓMO GARANTIZA LA PRIVACIDAD DE LOS DATOS DE SUS CLIENTES?	Se maneja una cláusula de confidencialidad en el contrato de servicio, y toda la información que es transmitida por la red de WISP se transporta de manera encriptada

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

"EL PROVEEDOR" 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. *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. *Instala antivirus en tus equipos de navegación.* Debido a que existen diversos tipos de softwares maliciosos cuyo objetivo es impenetrar en tus dispositivos para extraer tu información privada, se recomienda la utilización de antivirus que son programas digitales que brindan una mayor seguridad y protección a tus equipos ante cualquier tipo de amenaza cibernética.
3. *Actualiza tu sistema operativo, programas y aplicaciones instaladas en tus dispositivos.* Los desarrolladores fabricantes de los programas y aplicaciones se encuentran constantemente reforzando la estabilidad, así como la seguridad del software con la finalidad de evitar vacíos de que puedan ser aprovechados por los atacantes para la obtención de información; de lo anterior se sugiere actualizarlos de manera periódica y así garantizar una adecuada protección a sus dispositivos, así como de su información.
4. *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.

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	20 DE DICIEMBRE DE 2022
Versión	**1.0**
Elaboró	**JUAN CARLOS LÓPEZ VELASCO**