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

NOEVE
tecnologia y redes

EVERARDO VIDAL HERNANDEZ

ÍNDICE

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 **EVERARDO VIDAL HERNANDEZ,** (en adelante "**EL PROVEEDOR"**) con nombre comercial **NOEVE TECNOLOGÍA Y REDES (NOEVETYR),** 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 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 **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 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).

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 los números telefónicos ***7121615732*** *y* ***7121007614,*** *asimismo* podrá enviar sus preguntas al correo electrónico serviciosnoeve@gmail.com 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.noevetyr.com. Por otra parte, el domicilio de atención a clientes se ubica en Avenida. Independencia sin número, manzana #2, Santo Domingo de Guzmán, Ixtlahuaca, Estado de México. C.P.50773.

DERECHO 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.

Priorización de tráfico	
CONCEPTO	La priorización de tráfico es un tipo de Calidad de servicio enfocado en marcar los tipos de conexiones por servicio y priorizarlos de acuerdo a un orden preestablecido por el administrador o implementador, el éxito o fracaso de una priorización depende en su totalidad de la exactitud al identificar un servicio, aunque todos tienen un margen de error o una tasa de Éxito, entre mas alta sea la tasa de éxito mas exacto será la priorización y mejor será la experiencia del usuario al navegar por nuestro servicio como proveedor de internet. Dependiendo de la necesidad de la red se hace el estudio para realizar la priorización del tráfico. ¿Qué es la QoS? Calidad de servicio (QoS) es el término que se utiliza para definir la capacidad de una red para proporcionar diferentes niveles de garantías de servicio a las diversas formas de tráfico. La QoS es una técnica para optimizar el uso de la red priorizando el tráfico con base a sus objetivos de uso. Cada red es diferente en cuanto a la naturaleza del uso y los procesos que se siguen. Dependiendo de los diferentes objetivos comerciales o personales, la red se utiliza para diferentes propósitos en función de las necesidades de tráfico que se deben priorizar en la red. La QoS es un conjunto de normas y técnicas para garantizar un alto rendimiento de las aplicaciones críticas en la red. La QoS permite garantizar un alto rendimiento en la red, asignando la máxima prioridad a aquellas aplicaciones que son altamente críticas para el cliente. Esto garantiza la rápida entrega de aplicaciones críticas, lo cual permite utilizar la red de manera óptima.
CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.	No todo el tráfico que fluye en cada red es igual de importante. Por ejemplo, el tráfico perteneciente a la telefonía

	VoIP o a las peticiones de resoluciones de nombres DNS, son mucho más importantes que el tráfico que un usuario esté generando por el uso de redes P2P. Cuando tenemos una priorización de tráfico con una tasa de éxito elevada, podemos asegurarles a nuestros clientes que sus megas van a estar disponibles para sus servicios más usados o considerados hoy en día de uso de primer nivel como Streaming de video de múltiples plataformas. También se considera de primer nivel el uso de todas las redes sociales comunes en Latinoamérica. Esto tipo de QoS garantiza indefinidamente prioridad para los servicios anteriormente mencionados, así el usuario final usara pocos megas en actualizaciones e instalaciones u otros tipos de servicios que no sean de alta prioridad. Al momento que el cliente demande uno de estos servicios se le va dar prioridad en sus megas para estos.
IMPACTO EN EL SERVICIO DE INTERNET AL USUARIO FINAL.	En esta era actual de redes convergentes, es una sola red la que maneja varios tipos de tráfico como voz, datos y video. Lo que significa que todos ellos tienen las mismas posibilidades de ser afectados cuando se produce una congestión. Esto lleva a que se produzca una batalla entre las aplicaciones críticas para el usuario y las demás aplicaciones. Para hacer un uso eficiente del ancho de banda de red, es esencial que las aplicaciones críticas para el usuario tengan una mayor prioridad sobre las demás aplicaciones. Por lo tanto, priorizar el tipo de tráfico o aplicaciones, se vuelve un requisito indispensable. Las aplicaciones o tráfico que se ejecutan en la red, pueden ser de tipo voz, datos y video, los cuales manejan alguno de estos protocolos: SMTP (protocolo de transferencia simple de correo) Es el protocolo estándar para servicios de mensajería en una red TCP / IP. SMTP ofrece la posibilidad de enviar y recibir correos electrónicos. SMTP es un protocolo de capa de aplicación que generalmente usa el puerto 25. POP3 (Post Office Protocol) POP es un protocolo estándar de Internet que extrae y recupera el correo electrónico de un servidor de correo electrónico remoto para permitir que la máquina host acceda a él. POP es un protocolo de capa de aplicación del modelo

	OSI que ofrece a los usuarios finales la capacidad de recuperar y recibir correo electrónico. HTTP (protocolo de transferencia de hipertexto) HTTP es un conjunto de reglas para transferir archivos (texto, imágenes gráficas, archivos de audio, video y otros archivos multimedia) en la World Wide Web (WWW). Tan pronto como un usuario abre su navegador, usa HTTP indirectamente. HTTP es un protocolo de aplicación que se ejecuta en el conjunto de protocolos de red TCP/IP (los protocolos básicos de Internet). El protocolo HTTP generalmente usa el puerto 80. El protocolo RTP se usa para transportar los datos de voz en tiempo real (igual que para el protocolo H. 323, mientras que el protocolo SDP se usa para la negociación de las capacidades de los participantes, tipo de codificación, etc.) La mayoría de los sitios de streaming utiliza capas TCP/IP (protocolo de control de transmisión/Internet) estándar en lugar de UDP (protocolo de datagramas de usuario) para transmitir contenido de un servidor a un dispositivo.
POSIBLES AFECTACIONES EN CASO DE NO APLICARSE	**A LA RED.** Calidad de servicio (QoS) es un conjunto de tecnologías que permite que las aplicaciones soliciten y reciban niveles de servicio predecibles en términos de la capacidad de rendimiento de datos (ancho de banda), variaciones de latencia (fluctuación) y retraso. ¿Qué pasa si no priorizamos el tráfico? Si hay varias aplicaciones que consumen una gran cantidad de ancho de banda ejecutándose al mismo tiempo en la red, se genera una congestión debido a que el volumen de tráfico es mucho más alto del que realmente puede manejar. Cuando se produce una congestión, el tráfico se interrumpe, lo que podría dar lugar a la pérdida de datos y la red podría colapsar. **AL USUARIO FINAL O EN SU SUS COMUNICACIONES.** Retardo en la navegación: Degradación generalizada en la navegación del usuario en escenarios de congestión en los que todo el tráfico se vería afectado pues se atendería con la misma prioridad.

	Monopolización de tráfico; algunas aplicaciones tomaran más ancho de banda que otras, afectando a las que realmente tiene más importancia.

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(cortafuegos), 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 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.
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 que el tiempo de impacto sea mínimo.

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

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	24 de marzo del 2023
Versión	**1.0**
Elaboró	**EVERARDO VIDAL HERNÁNDEZ**