

CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE RED

2023

ENEREIDA NATALY FIGUEROA JIMENEZ

TECNO-COM



tecn
com
INTERNET A TÚ ALCANCE

CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE RED

OBJETIVO

El presente Código de Políticas de Gestión de Tráfico y Administración de Red tiene como objetivo principal informar a los usuarios finales del servicio de acceso a Internet provisto por *ENEREIDA NATALY FIGUEROA JIMENEZ (en adelante "TECNO-COM")* sobre los principios de neutralidad de la red, así como el conjunto de actividades, técnicas y procedimientos que se utilizan 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 objetivo es 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, así como los demás principios aplicables en materia de neutralidad de la red.

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 *TECNO-COM* 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.

El Código de Políticas de Gestión de Tráfico y Administración de Red regulados por el artículo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión, y el artículo 12 de los

Lineamientos para la Gestión de Tráfico y Administración de Red emitidos por el Instituto Federal de Telecomunicaciones (Instituto) por medio del Acuerdo P/IFT/EXT/280621/13.

JUSTIFICACIÓN

TECNO-COM es titular de una autorización para establecer y operar o explotar una comercializadora de servicio de telecomunicaciones 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).

TECNO-COM 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 bloquee 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 autorizado 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 JESÚS MANUEL BEAS PERALTA. 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.

El usuario final podrá recibir asesoría y atención mediante el número telefónico *3223994792* asimismo podrá enviar sus preguntas al correo electrónico contacto@tecno-com.net 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 <https://tecno-com.net/>.

DERECHOS DE LOS USUARIOS

- I. **LIBRE ELECCIÓN.** Los usuarios finales del Servicio de Acceso a Internet de *TECNO-COM* podrán 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. TECNO-COM no podrá limitar 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, reuniendo las condiciones técnicas necesarias para poder acceder al servicio, aplicación o contenido deseado, que sea ofrecido en Internet. Lo anterior, conforme a los términos, condiciones y estructuras tarifarias contenidas en las ofertas inscritas en el Instituto (Instituto Federal de Telecomunicaciones).
- 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, el cual puede ser consultado en <https://tecno-com.net/>

- IV. **TRANSPARENCIA E INFORMACIÓN.** *TECNO-COM* publica y actualiza 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, relacionadas con cuestiones que pueden ser consultadas en el Código de Prácticas comerciales.
- 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

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 *TECNO-COM*, 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 de la red. 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.

A continuación, se explicarán cada una de las políticas de gestión y administración de tráfico que *TECNO-COM* 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	<p><u>A LA RED.</u> 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.</p> <hr/> <p><u>AL USUARIO FINAL O EN SU SUS COMUNICACIONES.</u> No tendría afectación en su servicio, sin embargo, si pudiese repercutir a terceros usuarios que se encuentren consumiendo sus datos disponibles y, de aparecer congestiones en la red, recientan disminución en su velocidad de datos contratados.</p>

GESTIÓN DE CONGESTIÓN / OPTIMIZACIÓN DE TRÁFICO	
CONCEPTO	Consiste en la implementación de controles de congestión en ciertas partes de la red, derivadas

		<p>dichas implementaciones ante cambios inesperados en el entorno de la red.</p> <p>El proveedor garantiza la calidad del Servicio, una tasa de transmisión ascendente de por lo menos 1 Mbps en el borde de la cobertura exterior durante hora pico.</p>
CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.		<p>Los casos más comunes donde se aplicará los controles de congestión serían los siguientes:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
IMPACTO EN EL SERVICIO INTERNET USUARIO FINAL.	EN EL DE AL	<p>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.</p>
POSIBLES AFECTACIONES EN CASO DE APLICARSE	EN NO	<p><u>A LA RED.</u></p> <p>De no aplicarse, la red colapsaría debido a la expansión de la congestión de datos a la totalidad de las secciones de dicha red.</p> <p><u>AL USUARIO FINAL O EN SU SUS COMUNICACIONES.</u></p> <p>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.</p>

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.	<p>Los casos en los que se aplicaría esta técnica serían los siguientes:</p> <ul style="list-style-type: none"> • 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	<p><u>A LA RED.</u> 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.</p> <p><u>AL USUARIO FINAL O EN SU SUS COMUNICACIONES.</u> De no bloquearse contenido que afecten la integridad y seguridad de la red o que sean señalados como ilícitos, existe una gran posibilidad</p>

	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.	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	<p><u>A LA RED.</u> Posibles acontecimientos de congestión en partes de la red así de la deficiencia en el tráfico de datos.</p> <hr/> <p><u>AL USUARIO FINAL O EN SU SUS COMUNICACIONES.</u> 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.</p>

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.

CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.	<p>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).</p> <p>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.</p>
IMPACTO EN EL SERVICIO DE INTERNET DEL USUARIO FINAL.	<p>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.</p>
POSIBLES AFECTACIONES EN CASO DE NO APLICARSE	<p><u>A LA RED.</u></p> <p>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.</p> <p><u>AL USUARIO FINAL O EN SU SUS COMUNICACIONES.</u></p> <p>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.</p>

POLÍTICA DE ENRUTAMIENTO	
CONCEPTO	<p>La administración del tráfico en la red de IENTC Telecomunicaciones se hace mediante equipos enrutadores, consistente en una red IP (protocolo de Internet) que utiliza los diversos protocolos para proporcionar mayor seguridad. Los routers guían y dirigen los datos de red mediante paquetes y priorizan los datos y eligen la mejor ruta para cada transmisión.</p>
CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.	<p>Se aplica en casos donde garantiza utilizar la mejor ruta a los destinos de internet, actuando de forma</p>

	automática, para evitar pérdidas del servicio cuando se presentan eventos que pudieran afectarlas.
POSIBLES AFECTACIONES EN CASO DE NO APLICARSE	<p><u>A LA RED.</u> 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.</p> <p><u>AL USUARIO FINAL O EN SU SUS COMUNICACIONES.</u> 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.</p>

RECOMENDACIONES DE USO

TECNO-COM 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.

1. Utilizar un navegador seguro. Asegúrese que los equipos a través de los que accede al Servicio, cuenten con un programa (web browser o navegador) que brinde protección al navegar en Internet, el cual incluya un antivirus actualizado a fin de prevenir ataques de programas maliciosos (Malwares) que puedan afectar al equipo o bien, sustraer información personal y/o confidencial; así como herramientas para prevenir anuncios no deseados (Adware); accesos no deseados o conexiones en segundo plano (Backdoor); seguimiento y almacenamiento de contraseñas, tecleo o información de tarjetas de crédito (Keylogger, Password Sniffing); obtención de información personal y/o confidencial (Phishing), entre otros. Mientras más completa sea la solución que adquieras, mayor será su nivel de protección.
2. 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).

3. Manten 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.
4. 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.
5. Actualiza tus 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.
6. Instalar un Firewall. El Firewall, también conocido como Cortafuegos es una herramienta que protege al dispositivo utilizado para navegar en Internet y se encarga de bloquear los accesos no autorizados a nuestra red; son fáciles de descargar e instalar y existen varias opciones para todos los sistemas operativos.
7. 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.
8. Configurar el control parental: Instalar y utilizar herramientas de control parental para monitorear y controlar las actividades de los menores de edad cuando hagan uso de Internet y procurar sensibilizarlos acerca de los riesgos a los que se pueden enfrentar en Internet.

-
9. 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.
 10. Crear usuarios distintos: En caso de que varias personas utilicen el mismo dispositivo para navegar en la web, se recomienda que cada una cuente con un usuario y contraseña para ello, lo que brindará mayor seguridad para el tratamiento de datos personales y uso de archivos.
 11. Cierra sesión: Finalizar la sesión de las cuentas o perfiles cuando no estén siendo utilizados y antes de apagar los dispositivos; fomentará la protección de tu privacidad, en especial si se accede desde dispositivos públicos.
 12. Cuidar los permisos en las aplicaciones: Al instalar aplicaciones en los dispositivos, algunas aplicaciones solicitan 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.
 13. Realiza descargas solo 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.

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

MAYO, 2023.

Versión

PRIMERA

Elaboró

TECNO-COM

