

CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE RED

CONTENIDO

JUSTIFICACIÓN	2
DEFINICIONES	3
MARCO LEGAL.....	4
DERECHOS DE LOS USUARIOS FINALES DEL SERVICIO DE ACCESO A INTERNET	5
POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE LA RED	6
RECOMENDACIONES PARA EL USUARIO	10

JUSTIFICACIÓN

SRITELECOM S.A DE C.V (En adelante “SRITELECOM” emite el presente documento como sujeto obligado de los Lineamientos en virtud de que presta, a través de redes públicas de telecomunicaciones, el servicio de acceso a Internet al usuario final,

De conformidad con el Título Quinto "De las Redes y los Servicios de Telecomunicaciones", Capítulo VI "De la Neutralidad de las Redes", de la LFTR, establece en el artículo 145 que 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, para lo cual deberán sujetarse a los lineamientos de carácter general que al efecto expida el Instituto conforme a los principios de libre elección, no discriminación, privacidad, transparencia e información, calidad y desarrollo sostenido de la infraestructura.

Por su parte, el artículo 146 de la LFTR prevé que los concesionarios y autorizados, al prestar el servicio de acceso a Internet, deben respetar la capacidad, velocidad y calidad contratadas por los usuarios finales, con independencia del contenido, origen, destino, terminal, aplicación, así como de los servicios que se provean a través de Internet en cumplimiento de lo dispuesto en el artículo 145 de la misma LFTR.

El objetivo es dar a conocer los principios bajo los cuales implementarán la gestión de tráfico y administración de red a que refieren los lineamientos. Para ello, “NOMBRE COMERCIAL” publicará en www.sritelecom.com.mx el código de políticas de gestión de tráfico y administración de red, así como en el centro de atención a clientes ubicado en Blvd a villas 2766 , Col Villas de Irapuato, Irapuato Gto., CP 36670.

DEFINICIONES

Término	Definición
Administración de red	Conjunto de actividades, métodos, procedimientos y herramientas utilizadas por los proveedores del servicio de acceso a Internet, para la operación y el aprovechamiento de los recursos y capacidades de una red pública de telecomunicaciones.
Gestión de tráfico	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.
PACS	Proveedor de aplicaciones, contenidos y/o servicios.
PSI	Proveedor del servicio de acceso a Internet.
Servicio de acceso a Internet	Servicio público de telecomunicaciones que provee conectividad a Internet a los usuarios finales para que accedan a los contenidos, aplicaciones o/y servicios disponibles en Internet, mediante el intercambio, la carga y descarga de tráfico bajo el protocolo de comunicación de Internet IP.

MARCO LEGAL

- Constitución Política de los Estados Unidos Mexicanos.
- Ley Federal de Telecomunicaciones y Radiodifusión.
- 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.

DERECHOS DE LOS USUARIOS FINALES DEL SERVICIO DE ACCESO A INTERNET

De conformidad con lo establecido en la Ley Federal de Telecomunicaciones y Radiodifusión, los derechos de los usuarios finales son los siguientes:

Artículo 145. Los concesionarios y autorizados que presten el servicio de acceso a Internet deberán sujetarse a los lineamientos de carácter general que al efecto expida el Instituto conforme a lo siguiente:

I. Libre elección. Los usuarios de los servicios de acceso a Internet podrán 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. No podrán 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;

II. No discriminación. Los concesionarios y los autorizados a comercializar que presten el servicio de acceso a Internet se abstendrán de obstruir, interferir, inspeccionar, filtrar o discriminar contenidos, aplicaciones o servicio;

III. Privacidad. Deberán preservar la privacidad de los usuarios y la seguridad de la red;

IV. Transparencia e información. Deberán publicar en su página de Internet la información relativa a 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;

V. Gestión de tráfico. 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;

VI. Calidad. Deberán preservar los niveles mínimos de calidad que al efecto se establezcan en los lineamientos respectivos, y

VII. Desarrollo sostenido de la infraestructura. En los lineamientos respectivos el Instituto deberá fomentar el crecimiento sostenido de la infraestructura de telecomunicaciones.

En armonía con lo dispuesto por los Lineamientos, que establecen:

Artículo 4. Las políticas de gestión de tráfico y administración de red que implementen los PSI deberán asegurar:

- I. La libre elección de los usuarios finales para acceder a los contenidos, aplicaciones y servicios en Internet, sin que los PSI dificulten, limiten, degraden, restrinjan o discriminen el acceso a los mismos;
- II. El trato no discriminatorio a los usuarios finales, PACS, tipos de tráfico similares, así como al tráfico propio y el de terceros que curse por la red;
- III. La privacidad de los usuarios finales;
- IV. La inviolabilidad de las comunicaciones privadas de los usuarios finales.

En la implementación de políticas de gestión de tráfico y administración de red, bajo ningún supuesto, los PSI podrán inspeccionar, monitorear o alterar el contenido específico del tráfico que curse por su red.

POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE LA RED

Los lineamientos disponen que la administración de red considera el conjunto de actividades, métodos, procedimientos y herramientas que utilizan los PSI para la operación y aprovechamiento de los recursos y capacidades de la red pública de telecomunicaciones. Por su parte, la gestión de tráfico se conforma por el conjunto de técnicas empleadas por los PSI para el manejo, tratamiento y procesamiento del tráfico cursado por la red. En este sentido, como ha sido mencionado, 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.

POLÍTICA	TOPE DE DATOS	GESTIÓN DE CONGESTIÓN	PRIORIZACIÓN POR TIPOS DE DATOS	BLOQUEO
¿En qué consiste?	Se fija un tope de datos, de acuerdo a las condiciones contratadas por el usuario final, que impide el paso de paquetes de datos una vez que el usuario haya alcanzado su límite.	Esta técnica consiste en ralentizar la velocidad de transmisión a efecto de balancear el tráfico de una sección de la red a fin de descongestionarla, esto sin afectar directamente a un contenido, servicio o aplicación en específico.	Consiste en dar prioridad a la transmisión de ciertos tipos de datos frente a otros.	Técnica que impide el acceso de los usuarios finales a un sitio web determinado o la utilización de un tipo de contenido o servicio particular, ya sea de manera temporal o permanente.
¿En qué casos y para qué se utiliza?	Se aplica cuando el usuario final rebasa el límite de datos ofrecidos por el proveedor.	ante una congestión derivada de las fluctuaciones diarias o cambios inesperados en el entorno de la red.	Se utiliza para mejorar la transmisión de los datos sin degradar la calidad del servicio.	En casos excepcionales asociados a mitigar riesgos de determinados eventos adversos
Impactos de su implementación	El usuario no tendrá acceso a internet una vez agotado su	Posible reducción a la velocidad del servicio de acceso a internet	El usuario tendrá mayor fluidez de tráfico de datos en ciertas	Quita el control de los contenidos a los usuarios y lo detenta el PSI.

	paquete a menos que renueve o contrate un paquete adicional.	contratado por el usuario final, aunque dicho impacto será de manera temporal e inmediato.	características del contenido, aplicación o servicio que quiera acceder a internet.	
Posibles afectaciones a la red en caso de no aplicarse	Afectación al tráfico fluido dentro de la red, debido a una posible congestión y/o saturación de tráfico de datos.	No se podría reaccionar a la congestión de red para reducir al mínimo su intensidad, propagación y duración.	No se permitiría establecer funciones de balanceo del tráfico, eficiencia en el funcionamiento de la red y soluciones de seguridad.	la principal característica de esta técnica no es un impacto en la calidad del servicio que recibe, sino en el acceso restringido a ciertos contenidos. a fin de garantizar la continuidad del funcionamiento de la red o la seguridad de los usuarios y de sus equipos.

Por otra parte, debe observarse que, al implementar la gestión de tráfico y administración de red, los PSI pueden verse sujetos a 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:

- 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.
- 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 PSI ante una congestión temporal o excepcional no podrán implicar que exista discriminación entre tipos de tráfico similares.
- 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 del PSI. 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, sin perjuicio de las obligaciones que deban cumplir los PSI respecto a otras disposiciones.

RECOMENDACIONES PARA EL USUARIO

SRITELECOM 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. **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.
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.

Versión	PRIMERA
Fecha de última actualización	DICIEMBRE 2024