

Código de políticas de gestión de tráfico y administración de red

En atención al ACUERDO MEDIANTE EL CUAL EL PLENO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES EXPIDE 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, se emite la presente Política de Gestión de Tráfico y Administración De Red, para los efectos correspondientes:

Los Lineamientos plantean contribuir en:

- I. Garantizar que el usuario final tenga libertad de decisión sobre los contenidos, aplicaciones y servicios a los que accederá a través del servicio de acceso a Internet, así como conocimiento de la forma en que se gestiona su tráfico y se administra la red otorgar certidumbre jurídica a la industria en materia de neutralidad de red, dando claridad sobre las políticas de gestión de tráfico y administración de red permitidas, así como respecto de los servicios y ofertas que podrán poner a disposición de los usuarios finales
- II. Fomentar la innovación del sector mediante el uso de tecnologías más eficientes en el uso de las redes;
- III. Favorecer la disminución de la brecha digital, a través de ofertas comerciales con objetivos específicos;
- IV. Promover condiciones de competencia y libre concurrencia, y
- V. Incentivar la inversión en redes para la provisión de acceso a Internet fijo y móvil con mayor calidad y más cobertura.

Definiciones.

- **Política de administración de red:** conjunto de actividades, métodos, procedimientos y herramientas utilizadas por el proveedor del servicio de acceso a Internet, para la operación y el aprovechamiento de los recursos y capacidades de su red pública de telecomunicaciones;
- **Política de gestión de tráfico:** conjunto de técnicas utilizadas por el proveedor del servicio de acceso a Internet para el manejo, tratamiento y procesamiento del flujo de tráfico cursado por su red pública de telecomunicaciones;
- **Proveedor de aplicaciones, contenidos y/o servicios o PACS:** persona física o moral que proporciona a los usuarios finales, aplicaciones, contenidos, y/o servicios en Internet;
- **Proveedor del servicio de acceso a Internet o PSI:** aquellos concesionarios y autorizados que proporcionan a los usuarios finales el servicio de acceso a Internet, a través de una red pública de telecomunicaciones, y
- **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 y servicios disponibles en Internet, mediante el intercambio, la carga y descarga de tráfico bajo el protocolo de comunicación de Internet IP.

Gestión de Tráfico y Administración de Red

La administración de red considera el conjunto de actividades, métodos, procedimientos y herramientas que se utilizan 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 para el manejo, tratamiento y procesamiento del tráfico cursado por la red. En este sentido, 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

Al respecto, por este medio se comunica e informa a nuestros usuarios finales, que para la prestación del servicio de Acceso a Internet:

- I. Se asegura la calidad, capacidad y velocidad del servicio de acceso a Internet contratado por los usuarios finales, y
- II. Se preserva la integridad y seguridad de la red.

Nuestras políticas de gestión de tráfico y administración de red brindan y/u ofrecen lo siguiente:

- I. *La libre elección* de los usuarios finales para acceder a los contenidos, aplicaciones y servicios en Internet, sin que se 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, no se inspecciona, monitorea o altera el contenido específico del tráfico que curse por su red.

No se implementa políticas de gestión de tráfico y administración de red que resulten en la limitación, degradación, restricción, discriminación, obstrucción, interferencia, filtrado o bloqueo del acceso a contenidos, aplicaciones o servicios a los usuarios finales, salvo que se realicen de manera temporal y únicamente en aquellos casos en que se presente alguna de las siguientes situaciones:

- I. Riesgo, técnicamente comprobable, a la integridad y seguridad de la red, a la privacidad de los usuarios finales o a la inviolabilidad de sus comunicaciones privadas;
- II. Congestión excepcional y temporal de la red, sujeto a que no exista discriminación entre tipos de tráfico similares, y

III. Situaciones de emergencia y desastres que pongan en riesgo la operación de la red.

Se respeta el derecho de los usuarios finales a incorporar o utilizar cualquier clase de instrumentos, dispositivos, aparatos o equipos terminales que se conecten más allá del punto de conexión terminal de una red pública de telecomunicaciones, siempre y cuando estos se encuentren homologados, y en cumplimiento de la normatividad aplicable. Adicionalmente, no se limita cualesquiera de las funcionalidades o sistemas de operación de los referidos instrumentos, dispositivos, aparatos o equipos terminales.

No discriminación y neutralidad

En la prestación del servicio de acceso a Internet no inspecciona, filtra o discrimina los contenidos, no obstruye, no interfiere y no bloquea, información, contenidos, aplicaciones o servicios; 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).

Transparencia e información

Se proporciona información de sus ofertas de servicio de manera clara, transparente, adecuada y actualizada, a través de las ofertas comerciales públicas y disponibles en su portal, permitiendo al cliente tomar una decisión informada sobre las diferentes alternativas disponibles en el mercado.

Código de Políticas de Gestión de Tráfico y Administración de Red

El presente documento tiene como finalidad informar a los usuarios del servicio de acceso a Internet (el “CLIENTE”) provisto por nuestra empresa. (El “Proveedor” o “ISP”) SERVICIOS TECNOLOGICOS DE INTERNET S.A DE C.V. (PRONET), los principios de Neutralidad de Red establecidos en la Ley Federal de Telecomunicaciones y Radiodifusión, y en 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 (“Políticas” y/o “Lineamientos”) emitidos por el Instituto Federal de Telecomunicaciones (“IFT” o “Instituto”) mediante el Acuerdo P/IFT/EXT/280621/13, conforme a lo siguiente:

1. Derechos de los usuarios.

1.1 Libre elección. Los usuarios del Servicio podrán acceder (según lo contratado) a cualquier contenido, aplicación o servicio ofrecido por el ISP, sin limitar, degradar, restringir o discriminar el acceso a los mismos, ni bloquear funcionalidad alguna de los equipos. Igualmente, los usuarios podrán utilizar el Servicio mediante el dispositivo de su elección siempre y cuando el mismo se encuentre homologado, según se

especifica en el Código de Prácticas Comerciales. Lo anterior, no implica que cualquier equipo que el usuario pretenda utilizar, reúna las condiciones técnicas necesarias para el Servicio o poder acceder a un contenido, servicio o aplicación específico, ofrecido en Internet. Es responsabilidad del usuario validar que el equipo que pretenda utilizar cumpla con la normativa aplicable y cuente con las características técnicas necesarias.

1.2 No discriminación. El ISP se obliga a no obstruir, interferir, inspeccionar, filtrar o discriminar cualquier tipo de contenidos o servicios.

1.3 Privacidad. El ISP preserva la privacidad de los usuarios y la seguridad de la red. Para más información, consulta el Aviso de Privacidad.

1.4 Transparencia e información. Las características del Servicio, incluyendo las Políticas, velocidad, calidad, así como la naturaleza y garantía de éste, pueden ser consultados en nuestro Código de Prácticas Comerciales.

1.5 Gestión de tráfico. El ISP podrá tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red conforme a las políticas autorizadas por el Instituto y disposiciones aplicables, para garantizar la calidad o la velocidad de Servicio contratado por el usuario, siempre que ello no constituya una práctica contraria a la sana competencia y libre competencia.

1.6 Calidad. El acceso al Servicio se prestará de acuerdo con los niveles mínimos de calidad ofrecidos con base en la regulación aplicable en la materia.

1.7 Desarrollo sostenido de la infraestructura. El Instituto debe fomentar el crecimiento sostenido de la infraestructura de telecomunicaciones, con lo cual se promoverá un funcionamiento más eficiente y competitivo en el mercado de las telecomunicaciones.

2. Políticas de Gestión de Tráfico y Administración de Red. A continuación, se detallan las Políticas que utilizará el ISP para la eficiente prestación del Servicio, consistentes en:

2.1 Optimización del Tráfico. Son acciones que realiza el ISP con el objeto de mejorar la experiencia de navegación del usuario, (por ejemplo: la administración del tráfico o, gestión de ancho de bandas de los medios, entre otros) las cuales se traducen en un uso más eficiente de la red. La implementación de ese tipo de medidas por el ISP en el Servicio repercutirá en un mayor nivel de calidad del Servicio. Además, beneficiará la operación de la red, ya que disminuirá la posibilidad de escenarios de congestión de tráfico, altas latencias y altos costos

operativos en la red. La percepción del usuario derivado de la implementación de las medidas mencionadas pudiera generar que los tiempos de respuesta en el acceso y/o descargas de contenidos se mantenga o disminuya, y con ello, los usuarios pudieran experimentar una mejora en la navegación.

2.2 Administración de las Direcciones IP. Una dirección IP es una dirección única que identifica a un dispositivo en Internet o en una red local; es un identificador que permite el intercambio de información en Internet. Las direcciones IP son asignadas por el organismo internacional, Internet Assigned Numbers Authority, quien administra dichas direcciones de manera eficiente para permitir el acceso a Internet de todos los usuarios a nivel global de manera equitativa. Toda vez que se trata de insumos finitos, la administración de direcciones IP, se realiza de la siguiente manera:

- a. Asignación dinámica y compartida de las direcciones IP “públicas” de los tipos IPv4 e IPv6 para todos los usuarios del Servicio, lo que implica que una misma dirección puede ser compartida para una multiplicidad de direcciones IP privadas.
- b. Asignación dinámica o estática de direcciones IP “privadas” son utilizadas para con las que se presta el Servicio.
- c. La navegación en Internet genera lo que se conoce comúnmente como sesiones, las cuales emplean las direcciones IP privadas; el Proveedor podrá gestionar la cantidad de direcciones simultáneas disponibles al usuario.

La implementación de lo anterior generará:

- Ocupación adecuada de las direcciones IP públicas
- Disponibilidad de las direcciones IP públicas.

2.3 Administración de tráfico en casos de congestión. Consiste en que el Proveedor pueda prestar el Servicio considerando las características especiales de cada tipo de tráfico tales como aplicaciones en tiempo real, servicios de IoT y M2M, voz sobre IP y video conferencia de alta calidad, entre otros. El ISP podrá llevar a cabo acciones para la optimización del tráfico en caso de saturación de la red, haciendo uso adecuado de los recursos disponibles en un momento y ubicación determinados. Particularmente, ante situaciones que pudieran comprometer la calidad del Servicio. Al implementarse la prestación del Servicio podría ser (sin intermitencia y baja latencia), entre otros.

2.4 Bloqueo. El bloqueo es la 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. Política de bloqueo de puerto 25 SMTP: Causa: Por existir riesgo a la integridad de la red y a las comunicaciones legítimas de los usuarios finales. Debido a la prevalencia de máquinas que tienen gusanos, virus u otro software malintencionado que genere grandes cantidades de correo electrónico no deseado.

- a) En qué consiste: Bloqueo del puerto 25 (SMTP) del protocolo de transporte TCP.
- b) En qué casos y para qué se utiliza: Se establece este filtrado en la entrega inicial del servicio de acceso a Internet en todos los casos.
- c) Impacto en la experiencia del usuario final: Al intentar utilizar este puerto no obtendrá conexión. El usuario final puede solicitar la apertura de este filtro para efectos de soportar el servicio en el puerto 25.
- d) Afectaciones del usuario final en caso de que no fuera implementada: Afectación al servicio de los clientes que legítimamente usan este puerto, al ser potencialmente incluido en listas negras de correo.

3. Recomendaciones al usuario final. A continuación, se enlista una serie de recomendaciones para realizar una navegación más segura:

- 1)** Programa de Seguridad en Internet: Es valioso asegurarse que los equipos a través de los que accede al Servicio, cuenten con un programa (conocidos como navegadores o web browsers) que brinde protección a l navegar en Internet, el cual incluya un antivirus actualizado a fin de prevenir ataques de programas maliciosos 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)** Evitar navegación en sitios no conocidos: Al navegar en Internet asegúrate de validar que el sitio, servicio, contenido o aplicación visitado/utilizado cuente con certificados de seguridad y sellos de confianza emitidos por auditores y certificadores reconocidos. Recomendamos instalar complementos para navegadores web, así como, revisar las opciones de seguridad y privacidad del navegador que usas.
- 3)** Proporciona información solo cuando estés seguro: Recomendamos no proporcionar datos personales, números de cuenta, tarjetas bancarias, números telefónicos, NIP de seguridad, tokens, 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. De igual forma, te recomendamos no proporcionar ni compartir información sensible (tarjetas de crédito, números confidenciales, contraseñas, pines, tokens, imágenes, fotografías etc.) en Internet que contenga información confidencial.

4) Control parental: Instala y utiliza herramientas de control parental para monitorear y controlar las actividades de los menores de edad cuando hagan uso de Internet. Si tienes menores de edad a tu cargo procura sensibilizarlos acerca de los riesgos a los que se pueden enfrentar en Internet.

5) Actualización frecuente de contraseñas: Se recomienda hacer uso de contraseñas seguras que tengan al menos 8 caracteres. Te sugerimos utilizar una combinación de números, letras mayúsculas, minúsculas y símbolos. Cambia tu contraseña de manera frecuente.

6) 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.

7) Descarga programas informáticos (software) y aplicaciones de sitios oficiales y confiables: Para descargar software y aplicaciones de forma segura, recomendamos lo siguiente:

- a. No modificar la configuración de fábrica de los equipos;
- b. Descarga software y aplicaciones solo de sitios web y tiendas oficiales; y
- c. Verifica los permisos y accesos requeridos por el software o aplicación antes de otorgarlos.

8) Administra el equipo con el que hagas uso del Servicio: Es importante conocer las herramientas que permitan administrar los dispositivos de manera integral. El ISP cuenta con opciones para ayudarte a tener mayor control y seguridad en tu navegación en Internet. Consulta los antivirus y herramientas de control parental disponibles en nuestra página en Internet, así como en los distintos Centros de Atención a Clientes a nivel nacional.

4. Marco legal aplicable.

- 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.

Código emitido conforme a la Ley Federal de Telecomunicaciones y Radiodifusión, así como los “Lineamientos para la gestión de tráfico y administración de red a que se deberán sujetar los concesionarios y autorizados que presten el servicio de acceso a Internet”.