Código de Gestión de Tráfico y Administración de Redes

Contenido

1. Fundamento

Las presentes políticas de gestión de tráfico y administración de redes responden y están en consonancia a las disposiciones contenidas en el Artículo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión, así como a las previsiones 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", publicados en el Diario Oficial de la Federación el 5 de julio de 2021 (en lo sucesivo LINEAMIENTOS).

2. Objetivo

En el marco de la normatividad señalada, el presente Código tiene como función primordial dar a conocer a los usuarios del Servicio de Acceso a Internet (en adelante SERVICIO o SERVICIO DE INTERNET) las políticas de gestión de tráfico y administración de red que pueden ser utilizadas por el proveedor del SERVICIO DE INTERNET (en lo sucesivo PSI) en la prestación del SERVICIO, bajo el principio de Neutralidad de la Red, salvaguardando, en todo momento, la protección al usuario, su libertad de expresión y acceso a la información.

Las políticas implementadas tienen por objetivo ofrecer a los usuarios la mejor experiencia posible del SERVICIO DE INTERNET, según la velocidad contratada, mediante la adopción de mejores prácticas y estándares de la industria, respecto a la administración del ancho de banda y los recursos de la red que, por ser limitados, son materia de protección, en beneficio de los intereses de los clientes, para evitar congestión de tráfico y respetar el ancho de banda contratado por los usuarios.

3. Políticas Generales

El PSI, dentro del ámbito de su correspondencia, se compromete a implementar únicamente aquellas medidas de gestión de tráfico y administración de red que sean razonables y no discriminatorias -respecto de algún proveedor, servicios, contenido o protocolo específico-, siempre consistentes con los mejores estándares de la industria, destinadas al correcto funcionamiento de la red y de la prestación del SERVICIO; en otras palabas, se obliga únicamente a realizar acciones para:

- Reducir o mitigar los efectos de congestión de la red.
- Asegurar la integridad y seguridad de la red.
- Asegurar la seguridad del servicio a los usuarios.
- Proporcionar el SERVICIO de conformidad con las capacidades y/o velocidades contratadas, observando, en todo momento, las mejores prácticas y requisitos técnicos exigidos por la normatividad aplicable.

4. Derechos de los Usuarios

En términos del Artículo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión y al principio de Apertura y Neutralidad de la Red, el SERVICIO DE INTERNET será prestado bajo las siguientes pautas:

4.1 Libre elección

El PSI se compromete a garantizar la libre elección, a fin de que sus usuarios escojan y controlen sus actividades en línea, incluyendo proveedores, servicios y aplicaciones. De esta forma, los suscriptores podrán acceder a cualquier contenido, aplicación o servicio ofrecido por Internet, a través de cualquier equipo terminal homologado, sin que el PSI realice acción alguna para limitar, degradar, restringir o discriminar el acceso a los mismos.

En este sentido, cabe señalar que el PSI aplica el enfoque del "Mejor Esfuerzo" al traslado de datos por redes, mediante el cual se realiza todo lo posible para entregar todos los datos a su destino, en función de la disponibilidad de recursos de la propia red, sin priorizar u ofrecer un tratamiento preferencial a un(os) flujo(s) de datos sobre otros.

De igual manera, es brindada libertad al usuario para elegir cualquier Equipo Terminal y/o incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos, siempre que los mismos se encuentren debidamente homologados; no obstante, se indica que, en ciertos casos, los equipos deberán reunir ciertas condiciones técnicas necesarias para el acceso a Internet y/o al contenido, servicios y/o aplicaciones ofrecidas por distintos proveedores.

4.2 No discriminación

El PSI se obliga a no obstruir, interferir, bloquear, inspeccionar, filtrar o discriminar contenidos, aplicaciones o servicios, parcial o totalmente, incluyendo el tráfico Peer-to-Peer (P2P – Persona-a-Persona), salvo cuando tenga pleno conocimiento sobre que el tráfico es ilegal, ilícito o perjudicial y/o cuándo sea ordenado por autoridad competente.

Asimismo, se consigna que el PSI no restringe los tipos de dispositivos susceptibles de conectar a su red, siempre que estén homologados, de acuerdo con la legislación aplicable, y no afecten la prestación del SERVICIO o a terceros, dañen la red o impliquen una infracción a la política de uso aceptable del mismo.

4.3 Privacidad

El PSI cuenta con un Aviso de Privacidad que detalla los derechos y procedimientos bajo el cual trata datos personales proporcionados por los usuarios para contratar el SERVICIO.

El PSI podrá implementar acciones para bloquear el acceso a determinados contenidos, aplicaciones o servicios, con el propósito de garantizar la privacidad de los suscriptores y la seguridad de la red. Ain menoscabo de lo anterior, resulta necesario aclarar que la privacidad digital en Internet depende, primordialmente, de hábitos y acciones del usuario al utilizar el SERVICIO. Más adelante aparecen algunas recomendaciones para minimizar riesgos a la privacidad y comunicaciones de los suscriptores.

4.4 Transparencia–información a usuarios

La información publicitada, tanto en el Portal de Internet del PSI, como en los establecimientos, ocurre en términos de lo dispuesto en los "Lineamientos Generales para la publicación de información transparente, comparable, adecuada y actualizada relacionada con los servicios de telecomunicaciones", publicados en el Diario Oficial de la Federación el 12 de febrero de 2020.

Así es cabalmente garantizada la transparencia de información, importante para un acceso justo e imparcial a los recursos de Internet, procurando que los usuarios cuenten con la información vigente y completa, previo y durante la prestación del SERVICIO DE INTERNET.

En el caso de la prestación del Servicio de Internet Fijo, no es contemplada cuota alguna de tráfico por un tiempo o capacidad determinada, es decir, el servicio ofrecido es ilimitado, con algunas ofertas diferenciadas, en cuanto a la velocidad de ancho de banda contratada.

Los planes, paquetes, ancho de banda, características comerciales y tarifas vigentes, así como las presente políticas de gestión de tráfico y administración de red están publicadas en la Página de internet del concesionario/autorizado y/o podrán ser consultadas, en todo momento, en el establecimiento del PSI.

4.5 Gestión de tráfico–general

Como fue mencionado, el PSI implementará sólo aquellas prácticas razonables y necesarias, conforme a las mejores prácticas internacionales y/o estándares de la industria, para asegurar la correcta prestación del SERVICIO, garantizar la seguridad e integridad de la red y usuarios, evitar congestiones y cumplir con los niveles de calidad comprometidos y publicitados.

4.6 Calidad

EL PSI procurará realizar todas las gestiones necesarias, con objeto de garantizar oferta de calidad ofrecida, mediante una política de mejora continua y modernización de procesos, a efecto de cumplir con los estándares nacionales e internacionales, instrumentando políticas en cumplimiento de los “Lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores del servicio fijo”, publicados en el Diario Oficial de la Federación el 25 de febrero de 2020, bajo la premisa de mantener la continuidad del SERVICIO, según la factibilidad técnica y física.

4.7 Desarrollo sostenido de infraestructura

EL PSI está comprometido en mantener operativa su red, basándose en la disponibilidad tanto física como técnica, en un proceso de modernización y mejora continuas, en pro, todo momento, de la satisfacción del cliente.

Cabe señalar que, en los Lineamientos respectivos, el Órgano Regulador deberá fomentar el crecimiento sostenido de la infraestructura general de telecomunicaciones.

5. Políticas de Gestión Y Administración de Tráfico

5.1 Bloqueo y filtrado

Entendidas como las acciones tendientes a negar el acceso a usuarios finales de ciertos contenidos en línea.

Sobre el particular y en atención al Principio a la Libre Elección, es pertinente indicar que el PSI no realizará ninguna actividad de filtración selectiva de contenido, aplicaciones y/o servicios, salvo en función de determinados controles reglamentarios, esto es, sólo para proteger o limitar la proliferación de contenidos ilegales u objetables, siempre que medie una orden de autoridad administrativa o judicial competente.

De esta forma, atendiendo a que el SERVICIO DE INTERNET supone riesgos frente acciones deliberadas (e inclusive involuntarias), tanto de terceros, como de los propios usuarios, el PSI podrá realizar, en

circunstancias limitadas, cualquier acción para preservar la seguridad de la red y/o la privacidad de los suscriptores, incluyendo bloquear o filtrar el tráfico perjudicial entrante o saliente, así como el acceso a contenidos, aplicaciones o servicios que sean ilegales o ilícitos, o bien en los casos que medie orden de autoridad administrativa y/o judicial competente.

5.2 Gestión de IP

Entendida como la asignación y rotación de las IP asignadas y la dirección de paquetes a través de éstas.

Al igual que cualquier otro PSI, las direcciones IP son asignadas por terceros, ajenos al control del PSI; en dicho contexto, el primero realiza una asignación dinámica y compartidas de las IP y puede dirigir paquetes a través de rutas de comunicación distinta, a fin de evitar congestión y garantizar el ancho de banda contratado por los usuarios.

5.3 Vías rápidas de internet

Es la práctica de brindar tratamiento preferencial a ciertos flujos de datos.

Al respecto, se hace de su conocimiento que, conforme al Principio de No Discriminación y en términos del enfoque del "Mejor Esfuerzo", el PSI no inspecciona el contenido y, por tanto, tampoco interfiere o da preferencia a determinados datos, información y/o aplicaciones.

5.4 Estrangulamiento

El PSI sólo implementará esta práctica, por la cual se reducen las tasas de transferencia del contenido entregado a los usuarios finales, únicamente para garantizar, específicamente, las velocidades de carga o descarga de los usuarios, según los planes contratados, sin que tenga lugar para discriminar ciertos flujos de datos, proveedores, aplicaciones, entre otros recursos de Internet.

5.5 Monitoreo

La Monitorización se realiza exclusivamente para verificar que no se degrade la calidad del SERVICIO DE INTERNET y para verificar que, efectivamente, sea proporcionado el ancho de banda contratado por los usuarios. La evaluación de la calidad está basada en mediciones, estándares y normas entendidas de manera generalizada.

Al respecto aún y cuando el PSI conduzca sus acciones bajo el enfoque del "Mejor Esfuerzo" para gestionar la red, el crecimiento del acceso a Internet, así como de páginas, plataformas y aplicaciones cada vez más sofisticadas, pueden generar congestión y/o disminuir la velocidad de navegación de forma momentánea. Adicionalmente, existen otros factores que pueden afectar la calidad del servicio y que no dependen directamente del PSI:

- Las conexiones inalámbricas pueden tener un detrimento respecto a la velocidad alcanzada, aunado a que pudieran existir causas adicionales relacionadas (por ejemplo, tecnología y/o equipo terminal utilizados para acceder al SERVICIO DE INTERNET, ubicación del usuario en interiores, interferencias provenientes de otros aparatos eléctricos y electrodomésticos, etc.).
- Características del equipo terminal (Hardware y Software), incluyendo programas y aplicaciones instaladas y en ejecución, etc. Destacando que, en ocasiones, los equipos realizan ciertas gestiones

propias para mejorar la experiencia del usuario en Internet y/o en el uso de aplicaciones, que no son responsabilidad y/o del conocimiento del PSI.

- Caso Fortuito y/o de Fuerza mayor, incluyendo interferencias y daños generados por terceros.
- Eventos que generen un incremento de demanda extraordinaria de servicios de red.
- Características propias del Internet, dado que la capacidad y disponibilidad son limitados.
- Características propias de los servicios, aplicaciones y contenidos en internet, de las cuales el PSI no tiene control.

6. Recomendaciones de Privacidad Digital

En atención a uno de los puntos principales concerniente a la gestión de tráfico y administración de redes, resulta que las acciones de los PSI para garantizar la seguridad y privacidad del usuario acusan limitaciones, ante la priorización de Principio a la Libre Elección, así como el de NO DISCRIMINACIÓN, en el uso de internet, lo que conlleva a la no inspección y no limitación de acceso y flujo de tráfico, salvo por orden judicial o cuando, en limitadas circunstancias, se desprenda que el mismo es perjudicial para la red y/o para los usuarios.

Por lo anterior, la Privacidad Digital depende en gran medida del ámbito de actuación de los usuarios, en tanto que son éstos los que pueden ejercer un control sobre sus datos y, en gran medida, limitar, a discreción, el acceso de terceros, empresas o instituciones a su información privada y de carácter personal.

La Privacidad Digital y Protección de Datos comprende no sólo la información de identificación de cada individuo (nombre, domicilio, teléfono, etc.), sino también imágenes, videos, correo electrónico, geolocalización, historial de navegación, entre otros aspectos, que permiten reconocer a usuarios en la red. Esto resulta relevante para la creación y salvaguarda de la identidad digital que es proyectada y estar en aptitud de garantizar acceso a perfiles con consentimiento controlado, para lograr protección ante fraudes, ciberataques o suplantación de identidad.

A continuación, son descritos algunos consejos para proteger la Privacidad Digital y minimizar los riesgos de intrusión a comunicaciones personales:

6.1 Utilizar y Actualizar el Antivirus y Firewall.

Se recomienda utilizar instrumentos de protección y/o Software que proporcionan los Equipos Terminales y/o terceros, tales como Antivirus y Firewall, que constituyen herramientas adecuadas para combatir malware que vulnera la privacidad en Internet.

6.2 Utilizar Contraseñas Distintas, Seguras y Personales.

En general, la utilización de contraseñas es un método eficaz para garantizar la Privacidad Digital; resulta de mayor seguridad crear distintas para cada aplicación y/o servicio, de manera que la vulneración de una no implique riesgos a los otros.

De igual forma, es imperativo no utilizar contraseñas comunes y/o generales, mucho menos datos personales de fácil determinación, además de nunca compartirlas.

Asimismo, bien convendría utilizar sistemas o programas de cifrado de contraseñas para protegerlas con algoritmos, con la ventaja de que permiten al usuario acceder a diferentes servicios con diferentes contraseñas usando una de carácter maestra designada.

6.3 Evitar Acceder a Enlaces Sospechosos o Abrir Archivos de Procedencia Desconocida.

Se recomienda a los usuarios nunca abrir enlaces y/o documentos enviados por remitentes desconocidos, en otros idiomas y que no sea información de búsqueda específica para el propio interesado y/o que esperaba recibir. Principalmente, en correos electrónicos, la regla sería procurar abrir sólo los de fuentes confiables y conocidas, para evitar la propagación de malware, como virus, troyanos y cualquier tipo de código maliciosos.

6.4 Descarga de Aplicaciones.

La descarga de programas y/o aplicaciones debe ser restringida sólo a sitios oficiales, esto es, a través de la web de un fabricante o licenciatario reconocido y/o a través de tiendas oficiales. De igual manera, reviste gran importancia prestar atención a los permisos otorgados para poder descargar y/o utilizar cierta información, en tanto que, en una gran cantidad de aplicaciones, la configuración inicial trae aparejada la aceptación implícita de ceder datos para fines comerciales o publicitarios e incluso favorecer acceso a información y activación automática de funciones (por ejemplo, geolocalización, encendido de cámaras y micrófonos, entre otra), sin motivo aparente. También, debe considerarse la eliminación de todas aquellas aplicaciones no utilizadas, así como la información depositada en las mismas.

6.5 Conocer el Cumplimiento y las Políticas en Materia de Protección de Datos.

Una recomendación para salvaguardar la privacidad digital consiste en comprobar que las páginas web visitadas cumplan con la normatividad vigente en materia de protección datos –en México, debe ser acatada la Ley Federal de Protección de Datos Personales en Posesión de Particulares, con los llamados Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)– , situación verificable en la Política de Privacidad de cada empresa y la de cookies (ésta última puede ser parte de la Política de Privacidad o bien encontrarse por separado). Así, una vez validado el cumplimiento con la normatividad mencionada, el usuario podrá elegir, con conocimiento de causa, si proporciona datos requeridos por alguna página, así como la conveniencia de continuar navegando por la misma.

Además de verificar las Políticas de Privacidad y Tratamiento de los Datos Personales, el suscriptor debe cuidar a quién proporciona información y la cantidad y variedad objeto de registro. En otras palabras, debe desconfiarse, a manera de proceder general, de aquellas páginas web y/o aplicaciones que soliciten demasiados datos, específicamente los denominados sensibles, sin motivo aparente.

6.6 Conocer y Configurar las Opciones de Privacidad de Servicios, Aplicaciones, Redes Sociales y Equipo Terminal.

En la actualidad, tanto los dispositivos de acceso, como las aplicaciones, redes sociales y demás plataformas accesibles por Internet, donde es compartida información de carácter privado, cuentan con opciones para personalizar y/o configurar perfiles, publicidad, servicios y demás datos relacionados con la privacidad, de

manera que el usuario puede decidir la naturaleza de la información y destinatarios de la misma, así como configurar los anuncios y/o las aplicaciones a las que se acceden a través de plataformas, redes sociales, etc.

De hecho, el uso de las redes sociales implica grandes riesgos para la privacidad digital, en parte, por la cantidad y variedad de información personal que es ingresada por los propios usuarios, sin tomar conciencia de la huella digital generada con antecedentes y datos personales proporcionados, sin caer en cuenta en la merma auto infringida a la propia seguridad.

Por regla, la recomendación principal consiste en evitar la publicación de cualquier información personal, más aún, datos sensibles, que pudieran permitir la localización del usuario y/o una suplantación de identidad. Sin embargo, en reconocimiento del uso global de redes sociales, demás aplicaciones y contenido de Internet, cuando el suscriptor decide compartir cualquier referencia debe estar consciente, en todo momento, del riesgo implícito de hacerlo y de la temporalidad, prácticamente infinita, de permanencia de lo así compartido en el colectivo social virtual.

6.7 Recomendaciones adicionales.

- Dar preferencia a páginas web que ofrecen el sistema de navegación y cifrado SSL (Secure Socket Layer), que garantizan más seguridad al usuario y, de preferencia, evitar las que no aparecen en navegadores confiables de Internet y/o que no fueron referidos por fuente reconocida.
- Utilización de VPN y/o del Modo Incógnito de los Navegadores, herramientas útiles para evitar el registro e intercambio de datos.
- Optar por navegadores con actualizaciones continuas, manteniéndolos siempre al día. Los desarrolladores de los navegadores más conocidos constantemente implementan parches ante cualquier vulneración de seguridad e incluyen las últimas tecnologías de protección. En este sentido, conviene estudiar y aplicar cualquier protección adicional que ofrezcan los navegadores vía su configuración y/o la instalación de ciertos complementos; de igual manera, deben ser eliminados los innecesarios, principalmente los incluidos e instalados sin consentimiento del usuario.
- Configurar los navegadores, en la medida de lo posible, para bloquear ventanas emergentes y las cookies de terceros (por lo menos debe ocurrir lo anterior cuando se navegue en modo privado).
- Evitar redes de wifi abiertas y, principalmente, nunca acceder a cuentas personales desde esas y/o de ordenadores públicos; en caso de tener que hacerlo, asegurarse de cerrar las cesiones y borrar los datos de acceso.
- Generar conciencia de la huella digital generada a través del tiempo por el uso de redes, y, en su caso, realizar acciones para ejercer los Derechos ARCO, respecto a la publicación de cualquier dato personal ya no necesario y/o al que no se otorgó autorización.

7. 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", publicados en el Diario Oficial de la Federación el 5 de julio de 2021.

- "Lineamientos Generales para la publicación de información transparente, comparable, adecuada y actualizada relacionada con los servicios de telecomunicaciones", publicados en el Diario Oficial de la Federación el 12 de febrero de 2020.
- Ley Federal de Protección de Datos Personales en posesión de los Particulares.