

## Código de políticas de gestión de tráfico y administración de red

De conformidad con el artículo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión y con 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, emitidos por el Instituto Federal de Telecomunicaciones, este código establece los criterios y principios a los que se sujetará **StarGo Empresarial** en la prestación del **servicio de acceso a Internet<sup>1</sup> a usuarios empresariales**, mediante su red pública de telecomunicaciones, al implementar la gestión de tráfico y administración de red.

### I. Derechos de los usuarios

Nuestros usuarios gozan de los siguientes derechos:

- a) **Libre elección.** Los usuarios de **StarGo Empresarial** pueden acceder e intercambiar contenido y tráfico de manera abierta por Internet, siempre que los dispositivos y/o aparatos que nuestros usuarios conecten a Internet más allá del punto de conexión terminal de la red se encuentren homologados por el Instituto Federal de Telecomunicaciones y en cumplimiento de la normatividad aplicable.

Los paquetes del servicio de acceso a Internet de **StarGo Empresarial** permiten a los usuarios el acceso total al contenido, aplicaciones o servicios disponibles en internet –dependiendo del plan tarifario contratado–, salvo que algún usuario requiera aplicar ciertas pautas de filtrado, en cuyo caso deberá apegarse a las reglas económicas y operativas vigentes.

---

<sup>1</sup> Definido en la fracción VIII del artículo 2° del 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, publicado en el Diario Oficial de la Federación el 5 de julio de 2021, como el “*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*”.

A network diagram consisting of a grid of interconnected nodes (dots) and lines, representing a network structure, located in the top right corner of the page.

**StarGo Empresarial** no condiciona el acceso al usuario a aplicaciones, servicios o contenidos específicos disponibles en internet, siendo el proveedor de éstos el único responsable de los criterios de acceso. El uso aceptable del servicio de internet supone riesgos y responsabilidades para la seguridad y privacidad de los usuarios cuando buscan, acceden y/o descargan, por ejemplo, contenidos, aplicaciones o servicios ilegales, ilícitos, dañinos con malware, virus informáticos, adware, spyware, phishing, etc.

**StarGo Empresarial** no establece ninguna limitante para el uso de dispositivos o aplicaciones externos al módem satelital, pero el desempeño y/o calidad debe considerar las características operativas del servicio vía satélite -latencia, concurrencia comprometida, entre otros-.

- b) **No discriminación.** En la prestación del servicio de acceso a Internet, **StarGo Empresarial** no inspecciona, filtra o discrimina contenidos, así como tampoco obstruye, interfiere ni bloquea información, contenidos, aplicaciones o servicios.
- c) **Privacidad.** En ningún caso, la información que se cursa por medio de la plataforma satelital es inspeccionada, monitoreada ni alterada, asegurando así la integridad de la información cursada. Ello se complementa con el uso de algoritmos de encriptación que se utilizan como parte de la operación de la plataforma satelital de **StarGo Empresarial** para asegurar la privacidad de la información de los usuarios.

El servicio de acceso a Internet se provee manteniendo la privacidad de los usuarios. En el Aviso de Privacidad de **StarGo Empresarial**, nuestros usuarios pueden conocer el procedimiento bajo el cual es tratada su información personal, de conformidad con la normatividad aplicable.

- d) **Seguridad.** **StarGo Empresarial** podrá bloquear el acceso a determinados contenidos, aplicaciones o servicios con el fin de preservar la privacidad de sus usuarios, la seguridad de la red, así como para prevenir la comisión de delitos. Asimismo, **StarGo Empresarial** podrá bloquear el acceso a contenidos, aplicaciones o servicios ofrecidos en Internet, a petición expresa de sus usuarios, cuando exista orden de autoridad competente o sean contrarios a la normatividad aplicable.



- e) **Transparencia e información.** En la página de internet de **StarGo Empresarial** nuestros usuarios encontrarán la información relativa a las características del servicio ofrecido, por ejemplo, su velocidad e índices de calidad, con la finalidad de que tomen una decisión informada sobre las diferentes alternativas disponibles en el mercado.
- f) **Calidad.** **StarGo Empresarial** preservará en beneficio de sus usuarios los índices de calidad establecidos en los Lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores del servicio fijo emitidos por el Instituto Federal de Telecomunicaciones.

## II. Políticas de gestión de tráfico y administración de red

El servicio de acceso a Internet por medio de enlaces satelitales tiene características muy particulares, tales como el tiempo que toma a las señales recorrer el trayecto Terminal Remota- Satélite-Gateway -latencia-, la imposibilidad de incrementar la capacidad definida en el satélite utilizado, los riesgos de seguridad latentes, entre otros, por lo cual **StarGo Empresarial** debe aplicar las políticas de gestión de tráfico y administración de la red que se describen a continuación:

### A) Bloqueo de conexiones Peer-to-Peer

Las conexiones Peer to Peer -P2P- tienen una arquitectura destinada a la comunicación entre aplicaciones uno a uno, lo que permite a las personas o a los dispositivos compartir información y archivos de uno a otro sin necesidad de intermediarios. Esas conexiones se utilizan primordialmente para intercambiar contenidos o archivos que violan los derechos de propiedad intelectual y derechos de autor, por ejemplo, series, películas, música, videojuegos, además de que son una fuente importante de malware, razón por lo cual son bloqueadas en el Gateway de **StarGo Empresarial** a todos los usuarios, ya que ello permite reducir el riesgo de comprometer la integridad de la información de los usuarios y de terceros, así como los reclamos legales de los tenedores de los referidos derechos.

Al tener activa esta política, los usuarios **NO** tendrán acceso a conexiones P2P, excepto si el usuario presenta una solicitud de liberación por escrito a **StarGo Empresarial** con la debida argumentación para que esas conexiones sean habilitadas.



## **B) Regulación en la resolución de las aplicaciones de video en Streaming**

Esta política se aplica a todos los usuarios de **StarGo Empresarial** para que reciban una resolución adecuada y, por ende, para que la calidad de video sea razonable, sin alcanzar necesariamente la más alta disponible en el servidor de origen. Dicha acción tiene como objetivo evitar una excesiva demanda de tráfico que pueda comprometer la disponibilidad de servicio para el resto de los usuarios de la plataforma.

## **III. Recomendaciones para el usuario**

Algunas de las medidas que pueden adoptar los usuarios para minimizar riesgos en sus conexiones y su privacidad en las comunicaciones son las siguientes:

- No abrir ni responder mensajes o correos electrónicos de remitentes desconocidos que requieran datos personales.
- Utilizar herramientas para verificar la autenticidad de los correos electrónicos.
- Brindar datos personales solo en sitios de confianza.
- Verificar los enlaces antes de dar clic en ellos.
- Evitar dar clic a ligas que no se conocen, que se vean sospechosas o que no fueron solicitadas.
- Usar un navegador seguro y actualizarlo constantemente.
- Cerrar siempre las sesiones de cuentas personales y redes sociales.
- No aceptar en redes sociales invitaciones de desconocidos.
- Acceder directamente a los sitios de confianza para hacer búsquedas desde ellos.
- Verificar que, al navegar por internet, los sitios sean de confianza: la URL de esos sitios debe comenzar con "https".
- No descargar archivos de fuentes no fiables.
- Leer y, en su caso, aceptar los acuerdos de licencia para el usuario final.
- Navegar en sitios seguros.
- Entrar directamente a las páginas de los bancos y nunca desde las ligas de un mensaje.
- Aprovechar las opciones de seguridad integradas en los dispositivos móviles.
- Conocer todos los detalles de los dispositivos personales para prevenir ataques.
- No utilizar software sin licencia.
- Ocultar los datos de navegación haciendo uso de servidores proxy.



- Utilizar contraseñas seguras que no se repitan y que combinen letras, números y hasta símbolos.
- Utilizar un antivirus actualizado y protector de phishing en el dispositivo que ocupamos para conectarnos.
- Actualizar constantemente las aplicaciones y/o el sistema operativo de los dispositivos personales.
- No proporcionar datos sensibles en redes sociales o por correo electrónico.

#### **IV. Referencias al marco legal aplicable y a los estándares internacionales que dan origen a la gestión de tráfico y administración de nuestras redes**

Este código se apega a los protocolos de TCP/IP estandarizados por la organización internacional IETF –*Internet Engineering Task Force*–, así como a lo dispuesto 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, emitidos por el Instituto Federal de Telecomunicaciones.

En vigor a partir del 6 de septiembre de 2021 (Versión 2)