

# Código de Política de Gestión de Tráfico y Administración de Red para servicios fijos

## Objetivo

Cablemás Telecomunicaciones, S.A. de C.V., Cablevisión, S.A. de C.V., y/o Televisión Internacional, S.A. de C.V. (en adelante “izzi”) hacen del conocimiento a Suscriptores y proveedores del servicio de acceso a Internet fijo provisto por izzi, su Código de Política de Gestión de Tráfico y Administración de Red (en adelante “Código”), el cual tiene como objetivo asegurar la calidad, capacidad y velocidad del servicio de acceso a Internet, así como a preservar la integridad y seguridad de la red, de conformidad con lo establecido en el Artículo 3 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”*, así como los artículos 145 y 146 de la *Ley Federal de Telecomunicaciones y Radiodifusión*.

Mediante el presente Código, izzi informa oportunamente a sus Suscriptores y proveedores de servicio de acceso a Internet acerca de las medidas o acciones implementadas para la gestión de tráfico y administración de red.

## Reglas

El Código de Política de Gestión de Tráfico y Administración de Red implementada, asegura lo siguiente:

### 1. Libre elección

El servicio de acceso a Internet que ofrece izzi permite que los Suscriptores de izzi puedan acceder a cualquier contenido, aplicación o servicios en Internet, sin dificultar, limitar, degradar, restringir o discriminar el acceso a los mismos.

El Suscriptor puede elegir libremente el equipo terminal a través del cual pueda conectarse a la red de pública de telecomunicaciones al contratar el servicio de acceso a Internet, siempre y cuando éstos se encuentren homologados de acuerdo con las Normas Oficiales Mexicanas (NOM) o Normas Mexicanas (NMX) según sea aplicable.

### 2. Trato no discriminatorio

izzi se abstendrá de obstruir, interferir, inspeccionar, filtrar, discriminar o bloquear el acceso a contenidos, aplicaciones o servicios a los Suscriptores, salvo en situaciones de riesgos para la red, la privacidad de los usuarios o sus comunicaciones privadas, esto sólo podrá hacerse de manera temporal. Es decir, los Suscriptores de izzi pueden acceder de manera libre a contenidos, aplicaciones y servicios disponibles en internet.

izzi preservará un trato no discriminatorio entre Suscriptores, proveedores de aplicaciones, contenidos y servicios, tipos de tráfico similares, así como entre el tráfico propio y el de terceros que curse por la red de telecomunicaciones, con independencia del origen o destino de la comunicación. Por lo tanto, no priorizará o dará preferencia a contenidos, aplicaciones y/o servicios específicos.

### 3. Privacidad y seguridad de las comunicaciones

izzi garantizará la privacidad de los Suscriptores y la inviolabilidad de sus comunicaciones privadas, por lo que de ninguna manera podrá inspeccionar, monitorear o alterar el contenido específico del tráfico que transita por su red ni hacerse de información de los Suscriptores que no sea necesaria para proveerles el servicio. Salvo casos de solicitud expresa por parte de la autoridad competente.

#### 4. Transparencia e información

izzi publica en su página de internet la información relativa a las características del servicio, incluyendo las políticas, velocidad, calidad, así como la naturaleza y garantía de éste.

#### 5. Gestión de tráfico

izzi tomara las medidas o acciones necesarias para la gestión de tráfico y administración de red conforme a las disposiciones vigentes, 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; izzi podrá realizar manejo de congestión de datos en caso de fallas en la red (propias o generadas por terceros) por el tiempo estrictamente necesario que requiera para atender la contingencia que en su caso se presente.

izzi podrá realizar prácticas de bloqueo de manera temporal para impedir el acceso de los Suscriptores a un sitio web determinado (o desviar ese tráfico) cuando éstos causen riesgo a la integridad de la red y a las comunicaciones legítimas de los Suscriptores, que contengan gusanos, virus u otro software malintencionado que genere afectaciones en la red, en los servicios, o en las condiciones de seguridad en la red. Esto debido a que, de no llevar a cabo esta práctica, se podría poner en riesgo las condiciones de seguridad de la red y las comunicaciones legítimas de los Suscriptores.

Asimismo, izzi podrá realizar el bloqueo para impedir el acceso de los Suscriptores a un sitio web determinado, cuando reciba una orden de alguna autoridad competente debidamente facultada para ello en términos de la legislación vigente en México. Esto en tanto subsistan los efectos legales de la orden correspondiente.

Adicionalmente, izzi podrá realizar el bloqueo de la conexión a Internet a Suscriptores que presenten algún comportamiento que amenace la integridad de la red y el uso adecuado del servicio de otros clientes de acuerdo con lo establecido en el contrato de prestación de servicios y la Política de Uso Aceptables publicadas en su página web. Asimismo, podrá llevar a cabo tales acciones si fuera requerido por la autoridad competente.

#### 6. Calidad

izzi preserva los niveles mínimos de calidad establecidos en los *“Lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores del servicio fijo”*.

#### 7. Desarrollo sostenido de la infraestructura

El Instituto Federal de Telecomunicaciones debe fomentar el crecimiento sostenido de la infraestructura de telecomunicaciones.

#### 8. Recomendaciones al usuario final

- Utiliza equipos terminales debidamente homologados de acuerdo con las Normas Oficiales Mexicanas (NOM) o Normas Mexicanas (NMX) según sea aplicable y con software legítimo y autorizado por el titular de los derechos de este.
- Visita solamente sitios seguros. Asegúrate que los sitios que visitas sean oficiales y que la dirección preferentemente contenga “HTTPS”, ya que es un protocolo de comunicación de internet que protege la integridad y la confidencialidad de los datos intercambiados. Comprueba que la conexión con el sitio web sea segura (debe contar con un candado en la parte izquierda de la dirección web). Revisa el contenido de la página como ortografía, redacción, calidad de imágenes e idioma.

- Utiliza contraseñas robustas en todos los dispositivos o aplicaciones, en caso de que sospeches de robo, cámbiala inmediatamente. Procura utilizar diferentes contraseñas para tus cuentas de redes sociales, sitios financieros, sitios de compras y trabajo. Cuando crees una contraseña hazlo estructurando una frase, utiliza al menos 12 caracteres, combina letras mayúsculas, minúsculas, números y caracteres especiales, cámbiala al menos cada 60 días, no compartas tus contraseñas con nadie. Evita habilitar la función de recordar contraseña en los navegadores.
- Asegura tus dispositivos. Instala y mantén un programa de antivirus reconocido en tus dispositivos.
- Mantén segura tu red inalámbrica de tu casa/fija cambiando el nombre (evita usar un nombre relacionado contigo o tu familia), no utilices contraseñas por defecto, cámbiala por una robusta que incluya mayúsculas, minúsculas, números y caracteres especiales y cuida con quien compartes la contraseña de tu WiFi.
- Cuídate del “phishing”.
- Al recibir correos electrónicos, evita abrir correos de remitentes desconocidos. Si recibes un correo electrónico con algún archivo adjunto que no estabas esperando evita abrir archivos ejecutables. Revisa ligas o enlaces de páginas web que llegan a tu correo, valida que la dirección te dirija al sitio oficial pasando el mouse sobre esta. Sospecha de correos con ofertas y promociones, estos son uno de los medios más comunes para obtener información o instalar archivos maliciosos en los dispositivos.
- Mantente seguro en las redes sociales. Utiliza una contraseña robusta y cámbiala periódicamente. Evita conectarte a redes WiFi sin contraseña o gratuitas. Activa la opción de aviso de inicio de sesión y la verificación en dos pasos. Configura la privacidad y decide quién puede ver tus publicaciones. Acepta solicitudes de amistad solo de conocidos. Evita compartir información personal y/o confidencial. Desconfía de publicaciones con ofertas irresistibles, sorteos y evita dar clic en los enlaces que se incluyan. Asegúrate de cerrar sesión una vez que hayas terminado de utilizar un dispositivo que no es tuyo. Cuidado con los permisos que otorgas a las aplicaciones que utilizas. Mantente atento al listado de dispositivos y ubicaciones desde las que has tenido acceso.
- Protege tus datos personales. Protege los documentos que contienen información persona, de no ser necesarios, elimínalos de tal forma que no se puedan recuperar. Cuida la información que compartes. Verifica la autenticidad de los correos donde te soliciten comprobar o actualizar tus datos para no suspender tus cuentas o servicios. Usa contraseñas robustas para acceder a sitios y sistemas. No compartas tu información confidencial como contraseñas, códigos de autenticación o datos bancarios, a menos de que estés plenamente convencido de la autenticidad del sitio y que las finalidades de uso sean las pertinentes. Recuerda que izzi nunca te contactará para solicitar, ni confirmar datos referentes a tu tarjeta de crédito y débito.

#### Glosario

- Suscriptor: Persona física o moral que en forma eventual o permanente tiene acceso o utiliza el servicio de acceso a internet.
- Phishing: Es una forma de ciberdelincuencia que utiliza el correo electrónico y otros mecanismos de comunicación para engañar a la gente y robar información personal y/o financiera.