Código de Política de Gestión de Tráfico y Administración de Cablevisión Red, S.A. de C.V.

Objetivo

Cablevisión Red, S.A. de C.V. (en adelante "izzi") hace del conocimiento a Clientes y proveedores del servicio de acceso a Internet, su Código de Política de Gestión de Tráfico y Administración de Red (en adelante "Código") que realiza a través de los operadores de red móvil mediante los cuales provee el servicio, 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 Clientes y proveedores de servicio de acceso a Internet acerca de las medidas o acciones implementadas para la gestión de tráfico y administración de red. La infraestructura de Red Core al que le aplicará el Código será para el acceso a internet con los que cuenta izzi para tecnología "3G" en sus elementos SGSN, GGSN y de tecnología "4G" SGW, PGW y PCRF y en los elementos de salida de internet DNS, Firewall y CG-NAT.

El tráfico de datos proporcionado a través de la cobertura ofrecida por nuestros operadores móviles de red en el eNb opera bajo esquema best effort; es decir, no cuenta con una diferenciación, ni priorización por tipo de tráfico de datos entrante y saliente, excepto en casos de congestión.

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 Clientes 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 Cliente 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.

2. Trato no discriminatorio

izzi se abstendrá de obstruir, interferir, inspeccionar, filtrar, discriminar o bloquear el acceso a contenidos, aplicaciones o servicios a los Clientes, 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 Clientes de izzi pueden acceder de manera libre a contenidos, aplicaciones y servicios disponibles en internet.

izzi preservará un trato no discriminatorio entre Clientes, proveedores de aplicaciones, contenidos y servicios, tipos de tráficos 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 Clientes 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 Clientes que no sea necesaria para proveerles el servicio. Salvo casos de solicitud expresa por parte de la autoridad competente. izzi no utiliza las técnicas de DPI/DFI para monitoreo de tráfico.

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, de forma clara, comprensible y fácilmente accesible.

5. Gestión de tráfico basada en volumen de datos con una vigencia determinada

Consiste en ofrecer a los Clientes de izzi un volumen de datos con una vigencia determinada a velocidad best effort, es decir, que les permite navegar libremente en cualquier App y destino con la mayor velocidad de transferencia disponible en términos no discriminatorios. Sin embargo, en caso de que durante el mismo mes de servicio el Cliente alcance el volumen de datos del producto contratado, se aplicará una política de uso justo que reducirá la velocidad de transferencia a 512 Kbps. Este ajuste de velocidad no implica ninguna restricción para poder acceder a las distintas aplicaciones, servicios, contenidos o sitios Web ya que el usuario podrá continuar navegando libremente. La velocidad de navegación será reestablecida una vez que inicie el siguiente ciclo de facturación o, en su caso cuando haya disponibilidad, adquiera algún módulo adicional que le permita reestablecer la velocidad antes de que finalice el ciclo de facturación correspondiente.

Esta regla se utiliza para proporcionar los servicios móviles de izzi a efecto de asegurar la calidad de los servicios.

De no llevar a cabo esta práctica, se podría saturar la red y poner en riesgo el cumplimiento de los términos y condiciones ofertados.

6. Calidad y Gestión de congestión

izzi se encuentra sujeto a la calidad garantizada proporcionada por los operadores móviles de red (tasa de transmisión descendente y ascendente), la tasa de transmisión puede verse afectada por una mayor demanda de tráfico o saturación en la Radio base eNB/sector, sin embargo, se preservan 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 móvil".*

7. Desarrollo sostenido de la infraestructura

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

8. Bloqueo

izzi no lleva a cabo el bloqueo de tráfico de datos en los servicios, soló realiza prácticas de bloqueo de manera temporal en equipos no homologados que causen afectaciones en la red, en los servicios, o en las condiciones de seguridad en la Red Core.

De no llevar a cabo esta práctica, se podría saturar la red y poner en riesgo el cumplimiento de los términos y condiciones ofertados.

9. Recomendaciones al usuario final

- Utiliza equipos terminales móviles debidamente homologados y con software legítimo y autorizado.
- Visita solamente sitios seguros. Asegúrate que los sitios que visitas sean oficiales y que la dirección contenga "HTTPS", ya que es un protocolo de comunicación de internet que protege la integridad y la confidencialidad de los datos intercambiados. 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, incluyendo tu teléfono móvil.
- No te conectes a redes públicas. Existen múltiples amenazas al conectarte a redes WiFi públicas. Evita en la medida de lo posible conectar tus dispositivos a redes WiFi sin contraseña o gratuitas en sitios públicos a menos que sea absolutamente necesario.
- 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. 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. 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. 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.

- Protege la información en dispositivos móviles. Utiliza mecanismos de desbloqueo seguros como contraseñas biométricas, robustas o patrones. Mantén actualizados tus dispositivos con la última versión de software. Realiza copias de seguridad, ya que te ayudarán a recuperar tu información en caso de pérdida o daño de tu dispositivo. Asegúrate de descargas aplicaciones que provengan de fuentes confiables (tiendas oficiales), con esto evitarás el ingreso de malware a tu dispositivo. Usa la autenticación en dos pasos, agrega un nivel adicional de seguridad para garantizar el acceso seguro a cuentas, redes sociales y aplicaciones.

Glosario

- CG-NAT: se refiere a Carrier Grade Network Address Translation.
- Cliente: Persona física o moral que en forma eventual o permanente tiene acceso o utiliza el servicio de acceso a internet.
- Core: es la capa de red encargada de proporcionar conectividad entre los distintos puntos de acceso.
- DNS: se refiere a Domain Name System.
- DFI: se refiere a Deep Flow Inspection.
- DPI: se refiere a Deep Packet Inspection.
- eNB: se refiere a Evolved Node B.
- GGSN: Elemento de Red Core 3G para recepción de solicitud de sesión de datos de la BTS.
- PCRF: Elemento que aplica políticas de restricción y acceso de datos a los usuarios de acuerdo con el operador de red móvil. (Reducción de brecha).
- 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.
- PGW: Elemento de Red Core 4G para recepción de solicitud de sesión de datos de la eNB.
- SGSN: Elemento de Red Core 3G para recepción de solicitud de sesión de datos de la BTS.
- SGW: Elemento de Red Core 4G para recepción de solicitud de sesión de datos de la eNB.

Fecha de última actualización: 15 de julio 2022