*Versión 2_10/11/2022*

*Código de Política de Gestión de Tráfico y Administración de Operbes, S.A. de C.V.* y/o México Red de Telecomunicaciones, S. de R.L. de C.V.

## Objetivo.

Operbes, S.A. de C.V. y/o México Red de Telecomunicaciones, S. de R.L. de C.V. (en adelante "Bestel") hace del conocimiento a Clientes 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 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, Bestel informa oportunamente a sus Clientes del 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 Bestel para 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 implementado, asegura lo siguiente:

### 1. Libre elección.

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

El usuario puede elegir libremente el equipo terminal a través del cual pueda conectarse a la red pública de telecomunicaciones al contratar el servicio de acceso a Internet, siempre y cuando éstos se encuentren homologados.

### 2. Trato no discriminatorio.

Bestel 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 Bestel pueden acceder de manera libre a contenidos, aplicaciones y servicios disponibles en internet.

Bestel 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

Bestel 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. Bestel no utiliza las técnicas de DPI/DFI para monitoreo de tráfico.

4. Transparencia e información.

Bestel 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 regular la tasa de transferencia de la red, es decir, que la velocidad de navegación que aplicará cuando se rebase la cuota de datos establecida en la oferta contratada dentro de un periodo de 30 días naturales; esta gestión evita la sobresaturación de la red para que todos los Clientes puedan disfrutar de una adecuada experiencia de navegación. Los Clientes podrán navegar libremente en cualquier App y destino hasta la velocidad contratada, sin embargo, en caso de exceder el volumen de datos con una vigencia determinada, en la velocidad de navegación de bajada se aplicará una política de uso justo que reducirá la velocidad de transferencia. Este ajuste de velocidad no implica ninguna restricción para poder acceder a las distintas aplicaciones, servicios, contenidos o sitios Web ya que el Cliente podrá continuar navegando libremente. El Cliente podrá navegar normalmente al concluir su ciclo vigente de 30 días naturales y comenzar un nuevo ciclo mediante el pago de una recarga.

Esta regla se utiliza para proporcionar los servicios de acceso a internet de Bestel 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.

Bestel garantiza la calidad de los servicios de Internet, por lo cual ofrece a sus Clientes una tasa de transmisión descendente de al menos 4 Mbps y una tasa de transmisión ascendente de al menos 1 Mbps en el borde de la cobertura exterior en hora pico, aplicable a todo tipo de tráfico que curse por su red.

La calidad de los servicios puede verse afectada por una mayor demanda de tráfico de la originalmente prevista por el Cliente.

La gestión de congestión consiste en que Bestel ajustará los parámetros técnicos en el servicio de Internet, por lo que puede implementar una reducción de velocidad de hasta 2.5Mbps en hora pico y sitios saturados. Aplica en caso de un incremento significativo en la demanda de tráfico en un determinado eNB/sector. Se utiliza para preservar la operación y calidad de la red, de tal manera que se garantice la mejor experiencia del Cliente. La reducción de velocidad aplica para todo el tráfico de datos, por lo que de no implementarla podría afectar la operación de la red y a la calidad de los servicios ofrecidos.

7. Desarrollo sostenido de la infraestructura.

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

8. Bloqueo.

Bestel 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.

7. 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.

- 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. 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 personal, 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 Bestel 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 descargar 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.