



CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE RED

En cumplimiento con lo dispuesto por el artículo 12 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 el día 5 de julio de 2021 en el Diario Oficial de la Federación, CONECT da a conocer a sus usuarios el Código de Políticas de Gestión de Tráfico y Administración de Red.

1. GLOSARIO.

Código: El Código de Políticas de Gestión de Tráfico y Administración de Red.

Operador: Renato Gonzalez Velazquez, en lo sucesivo "CONECT"

Usuarios: Los usuarios finales del servicio de internet provisto por CONECT.

2. ACCESO A CONTENIDOS DE INTERNET

Los Usuarios podrán acceder de manera libre y sin restricciones a cualquier contenido, aplicación o servicio provisto por esta siempre y cuando no exista un mandamiento judicial que obligue al operador a suspender el servicio de forma parcial o total. CONECT garantiza a sus Usuarios que podrán conectar a su red de internet, cualquier equipo que previamente haya sido homologado por las autoridades competentes.

3. NO DISCRIMINACIÓN

CONECT se compromete con los Usuarios a que durante el tiempo que les preste el servicio, no obstruirá, interferirá, inspeccionará, filtrará o discriminará los contenidos, aplicaciones o servicios en los que pretenda navegar y consultar.

4. PRIVACIDAD

CONECT se compromete con los Usuarios a preservar la privacidad de sus usuarios y la seguridad de la red, para ello, ha implementado las medidas de seguridad necesarias que consisten, de manera enunciativa mas no limitativa en, contraseñas de seguridad, accesos controlados a las instalaciones del operador, actualización de software de seguridad y monitoreo continuo de su red.

5. TRANSPARENCIA E INFORMACIÓN

La gestión de tráfico y administración de la red se encontrará apegada a lo estipulado en el presente Código.

CONECT ofrece a sus Usuarios el servicio de internet dedicado, el cual provee una conexión a internet sin los riesgos de bajo rendimiento que implica compartir la red con otros usuarios.



Cuenta con el ancho de banda simétrico y dedicado que más se adecúe a las necesidades de sus Usuarios, transmite y controla grandes volúmenes de información con máxima velocidad, menor latencia y seguridad.

La conexión eficiente y exclusiva optimiza aplicaciones como: Conexión a Data Centers, transferencias bancarias, transacciones en la web, correo electrónico, transferencia de archivos y videoconferencias, aplicaciones relacionadas con la oficina virtual, tales como transferencia de archivos a través de la nube y educación a distancia.

6. GESTIÓN DE TRÁFICO

Los concesionarios y autorizados podrán tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red conforme a las políticas autorizadas por el Instituto, 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 competencia.

En ese orden de ideas, la gestión del tráfico de internet, también conocida como gestión del tráfico de aplicaciones, se refiere a los instrumentos que vigilan el flujo del tráfico de aplicaciones web a través de una red. Estas herramientas enrutan el tráfico entre múltiples dispositivos dentro de una red, limitando las demoras y liberando ancho de banda.

De acuerdo con la definición, la gestión del tráfico que se cursa por la red de CONECT se realiza a través de nuestros equipos enrutadores, la cual consiste en una red IP que utiliza los protocolos Ospf, BGP y MPLS. CONECT garantizará utilizar la mejor ruta a los destinos de internet, actuando de forma automática, para evitar pérdidas del servicio cuando se presentan eventos que pudieran afectarlas.

7. CALIDAD

CONNECT garantizará la continuidad de los servicios en estricto apego a los Lineamientos que fijan los índices y parámetros de calidad a que deberán apegarse los prestadores del servicio fijo.

8. DESARROLLO SOSTENIDO DE LA INFRAESTRUCTURA

CONNECT se apegará en todo momento a los lineamientos que el Instituto Federal de Telecomunicaciones emita con la finalidad de fomentar el crecimiento sostenido de la infraestructura de telecomunicaciones de los operadores.

9. POLÍTICAS DE GESTIÓN Y ADMINISTRACIÓN DE TRÁFICO IMPLEMENTADAS POR CONECT

a. ¿En qué consiste la política? .

La política de enrutamiento consiste en tomar las mejores rutas salidas a internet con las que cuenta CONECT; para ello, se apoya en sus proveedores en Estados Unidos de América, además de las conexiones directas



conocidas como peerings con clientes de otros proveedores nacionales, tales como como IZZI y Teléfonos de México, así como del acceso directo mediante peering con proveedores de contenido, tales como Amazon, Google, Facebook y Verizon.

b. ¿En qué casos y para qué se utiliza?

La política de gestión es la convergencia automática de la red en caso de fallas en las diferentes trayectorias, salidas a internet o peerings, por eventos de corte de fibra en los enlaces del backbone de la red IP.

c. ¿Qué impacto tiene la política de gestión y administración de tráfico implementada por CONECT en la experiencia al Usuario?

Permite al usuario final tener un servicio de internet con un mínimo de falla.

d. ¿Qué afectaciones podría tener el Usuario respecto de la aplicación de la política de gestión y administración de tráfico implementada por CONECT?

No existe una implementación de gestión de tráfico que limite aplicaciones o usuarios de forma particular, por lo que las políticas de gestión son aplicadas de forma general para todos los Usuarios de CONECT.

10. RECOMENDACIONES A LOS USUARIOS PARA MINIMIZAR RIESGOS A SU PRIVACIDAD Y DE SUS COMUNICACIONES PRIVADAS

- Utilizar navegadores que cuenten con identificadores para ataques de phishing.
- Mantener equipos y sistemas actualizados y realizar continuamente la instalación de parches de seguridad en sistemas operativos y aplicaciones.
- Contar con antivirus en los equipos con los que se acceda a la red global de internet.
- Observar los enlaces y páginas que se pretenden abrir de tal forma que, se evite acceder a sitios inseguros o donde se solicite información confidencial, personal o sensible.
- Cerciorarse de que se está navegando en sitios web seguros.
- No hacer clic en correos electrónicos no solicitados o que provengan de fuentes desconocidas.
- Evitar hacer caso de mensajes cuyo contenido sea atractivo, por ejemplo, adjudicación de premios provenientes de concursos donde el usuario no participó.
- Evitar relevar contraseñas de los sitios web que se frecuentan, por ejemplo, de correos electrónicos, banca electrónica, servicios públicos o cualquier otro.
- Utilizar herramientas de borrado seguro de información en los equipos de cómputo que sean desechados por el usuario.
- Actualizar periódicamente las contraseñas de sistemas y/o aplicaciones para prevenir que usuarios no autorizados tengan acceso a la información de los usuarios.
- Utilizar contraseñas seguras y robustas para proteger el acceso al sistema operativo, aplicaciones y cuentas personales de los usuarios.



- Habilitar doble factor de autenticación en aquellos sitios en donde sea posible.
- De ser necesario, comunicarse directamente con la institución a través de la información de contacto publicada en sitios oficiales.

Fecha de publicación 15 de abril de 2024.

Versión 1.0