CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE RED

OBJETIVO

El presente **Código de Políticas de Gestión de Tráfico y Administración de Red** tiene como objetivo principal informar a los usuarios finales sobre las actividades, técnicas y procedimientos que **ISMAEL URBIETA QUIÑONEZ** (en lo sucesivo "**EL PROVEEDOR**") aplica para la operación, uso eficiente y seguridad de su **red pública de telecomunicaciones**, así como para el manejo, tratamiento y procesamiento del tráfico que circula dentro de dicha red.

Estas acciones son esenciales para:

- Garantizar la adecuada gestión del tráfico,
- Cumplir con las condiciones de contratación acordadas con los usuarios finales, y
- Atender situaciones como la congestión de red, la seguridad de la infraestructura y la protección de la privacidad de los usuarios.

"EL PROVEEDOR" busca con ello asegurar la **continuidad y calidad del servicio**, promover la **libre elección del suscriptor**, garantizar un **trato no discriminatorio**, así como proteger la **privacidad e inviolabilidad de las comunicaciones**. Además, se compromete a mantener la **capacidad, velocidad y calidad de los servicios contratados**, de conformidad con los estándares nacionales e internacionales, las buenas prácticas de la industria y la normatividad vigente.

La aplicación permanente de políticas de gestión de tráfico y administración de red aporta beneficios significativos al funcionamiento estable y eficiente de la red, permitiendo:

- Salvaguardar la **seguridad e integridad** de la red ante amenazas como **ataques maliciosos**,
- Ofrecer **diversidad de servicios** adaptados a las necesidades del usuario, y
- **Garantizar los niveles de calidad de servicio** comprometidos contractualmente.

Este Código se emite en apego a lo dispuesto en los artículos 1, 2 fracción VII y 12 de los **Lineamientos para la Gestión de Tráfico y Administración de Red**, aplicables a concesionarios y autorizados que presten servicios de acceso a Internet, en correlación con lo establecido en el **artículo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión**.

CONDICIONES DE PRESTACIÓN DEL SERVICIO Y POLÍTICAS DE GESTIÓN DE RED DEL PROVEEDOR

"EL PROVEEDOR" es titular de una **Concesión Única con fines comerciales**, otorgada por el **Instituto Federal de Telecomunicaciones (IFT)**, que le autoriza a prestar servicios de telecomunicaciones y

radiodifusión, en particular el **servicio de acceso a Internet** mediante la oferta de distintos paquetes a los usuarios finales. Todos los servicios proporcionados por **"EL PROVEEDOR"** se encuentran debidamente autorizados por el IFT.

En el ejercicio de sus funciones, **"EL PROVEEDOR"** implementa políticas de **gestión de tráfico y administración de red**, las cuales pueden incluir, de manera **excepcional y temporal**, medidas como la **limitación, degradación, restricción, discriminación, obstrucción, interferencia, filtrado o bloqueo** de contenidos y aplicaciones. Estas medidas se aplicarán exclusivamente cuando sean indispensables para garantizar la **operación, seguridad e integridad** de la red, así como la **continuidad en la prestación del servicio de acceso a Internet**.

Dichas acciones se consideran razonables y justificadas solo en los siguientes casos:

a) Riesgo a la integridad de la red o de las comunicaciones privadas de los usuarios:

Cuando existan amenazas técnicamente comprobables que puedan comprometer la continuidad del servicio o la confidencialidad de las comunicaciones, tales como ataques cibernéticos u otras formas de intrusión.

b) Congestión excepcional y temporal:

Entendida como un aumento repentino y de corta duración en el tráfico de red o número de usuarios, que no corresponde a congestiones habituales en determinadas franjas horarias. En estos casos, "EL PROVEEDOR" podrá aplicar medidas temporales de gestión, **sin discriminar entre tipos de tráfico similares**. Las congestiones persistentes deben ser tratadas con mecanismos diferentes e incluso pueden señalar la necesidad de ampliar la capacidad de la red.

c) Situaciones de emergencia o desastre:

Conforme a lo establecido en la **Ley General de Protección Civil**, cuando se presenten eventos que afecten de manera directa la infraestructura de red, "EL PROVEEDOR" podrá aplicar políticas restrictivas mientras sean indispensables para atender la emergencia.

Estas acciones no eximen a "EL PROVEEDOR" de cumplir con las demás obligaciones legales y regulatorias que le son aplicables como proveedor de servicios de acceso a Internet.

Para cualquier duda, aclaración o solicitud, el usuario final podrá comunicarse a través de los siguientes canales de atención:

- **Teléfono de atención al cliente:** 6722237273
- **Correo electrónico:** Soporteultraenlace@gmail.com
- **Sitio web:** https://ultraenlace.com.mx/

- **Domicilio de atención presencial:** Calle Guillermo Prieto poste 711 B, colonia Las Cupias, entre Francisco Zarco y Mariano Escobedo, C.P. 80378, Villa Juárez, Navolato, Sinaloa.

DERECHOS DE LOS USUARIOS FINALES DEL SERVICIO DE ACCESO A INTERNET

"EL PROVEEDOR" se compromete a respetar en todo momento los derechos de los usuarios finales que hacen uso del servicio de acceso a Internet a través de su red pública de telecomunicaciones. Estos derechos, establecidos en la normatividad vigente, incluyen los siguientes:

1. **Libre elección**

   Los usuarios tienen derecho a acceder libremente a cualquier contenido, aplicación o servicio disponible en Internet, dentro del marco legal aplicable. No se les deberá limitar, degradar, restringir ni discriminar dicho acceso. Asimismo, podrán intercambiar tráfico de datos de forma abierta, utilizando dispositivos homologados en el país.

2. **No discriminación**

   "EL PROVEEDOR" se abstendrá de bloquear, interferir, inspeccionar, filtrar o discriminar el tráfico de contenidos, aplicaciones o servicios. Solo podrá realizarlo si el propio usuario lo solicita mediante servicios adicionales voluntarios, como el control parental o filtros de contenido.

3. **Privacidad**

   "EL PROVEEDOR" garantizará la confidencialidad de las comunicaciones y la protección de los datos personales del usuario final. Cuenta con un Aviso de Privacidad accesible para los clientes, en el cual se detalla el tratamiento de su información conforme a la legislación aplicable.

4. **Transparencia e información**

   "EL PROVEEDOR" deberá proporcionar información clara, veraz y actualizada sobre las características del servicio ofrecido, incluyendo velocidad, calidad, condiciones de garantía y políticas de gestión de tráfico. Esta información estará disponible públicamente a través de su sitio web oficial.

5. Gestión de tráfico

"EL PROVEEDOR" podrá aplicar medidas técnicas para administrar el tráfico en la red y garantizar la calidad del servicio contratado. Estas medidas deberán ser razonables, proporcionales, no discriminatorias y no deberán constituir prácticas contrarias a la competencia ni a la libre concurrencia.

6. Calidad del servicio

"EL PROVEEDOR" está obligado a cumplir con los parámetros de calidad establecidos en los Lineamientos de calidad del servicio fijo emitidos por el Instituto Federal de Telecomunicaciones (IFT), publicados el 25 de febrero de 2020, así como con cualquier otra disposición técnica o administrativa vigente.

7. Desarrollo sostenido de la infraestructura

"EL PROVEEDOR" se compromete a mantener y desarrollar su red de forma continua, con base en la estrategia de negocio, la disponibilidad técnica y física, y con el objetivo de garantizar un servicio eficiente y satisfactorio para los usuarios finales, en alineación con los lineamientos del IFT que promueven el crecimiento de la infraestructura de telecomunicaciones.

POLÍTICAS DE GESTIÓN Y ADMINISTRACIÓN DE TRÁFICO DEL PROVEEDOR DEL SERVICIO DE INTERNET

A continuación, se describen de manera clara y accesible las **políticas de gestión y administración de tráfico** que aplica **"EL PROVEEDOR"** en su red pública de telecomunicaciones, con el objetivo de ofrecer a los usuarios finales un **servicio eficiente, continuo y con la calidad contratada**. Estas políticas se implementan conforme a la normatividad vigente, con plena transparencia y respeto a los derechos de los usuarios.

GESTIÓN DE CONGESTIÓN / OPTIMIZACIÓN DE TRÁFICO

Se refiere a la implementación de mecanismos de control en puntos específicos de la red, activados ante eventos imprevistos que alteran su desempeño, con el fin de garantizar un flujo estable y eficiente de datos.

1. Casos en que se aplica y para qué se utiliza

Estos controles se aplican en situaciones como:
- Fallas técnicas o interrupciones en nodos de red.
- Aumentos imprevistos y excesivos en el tráfico de datos por parte de los usuarios.
- Eventos que puedan comprometer el rendimiento normal de la red.

Su finalidad es redistribuir el tráfico para aliviar las zonas saturadas y restablecer la estabilidad operativa, **sin bloquear ni discriminar contenido, aplicaciones o servicios**.

2. Impacto en el servicio al usuario final

   Puede presentarse una **reducción temporal en la velocidad de navegación**, la cual será controlada y limitada al tiempo estrictamente necesario para estabilizar la red.

3. Posibles afectaciones si no se aplica

   - **A la red:** Se corre el riesgo de un colapso progresivo en la red por la acumulación de tráfico, lo cual puede afectar a múltiples zonas.
   - **Al usuario final:** Se traduciría en **una degradación severa del servicio**, disminuyendo la velocidad hasta hacerla nula, afectando la experiencia de navegación y el uso de aplicaciones conectadas.

BLOQUEO DE CONTENIDO

Es la acción de restringir temporal o permanentemente el acceso del usuario final a determinados sitios web, contenidos, aplicaciones o servicios, ya sea por motivos de seguridad, solicitud expresa del usuario o mandato legal

1. Casos en que se aplica y para qué se utiliza

El bloqueo de contenido puede aplicarse en los siguientes casos:
• A solicitud del usuario final, quien podrá pedir el bloqueo específico de ciertos sitios o servicios por razones personales (ej. control parental).
• Por razones técnicas de seguridad, cuando un contenido o servicio represente una amenaza comprobable a la red, como malware, intentos de phishing o ataques cibernéticos. En este caso, su finalidad es proteger la integridad de la red y la privacidad de los usuarios.
• Por disposición legal o autoridad competente, en cumplimiento de resoluciones judiciales o administrativas que determinen la ilegalidad de ciertos contenidos.

2. Impacto en el servicio al usuario final

El usuario no podrá acceder al contenido, aplicación o servicio bloqueado, mientras persista la causa que justifique el bloqueo. En los casos solicitados por el usuario, el bloqueo se limitará a lo expresamente solicitado.

3. Posibles afectaciones si no se aplica

- **A la red:** Se incrementa el riesgo de ataques, filtración de datos y vulnerabilidad en la infraestructura tecnológica si se permite el acceso a contenidos maliciosos o ilícitos.
- **Al usuario final:** Puede exponerse a pérdidas de información, violaciones a su privacidad y a posibles fraudes electrónicos o suplantación de identidad, si no se bloquean los contenidos peligrosos o ilegales. En el caso de solicitudes personales no atendidas, podría no verse reflejada la personalización del servicio esperada por el usuario.

PRIORIZACIÓN DE DATOS

Es la práctica de asignar preferencia en la transmisión de ciertos tipos de datos sobre otros dentro de la red, con base en criterios técnicos previamente definidos. Esta priorización es implementada por **"EL PROVEEDOR"** con el fin de optimizar el funcionamiento de la red sin afectar la calidad del servicio contratado por los usuarios.

1. Casos en que se aplica y para qué se utiliza

La priorización de datos se aplica de manera continua durante la prestación del servicio de internet, particularmente en:
• Situaciones donde se requiere garantizar la eficiencia del flujo de tráfico en tiempo real (por ejemplo, videollamadas, servicios de emergencia o plataformas críticas).
• Escenarios que demandan balanceo de carga para evitar congestión.
• Implementación de funciones de seguridad que requieren canalizar ciertos paquetes de datos con prioridad.
Su objetivo principal es mejorar el desempeño general de la red y ofrecer una experiencia de uso más estable y eficiente.

2. Impacto en el servicio al usuario final

La priorización de datos se aplica de manera continua durante la prestación del servicio de internet, particularmente en:
• Situaciones donde se requiere garantizar la eficiencia del flujo de tráfico en tiempo real (por ejemplo, videollamadas, servicios de emergencia o plataformas críticas).
• Escenarios que demandan balanceo de carga para evitar congestión.
• Implementación de funciones de seguridad que requieren canalizar ciertos paquetes de datos con prioridad.
Su objetivo principal es mejorar el desempeño general de la red y ofrecer una experiencia de uso más estable y eficiente.

3. Posibles afectaciones si no se aplica

- **A la red:** Mayor riesgo de congestión en determinados segmentos, pérdida de eficiencia en la administración del tráfico y dificultad para mantener una calidad de servicio uniforme.
- **Al usuario final:** Aunque no se afectaría directamente la velocidad contratada, podría presentarse inestabilidad en ciertos servicios sensibles al retardo (como llamadas VoIP, videoconferencias o juegos en línea), afectando la calidad de la experiencia de uso.

SEGURIDAD DE LA RED

La seguridad de la red se refiere a la implementación de medidas, herramientas y técnicas informáticas orientadas a proteger la infraestructura, integridad y funcionamiento continuo de la red pública de telecomunicaciones operada por **"EL PROVEEDOR".** Estas acciones están diseñadas para

prevenir, detectar, mitigar y contrarrestar cualquier intento de intrusión, ataque o vulnerabilidad que pudiera afectar la red.

1. Casos en que se aplica y para qué se utiliza

Se activa en situaciones donde la red se ve amenazada por agentes externos o internos a través de ataques cibernéticos como virus, malware, spyware, ransomware o cualquier software malicioso que intente alterar, interrumpir o dañar la operatividad de la red. El objetivo es proteger tanto la infraestructura del proveedor como la información y experiencia de los usuarios finales.

2. Impacto en el servicio al usuario final

Durante la implementación de medidas de seguridad, el usuario podría experimentar disminución temporal en la velocidad de navegación o interrupción momentánea en el acceso a ciertos servicios, aplicaciones o contenidos. Sin embargo, estas afectaciones serán mitigadas al máximo y limitadas a lo estrictamente necesario para preservar la integridad de la red.

3. Posibles afectaciones si no se aplica

A la red: La ausencia de mecanismos de seguridad puede derivar en la propagación de software malicioso, afectando la estabilidad, disponibilidad y rendimiento general de la red. Esto comprometería la continuidad del servicio y los datos en tránsito.

Al usuario final o en sus comunicaciones: Riesgo de filtración o pérdida de información personal, accesos no autorizados, interceptación de comunicaciones, así como afectaciones en la calidad del servicio recibido.

RECOMENDACIONES PARA LOS USUARIOS FINALES PARA MINIMIZAR RIESGOS A LA PRIVACIDAD

Con el fin de proteger su información personal y navegar de forma más segura en internet, **“EL PROVEEDOR”** emite las siguientes recomendaciones para sus usuarios finales:

1. Evite sitios no confiables o de dudosa reputación.

   No acceda a páginas desconocidas o con ofertas engañosas. Estas pueden estar controladas por terceros maliciosos que buscan robar o dañar su información. Asegúrese de visitar sitios seguros, preferentemente con el protocolo HTTPS, y evite dar clic en anuncios sospechosos o promociones "gratuitas".

2. Proteja sus dispositivos con contraseñas seguras.

   Use contraseñas robustas con combinaciones de letras, números y símbolos. Bloquee sus equipos con códigos de acceso o reconocimiento biométrico para prevenir el uso no autorizado en caso de extravío o robo.

3. Instale y mantenga actualizado un antivirus confiable.

   Un software antivirus ayuda a detectar y bloquear programas maliciosos que intentan acceder a sus datos. Mantenga su antivirus activo y en su versión más reciente para una protección continua.

4. Mantenga sus sistemas y aplicaciones actualizados.

   Actualizar periódicamente su sistema operativo, navegador y aplicaciones reduce las vulnerabilidades que podrían ser explotadas por atacantes. Los fabricantes publican parches de seguridad que refuerzan la protección de su información.

5. Realice copias de seguridad de su información.

   Para prevenir la pérdida de datos, respalde periódicamente sus archivos en dispositivos externos (como discos duros) o en servicios confiables de almacenamiento en la nube.

MARCO LEGAL APLICABLE

- Constitución Política de los Estados Unidos Mexicanos, artículos 1,6,7,28 y demás aplicables
- Ley Federal de Telecomunicaciones y Radiodifusión artículos 145, 146 y demás aplicables.
- 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.
- Lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores del servicio fijo

Última actualización:11/08/2025