



# CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE RED

---

## 1. INTRODUCCIÓN

Este documento describe las políticas de gestión de tráfico y administración de red (en adelante, el “Código”), en su calidad de Proveedor del Servicio de Acceso a Internet (PSI). Su propósito es transparentar los principios, prácticas y medidas técnicas aplicadas para garantizar un uso eficiente de la red, preservar la calidad del servicio contratado y respetar en todo momento los derechos de los usuarios finales, conforme al **Artículo 12** de los Lineamientos y demás normatividad aplicable.

## 2. DERECHOS DE LOS USUARIOS FINALES (conforme al artículo 145 de la LFTR)

Se garantiza a todos los usuarios finales los siguientes derechos:

### 2.1. Libre elección

Los usuarios pueden acceder y utilizar cualquier contenido, aplicación o servicio legal disponible en Internet, sin discriminación ni bloqueos técnicos por parte del proveedor.

### 2.2. No discriminación

El tráfico generado por los usuarios es tratado de forma equitativa, sin que se favorezca, degrade o restrinja selectivamente algún tipo de contenido, servicio o aplicación.

### 2.3. Privacidad

Se protegen los datos personales y la privacidad de las comunicaciones de sus usuarios, conforme al Aviso de Privacidad disponible en su portal web.

### 2.4. Transparencia e información

Toda la información relacionada con la calidad, velocidad, latencia, administración de red, así como las presentes políticas, está disponible en el sitio web oficial y en el Código de Prácticas Comerciales.

### 2.5. Calidad

Se proporciona el servicio conforme a los niveles mínimos de calidad definidos por el IFT, incluyendo velocidad de acceso, disponibilidad y continuidad.



# CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE RED

---

## 3. POLÍTICAS DE GESTIÓN Y ADMINISTRACIÓN DE TRÁFICO

A continuación se describen cada una de las políticas adoptadas, conforme a los lineamientos aplicables:

### 3.1. Optimización de tráfico

#### ¿En qué consiste?

Aplicación de técnicas como balanceo de carga, gestión del ancho de banda y priorización de tráfico.

#### ¿Cuándo y para qué se utiliza?

Durante periodos de alta demanda o congestión para garantizar el uso eficiente de recursos y mantener una experiencia estable.

#### Impactos en la experiencia del usuario:

Mejora en los tiempos de carga, estabilidad de la conexión y calidad del servicio.

#### Consecuencias si no se implementa:

Riesgo de saturación, latencia elevada, interrupciones del servicio o degradación en el desempeño general.

### 3.2. Administración de direcciones IP

#### ¿En qué consiste?

Asignación dinámica o estática de direcciones IP conforme a las mejores prácticas de la IANA.

#### ¿Cuándo y para qué se utiliza?

Para identificar dispositivos en la red, garantizar conectividad y prevenir abusos de recursos.

#### Impacto:

No perceptible directamente para el usuario, pero esencial para una operación segura y eficiente.

#### Consecuencias si no se implementa:

Riesgo de conflictos de red, imposibilidad de conexión, problemas de rastreabilidad o mal uso del servicio.

### 3.3. Gestión de tráfico en congestión



## CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE RED

---

### ¿En qué consiste?

Priorización temporal de ciertos tipos de tráfico (p. ej., videollamadas, VoIP) ante congestión puntual.

### ¿Cuándo se aplica?

En momentos críticos para asegurar continuidad del servicio esencial sin degradar otros tipos de tráfico.

### Impacto:

Experiencia más fluida en servicios sensibles a la latencia.

### Consecuencias si no se implementa:

Congestión sostenida, interrupciones y frustración del usuario final.

## 3.4. Protección contra amenazas

### ¿En qué consiste?

Monitorización del tráfico para detectar patrones anómalos o código malicioso.

### ¿Cuándo se utiliza?

De forma continua para prevenir ataques (DDoS, malware, etc.).

### Impacto:

Incremento en la seguridad general del servicio.

### Consecuencias si no se implementa:

Infecciones, vulneraciones de seguridad, filtraciones de datos.

## 4. RECOMENDACIONES DE PRIVACIDAD Y SEGURIDAD PARA EL USUARIO FINAL

Para minimizar los riesgos a la privacidad y a sus comunicaciones privadas, CLEAR SIGNAL recomienda:

- Usar **software antivirus actualizado** y activar cortafuegos.
- Evitar visitar sitios sin **certificados de seguridad** o que no sean reconocidos.
- **Actualizar contraseñas periódicamente** y usar combinaciones robustas.
- Configurar adecuadamente los **niveles de privacidad en redes sociales**.
- Instalar **herramientas de control parental** cuando menores utilicen el servicio.
- Descargar aplicaciones **únicamente de fuentes oficiales**.
- Evitar proporcionar datos sensibles a sitios no verificados.



# CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE RED

---

## 5. MARCO LEGAL Y ESTÁNDARES INTERNACIONALES

Esta Política se encuentra sustentada en:

- **Ley Federal de Telecomunicaciones y Radiodifusión**, en particular el artículo 145.
- **Lineamientos de gestión de tráfico y administración de red**, emitidos por el Instituto Federal de Telecomunicaciones.
- **Estándares internacionales** de la Internet Engineering Task Force (IETF) y otras entidades reconocidas, como IEEE, ICANN, ISOC.

## 6. INFORMACIÓN ADICIONAL Y ACTUALIZACIONES

Este Código es revisado y actualizado periódicamente en cumplimiento de la normativa vigente.

- **Última actualización:** diciembre 2025.
- **Ubicación del documento:** Disponible en el portal web <https://catvcentro.com/>, en la sección "Gestión de Red y Políticas de Tráfico".
- **Contacto para dudas o comentarios:** [ctvcentro@gmail.com](mailto:ctvcentro@gmail.com)