

Gestión de Tráfico y Administración de Red

DEFDO, S.A.S. DE C.V.

Estructura del servicio

DEFDO, S.A.S. DE C.V. opera la marca DEFDO, sus sitios y la relación comercial con el usuario. GRUPO BITELIT, S.A. DE C.V. proporciona a DEFDO los servicios móviles subyacentes. La conectividad se presta principalmente sobre la Red Compartida operada por Altán Redes y, cuando corresponda, sobre redes de terceros.

Este documento describe, en lenguaje orientado a usuarios, los principios y prácticas aplicables a la gestión de tráfico y administración de red de los servicios de acceso a Internet comercializados por DEFDO. Las funciones técnicas son ejecutadas por el proveedor móvil y los operadores de red correspondientes; DEFDO no administra directamente la Red Compartida.

1. Marco regulatorio

Los Lineamientos para la gestión de tráfico y administración de red emitidos en 2021 continúan siendo referenciados por la Comisión Reguladora de Telecomunicaciones (CRT) en 2026. Su aplicación debe interpretarse junto con la Ley en Materia de Telecomunicaciones y Radiodifusión vigente y las disposiciones que la sustituyan, modifiquen o complementen.

2. Principios

- Libre elección: el usuario puede acceder a contenidos, aplicaciones y servicios lícitos de su elección, sujeto a la capacidad de su servicio y a la normativa aplicable.
- No discriminación: el tráfico no debe ser bloqueado, degradado o priorizado arbitrariamente por razón de su origen, destino, contenido, aplicación o servicio, salvo prácticas permitidas por la regulación.
- Privacidad e inviolabilidad de las comunicaciones: las técnicas de gestión deben respetar la legislación de privacidad y las comunicaciones privadas.
- Transparencia: las prácticas relevantes deben explicarse de manera clara, indicando su finalidad e impacto potencial.
- Gestión eficiente: pueden aplicarse medidas técnicas razonables para preservar calidad, capacidad, seguridad e integridad de la red.

3. Prácticas que pueden aplicarse

GRUPO BITELIT y/o el operador de red pueden implementar medidas temporales, proporcionales y técnicamente justificadas para:

- Mitigar congestión excepcional o temporal y mantener la estabilidad del servicio.
- Proteger la red y a los usuarios frente a ataques, fraude, malware, spam, tráfico malicioso o vulnerabilidades.
- Aplicar límites de datos, velocidades o condiciones expresamente establecidos en la oferta contratada.
- Gestionar fallas, mantenimiento, recuperación ante desastres y continuidad operativa.
- Dar prioridad a comunicaciones de emergencia o cumplir instrucciones legalmente válidas de la autoridad competente.
- Impedir usos que degraden la red o vulneren políticas de uso justo, siempre bajo criterios objetivos y no discriminatorios.

4. Lo que no debe ocurrir

No se aplicarán bloqueos, degradaciones o interferencias arbitrarias para favorecer contenidos propios o perjudicar competidores. Cualquier restricción deberá tener fundamento técnico, contractual o legal válido, limitarse a lo necesario y respetar los derechos de las personas usuarias.

5. Impacto en la experiencia

La velocidad y latencia pueden variar por cobertura, capacidad radioeléctrica, número de usuarios concurrentes, ubicación, interiores, condiciones climáticas, interferencia, características del equipo, mantenimiento o congestión. Las medidas de gestión legítimas pueden producir reducciones temporales de velocidad o priorización técnica durante eventos excepcionales, buscando mantener la disponibilidad del servicio para el mayor número de usuarios.

6. Planes, bolsas y uso de datos

Las bolsas de datos, vigencias, velocidades y beneficios se rigen por la oferta contratada. Agotada una bolsa, el servicio podrá terminar, reducir velocidad o requerir una nueva recarga según lo informado en la oferta. El tráfico patrocinado o beneficios de aplicaciones específicas sólo aplicarán cuando formen parte expresa de la oferta y cumplan los requisitos regulatorios correspondientes.

7. Privacidad y seguridad del usuario

- Mantener actualizado el sistema operativo y aplicaciones del dispositivo.
- Utilizar contraseñas robustas y mecanismos de autenticación disponibles.
- Evitar redes Wi-Fi desconocidas o servicios que soliciten credenciales sin una razón clara.
- Revisar permisos de aplicaciones y las políticas de privacidad de terceros.
- Reportar a DEFDO comportamientos anómalos, accesos no reconocidos o indicios de fraude.

8. Actualizaciones

Versión 2.0. Última actualización: 2 de octubre de 2026. DEFDO publicará la versión vigente cuando existan cambios técnicos, comerciales o regulatorios relevantes.