PRÁCTICAS DE GESTIÓN DE TRÁFICO

Servicio de Internet Fijo – INSITEL S.A.S. (marca bitwan)

Versión 1.0 – Vigente desde noviembre de 2026

1. Objeto y marco normativo

En cumplimiento del artículo 56 de la Ley 1450 de 2011 y del régimen de neutralidad en Internet contenido en la Resolución CRC 5050 de 2016 (en particular su artículo 2.9.2.4), INSITEL S.A.S., que presta el servicio de acceso a Internet fijo bajo la marca **bitwan**, informa a sus usuarios las prácticas de gestión de tráfico que aplica en su red, la finalidad de cada una y la forma en que pueden afectar el servicio.

Estas prácticas aplican a todos los servicios de Internet fijo de bitwan, tanto en las redes de fibra óptica como en las de radioenlace, y al tráfico IPv4 e IPv6.

2. Principios

Toda práctica de gestión de tráfico que aplica bitwan cumple los siguientes principios:

- **Finalidad legítima:** solo se aplican para preservar la seguridad e integridad de la red, gestionar la congestión, garantizar la calidad del servicio o cumplir la ley y las órdenes de autoridad competente.
- **Razonabilidad y proporcionalidad:** se usa la medida menos restrictiva posible y se limita al tráfico, servicio o equipo que origina el problema.
- **Temporalidad:** las medidas dirigidas a un servicio específico se mantienen solo mientras persista la causa que las originó.
- **No discriminación:** las medidas no se aplican con fines comerciales ni para favorecer o perjudicar a un proveedor, contenido o aplicación en particular.
- **Transparencia:** todas las prácticas se describen en este documento, que se mantiene publicado y actualizado.

3. Gestión de la congestión y calidad del servicio

- bitwan monitorea de forma permanente el uso de su red troncal, nodos y enlaces de salida a Internet, y amplía capacidad cuando los niveles de ocupación lo requieren.
- La velocidad de cada servicio se administra mediante colas de reparto equitativo según el plan contratado. Estas colas garantizan que cada usuario reciba su velocidad contratada y que, en momentos de alta demanda, la capacidad se distribuya de manera equitativa entre los usuarios del mismo plan.
- La gestión de la congestión se aplica al tráfico en general. No se reduce la velocidad ni se da menor prioridad a aplicaciones, contenidos o proveedores específicos.

4. Direccionamiento IP

- **IPv4 compartida (CGNAT):** por la escasez mundial de direcciones IPv4, los servicios residenciales navegan a través de direcciones IPv4 públicas compartidas por varios usuarios. Esto no afecta la navegación ni el uso normal de aplicaciones, pero impide recibir conexiones entrantes desde Internet por IPv4 (por ejemplo, para alojar servidores, acceder de forma remota a cámaras o grabadores, o abrir puertos).
- **IP pública dedicada:** el usuario que necesite recibir conexiones entrantes por IPv4 puede solicitar una dirección IP pública dedicada a través de los canales de atención, según las condiciones comerciales vigentes.

- **IPv6:** bitwan asigna direccionamiento IPv6 público a los servicios que cuentan con equipos compatibles. Por seguridad, las conexiones entrantes desde Internet hacia los puertos web (80 y 443) de los equipos de los usuarios se filtran en IPv6.

5. Seguridad e integridad de la red

Las siguientes medidas protegen a los usuarios y a la red frente a ataques, software malicioso y usos que pueden afectar la calidad del servicio de todos los usuarios o la reputación de las direcciones IP compartidas.

5.1 Puertos restringidos

Para todos los servicios se restringe el tráfico en los siguientes puertos, que son usados de forma recurrente para propagar software malicioso, enviar correo no deseado o realizar ataques:

Puerto(s)	Protocolo	Motivo de la restricción
25 (salida hacia Internet)	TCP	Envío de correo no deseado (spam) desde equipos infectados. El envío de correo desde programas como Outlook, Thunderbird o aplicaciones móviles funciona normalmente por los puertos autenticados 465 y 587.
135, 137, 138, 139 y 445	TCP / UDP	Servicios para compartir archivos de Windows (NetBIOS/SMB), usados para propagar virus y ransomware entre redes. No están diseñados para usarse a través de Internet.
111	TCP / UDP	Servicio RPC, usado en ataques de amplificación y reconocimiento de redes.
11 y 19	TCP / UDP	Servicios obsoletos (systat y chargen) usados en ataques de amplificación.
5683 y 5684	TCP / UDP	Protocolo CoAP de dispositivos IoT, usado en ataques de amplificación.

5.2 Bloqueo de destinos maliciosos

bitwan bloquea la comunicación con direcciones IP identificadas por fuentes de seguridad reconocidas como servidores de comando y control de redes de equipos infectados (botnets), sumideros de malware e infraestructura usada en ataques coordinados. Esta medida impide que un equipo infectado reciba instrucciones o envíe información robada. Las listas se revisan y actualizan periódicamente; si un usuario considera que un destino legítimo está afectado, puede solicitar su revisión mediante PQR.

5.3 Detección de comportamiento anómalo

La red cuenta con mecanismos automáticos que identifican servicios cuyo tráfico presenta patrones propios de equipos comprometidos, como:

- escaneo masivo de direcciones o puertos en Internet;
- intentos repetidos de acceso a servicios remotos (fuerza bruta);
- envío masivo de correo o de consultas DNS;
- participación en ataques de denegación de servicio o de amplificación;
- cantidades de conexiones simultáneas muy superiores a las de un uso doméstico o empresarial normal;
- comunicación con servidores de comando y control de malware.

Esta detección no bloquea el servicio por sí misma: identifica los casos para que el personal técnico los analice antes de aplicar cualquier medida.

5.4 Medidas sobre equipos comprometidos

Cuando bitwan confirma que un equipo conectado al servicio de un usuario (por ejemplo, decodificadores o TV box, cámaras, computadores u otros dispositivos) genera tráfico malicioso, participa en redes de proxy o en ataques contra terceros, o provoca reportes de abuso contra las direcciones IP de la red, podrá aplicar una o varias de las siguientes medidas:

- restringir el acceso a Internet únicamente del equipo afectado, desde el equipo terminal (ONT/router) instalado en el domicilio;
- limitar la cantidad de conexiones simultáneas del servicio o bloquear tipos de tráfico específicos usados por el software malicioso;
- bloquear la comunicación del servicio con los destinos asociados al ataque.

Estas medidas se limitan al equipo o al tipo de tráfico que origina el problema, no reducen la velocidad contratada ni afectan los demás equipos del hogar, y se retiran cuando el equipo se desconecta, se desinfecta o se restablece a su configuración de fábrica. bitwan podrá contactar al titular del servicio para informarle la situación y orientarlo. El usuario puede consultar en cualquier momento, a través de los canales de atención, si su servicio tiene alguna medida aplicada y solicitar su revisión.

Recomendación: muchos decodificadores y aplicaciones que ofrecen canales o contenidos de pago de forma gratuita incluyen software que utiliza la conexión del usuario sin su conocimiento. bitwan recomienda adquirir equipos de fabricantes reconocidos y usar únicamente aplicaciones de proveedores autorizados.

5.5 Protección contra ataques de denegación de servicio

bitwan cuenta con un servicio especializado de detección y mitigación de ataques de denegación de servicio (DDoS) en su salida a Internet. Durante un ataque, el tráfico malicioso dirigido a la red se filtra para mantener la disponibilidad del servicio. Esta medida se aplica únicamente al tráfico del ataque.

5.6 Protección contra suplantación de direcciones

La red solo permite el tráfico originado desde las direcciones asignadas a servicios activos y descarta el tráfico con direcciones de origen falsas o reservadas. Esto impide que la red sea usada para lanzar ataques con direcciones suplantadas.

6. Bloqueos por mandato legal u orden de autoridad

- Conforme a la Ley 679 de 2001 y el Decreto 1524 de 2002, bitwan bloquea el acceso a páginas con contenido de explotación sexual de niños, niñas y adolescentes, según los listados que suministran las autoridades competentes.
- bitwan bloquea el acceso a los sitios, aplicaciones y direcciones cuyo bloqueo ordenen las autoridades judiciales o administrativas competentes, entre ellos las plataformas de distribución no autorizada de contenidos audiovisuales ordenadas por protección de derechos de autor.

7. Suspensión del servicio

Cuando el servicio se suspende por falta de pago u otras causales previstas en el contrato, el acceso a Internet se restringe en los términos del contrato y se restablece una vez superada la causa de la suspensión.

8. Control parental

En cumplimiento del artículo 56 de la Ley 1450 de 2011, bitwan informa a los usuarios que lo soliciten sobre herramientas de control parental para restringir el acceso a contenidos que atenten contra la ley o no sean aptos para menores de edad, y sobre su funcionamiento. Estos filtros se aplican únicamente por solicitud expresa del titular del servicio.

9. Responsabilidades del usuario

- La seguridad de los equipos del usuario (computadores, celulares, tabletas, decodificadores, cámaras y similares) y la protección de sus contraseñas son responsabilidad del usuario.
- El uso del servicio y de los dispositivos conectados al equipo instalado en el domicilio es responsabilidad del titular, de acuerdo con su contrato.
- bitwan no administra la autenticación ni la seguridad de aplicaciones y servicios de terceros.

10. No discriminación

Salvo las medidas descritas en este documento, bitwan no bloquea, interfiere, discrimina, prioriza ni restringe el derecho de los usuarios a acceder, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio lícito a través de Internet. Las prácticas descritas no se usan con fines comerciales ni reducen la velocidad contratada.

11. Actualización de este documento

bitwan actualizará este documento cuando incorpore, modifique o retire prácticas de gestión de tráfico. La versión vigente estará siempre publicada en www.bitwan.co.

12. Inquietudes y PQR

Si tiene dudas sobre estas prácticas, considera que afectan su servicio o desea solicitar la revisión de una medida aplicada, puede presentar una petición, queja o recurso (PQR) a través de:

- Línea gratuita: 01 8000 930 141
- Página web: www.bitwan.co
- Oficina: Calle 5 # 8-25, Alcalá, Valle del Cauca