

Código de Políticas de Gestión de Tráfico y Administración de Red

Cuestión Previa

El presente Código de Políticas de Gestión de Tráfico y Administración de Red (en adelante, “**Código**”), se elaboró de conformidad con el último párrafo del 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 en el Diario Oficial de la Federación el 5 de julio de 2021 (en adelante, “**Lineamientos**”), en el entendido de los elementos de red necesarios para implementar políticas de gestión de tráfico y administración de red son con base a las políticas que fueron emitidas por el operador de red Altán Redes, S.A.P.I. de C.V. (en adelante, “**Altán**”).

Objeto

El presente Código tiene por objeto establecer los criterios para la implementación de la gestión de tráfico y administración de red del servicio de acceso a Internet respecto a la calidad, capacidad y velocidad de dicho servicio contratado por nuestros usuarios finales, así como para preservar la integridad y seguridad de la red.

Es por ello, que, a través del Código, se da a conocer a nuestros usuarios finales las medidas o acciones que se encuentran implementadas en la red de Altán para la gestión de tráfico y administración de red.

Asimismo, se hace del conocimiento que el presente Código garantiza la libre elección de los usuarios finales para acceder a cualquier tipo de contenido, aplicaciones y servicios disponibles en internet, sin bloquear, estrangular, priorizar, limitar, degradar, restringir o discriminar el acceso a los mismos de forma arbitraria, tal y como lo establece el artículo 7 de los Lineamientos.

Principios del servicio de acceso a Internet y políticas de gestión

De conformidad con el artículo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión, el Código se ha elaborado con los principios mínimos que debe de contener el servicio de acceso a Internet, los cuales son:

i. Libre elección

El servicio de acceso a Internet permite que los usuarios finales de bait puedan acceder a cualquier contenido, aplicación o servicios en Internet sin limitar, degradar, restringir o discriminar el acceso a los mismos. Lo anterior, conforme a los términos, condiciones y estructuras tarifarias contenidas en los paquetes de beneficios registrados ante el Instituto Federal de Telecomunicaciones.



ii. Trato de discriminatorio

Bait a través de la red de Altán, se abstendrá de obstruir, interferir, inspeccionar, filtrar o discriminar contenidos, aplicaciones o servicios.

iii. Privacidad y seguridad de las comunicaciones

A nivel de técnico, bait se encuentra obligado a asegurar la inviolabilidad de las comunicaciones privadas de los usuarios finales a través de la red de Altán y su privacidad, así como garantizar la calidad y velocidad de servicio contratado por el usuario final, siempre que ello no constituya prácticas contrarias a la sana competencia y libre competencia. Por tal motivo, no se utilizan técnicas de gestión de tráfico mediante DPI/DFI para mantener la privacidad de los usuarios de forma segura.

iv. Gestión de tráfico basada en volumen de datos con una vigencia determinada

Consiste en ofrecer a los usuarios finales de bait un volumen de datos con una vigencia determinada a las velocidades que tecnológicamente sea permitido y respecto a un esquema *Best Effort*. Una vez alcanzado el volumen de datos del producto contratado por el usuario final de bait, puede contratar un nuevo paquete de beneficios para alcanzar máximas velocidades o bien, continuar con su servicio a velocidad reducida de 512 Kbps hasta la conclusión de esta. En todos los casos, el tráfico de datos incluye el acceso a cualquier contenido, aplicación o servicio en Internet en términos no discriminatorios.

De no llevar a cabo la reducción de velocidades podría saturar la red y poner en riesgo el cumplimiento de los términos y condiciones de calidad de los paquetes de beneficios.

Lo anterior es aplicado tanto a los servicios de telefonía móvil como Internet al Hogar de conformidad con las estructuras tarifarias y promociones registradas ante el Instituto Federal de Telecomunicaciones.



v. Calidad y gestión de congestión

Bait garantiza la calidad de los servicios móviles y de Internet al Hogar, por lo cual ofrece a sus usuarios finales una tasa de transmisión descendente de al menos 4 Mbps y una tasa de transmisión ascendente de al menos 1Mbps en el borde de la cobertura exterior en hora pico, aplicable a todo tipo de tráfico que curse por la red.

La calidad de los servicios puede verse afectada por una mayor demanda de tráfico o una mayor conexión de usuarios finales de los originalmente previstos por bait. Para dichos efectos y con la finalidad de mantener la integridad de la red utilizada por bait.

La gestión de congestión consiste en que bait a través de la red de Altán ajustará los parámetros técnicos en el servicio de Internet al Hogar, por lo que puede implementar una reducción de velocidad de hasta 2.5Mbps en hora pico y sitios saturados. Aplica en caso de un incremento significativo en la demanda de tráfico y/o usuarios finales en un determinado sector. Se utiliza para preservar la operación y calidad de la red, de tal manera que se garantice la mejor experiencia del conjunto de usuarios finales de bait. La reducción de velocidad aplica para todo el tráfico de datos, por lo que de no implementarla podría afectar la operación de la red y a la calidad de los servicios ofrecidos.

Por otro lado, la calidad ofrecida siempre cumple con los márgenes de calidad establecidos de tiempo en tiempo por el Instituto Federal de Telecomunicaciones.

Características

Los paquetes de beneficios que incluyen el acceso a Internet y que se ofertan por bait a sus usuarios finales, utilizan *Domain Name System* (DNS, por sus siglas en inglés) Firewall y *Carrier Grade Network Address Translation* (CG-NAT, por sus siglas en inglés) que permiten lo siguiente:

- Traducción de las direcciones IP privadas a IP públicas en Internet, con el fin de poder proveer el servicio a todos nuestros usuarios.
- Resolver nombres en las redes, en el entendido de que el DNS es utilizado para conocer la dirección IP de la máquina donde se encuentra alojado el dominio al que se quiera acceder.
- Es utilizado el Firewall que su función es prevenir y proteger la red de telecomunicaciones que proveen el acceso a Internet de intrusiones o ataques de otras redes.



El tráfico de datos sobre la cobertura ofrecida opera bajo esquema de *Best Effort*, es decir, que la calidad del servicio (QoS, por sus siglas en inglés) del tráfico puede verse mermada en casos de saturación o congestión de tráfico, así como también, no hace diferencia prioriza el tipo de tráfico de datos de los usuarios finales hacia/desde Internet, salvo en casos de saturación o congestión en donde se tienen que habilitar servicios de mayor importancia, tales como los de emergencia, entre otros.

Recomendaciones para usuarios finales

Para que nuestros usuarios tengan una mejor experiencia y en todo lo posible, se reduzcan o minimicen los riesgos a su privacidad y de sus comunicaciones privadas, a continuación, se presentan las siguientes recomendaciones:

- Elegir contraseñas seguras y cambiarlas de manera regular. Se deben de establecer contraseñas que sean combinadas con caracteres, mayúsculas y minúsculas, lo que ayudará a que la persona sea difícilmente identificable mediante datos básicos como edad, año de nacimiento, entre otras, así como modificarlas con frecuencia
- Compartir información. Cuidar en donde, qué información y a quien se comparte i ya que existen sitios web que pueden utilizar tu información para otro tipo de finalidades. Por lo que, es importante que el usuario solamente comparta información en sitios de confianza que inicien con https.
- Descarga segura de software y aplicaciones. De igual forma, se recomienda realizar descarga de cualquier, software o aplicación a través de medios reconocidos y lugares oficiales, que garanticen que las descargas son seguras y confiables.
- Contar con medidas de protección contra malware y otros virus informáticos. Es importante contar con herramientas de seguridad toda vez que existen virus que pueden obtener datos y acceso a su dispositivo y al descargarlos, ejecutan contenidos maliciosos que destruyen o se apropian de los datos almacenados.
- Precaución con dar click a enlaces sospechosos y descargar documentos adjuntos en mensajes de destinatarios desconocidos, ya que podríamos estar facilitando el acceso a terceros y/o virus informáticos, a nuestros datos sin nuestro consentimiento.



- Revisa las políticas de privacidad y avisos de privacidad de los sitios web a los que ingresas, a efectos de que tengas conocimiento el procesamiento que realizan de tu información, las finalidades y los mecanismos con los que cuentas para oponerte o revocar tu consentimiento a dicho tratamiento, en caso de que lo hayas otorgado.
- Herramienta de seguimiento en línea. Hay que tomar en cuenta que algunos sitios en internet utilizan herramientas de seguimiento en línea que recaban información sobre tu comportamiento y navegación en el sitio, así como de intereses y preferencias, por ello es importante que revises los avisos y leyendas en donde informan de qué manera utilizan este tipo de herramientas y la forma en cómo puedes ajustar tu configuración para deshabilitarlas si no deseas que recopilen tus datos.
- La instalación de actualizaciones en software y aplicaciones. Las actualizaciones permiten reforzar elementos como la seguridad de aplicaciones y programas en beneficio de la protección de nuestra información.

Configura tu privacidad en redes sociales. Las redes sociales cuentan con opciones para configurar nuestra privacidad, controlar el acceso y permisos que damos a terceros a nuestra información personal, las cuales se recomienda utilizar.

- Leer términos y condiciones. Es importante que el usuario al descargar o hacer uso de una página web, lea los términos y condiciones de la misma, toda vez que así el usuario sabrá con certeza que tratamiento se les dará a sus datos personales.
- Redes públicas. Se recomienda no utilizar el acceso de Wi-Fi gratuito ya que se desconocen las medidas de seguridad que esas redes puedan tener y, por ende, si pueden tener acceso a su dispositivo. En caso de contestarse, evitar hacer uso de servicios bancarios, correo electrónico y/o redes sociales.



Referencias

Instituto Federal de Telecomunicaciones. Estudio: Neutralidad de Red. Recuperado de http://www.ift.org.mx/sites/default/files/industria/temasrelevantes/13791/documentos/3estudio_sobreneutralidaddered.pdf

Instituto Federal de Telecomunicaciones. Neutralidad de la red. Recuperado de http://www.ift.org.mx/sites/default/files/neutralidad_de_la_red_v.pdf

Microsip. Protección de tus datos personales: 9 medidas de seguridad. Recuperado de <https://blog.microsip.com/9-medidas-para-proteger-tus-datos-personales/>

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Recomendaciones para mantener segura tu privacidad y Datos Personales en el entorno digital. Recuperado de: https://home.inai.org.mx/wp-content/uploads/5RecomendacionesPDP_Web.pdf (inai.org.mx)

Ley Federal de Telecomunicaciones y Radiodifusión.

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.

Fecha de actualización. 3 de septiembre de 2021.



Glosario

Core. Es la capa de red encargada de proporcionar conectividad entre los distintos puntos de acceso.

DNS. Domain Name System

eNB: Evolved Node B

URL. Uniform Resource Locator

