Código de Políticas de Gestión de Tráfico y Administración de Red

Neutralidad de Red

Actualizado al 03/Sep/2021 – Versión 1

El presente documento se expide en cumplimiento de lo señalado en el artículo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión y a 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, publicados en el Diario Oficial de la Federación el 5 de julio de 2021, en específico el Lineamiento 12 último párrafo.

Este documento describe las políticas de gestión de tráfico y administración de red para el acceso a la red de Internet, ello para que el usuario esté informado de éstas y sepa que dichas políticas están se elaboraron atendiendo a los siguientes derechos y prinicipios que se mencionan en éste Código.

En nuestra oferta de servicios de telecomunicaciones en específico del servicio de acceso a Internet se incluye el servicio de DNS, Firewall y CG-NAT (Network Address Translation) que permite la traducción de IPs privadas a IPs públicas en Internet, así como el ISP para que el usuario cuente con navegación en Internet.

El tráfico de datos sobre nuestra cobertura opera bajo esquema de calidad y disponibilidad de *mejor esfuerzo ("Best effort")*, toda vez que la red no garantiza la calidad del servicio (QoS) del tráfico, es decir, no diferencia ni prioriza el tipo de tráfico de Datos de los clientes hacia/desde Internet, excepto en casos de congestión.

Políticas de Gestión de Tráfico.

La Política de Gestión de Tráfico y Administración de Red implementada por nuestro proveedor de acceso de red asegura lo siguiente:

1. Libre elección.

El servicio de acceso a Internet que ofrece nuestro proveedor de red permite que los usuarios finales de los puedan acceder a cualquier contenido, aplicación o servicios en Internet, sin dificultar, limitar, degradar, restringir o discriminar el acceso a los mismos. Lo anterior, conforme a los términos, condiciones y estructuras tarifarias contenidas en las ofertas inscritas en el Instituto Federal de Telecomunicaciones (IFT).

2. Trato no discriminatorio.

Nuestro proveedor de acceso a la red se obliga a tratar de la misma manera el tráfico de los contenidos, aplicaciones o servicios de tipo similar en Internet entre los usuarios finales.

3. Privacidad y seguridad de las comunicaciones.

A nivel técnico, nuestro proveedor de acceso a la red se encuentra obligado a asegurar la inviolabilidad de las comunicaciones privadas de los usuarios finales a través de su red de acceso y garantizar su privacidad. Nuestro proveedor de acceso a la red no utiliza las técnicas de DPI/DFI para monitoreo de tráfico.

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

Consiste en ofrecer a los usuarios finales acceso a la red con un volumen de datos, con una vigencia determinada, y a la velocidad más rápida haciendo nuestro *mejor esfuerzo ("best effort")*, una vez alcanzado el volumen de datos del producto contratado para un usuario final éste de acuerdo con su paquete puede contratar un nuevo producto y/o contratar un producto de consumo excedente que incluye un volumen de datos a velocidad reducida de 512 kbps. En todos los casos, el tráfico de datos incluye el acceso a cualquier contenido, aplicación o servicio en Internet en términos no discriminatorios. Los productos ofrecidos a los usuarios finales se encuentran previamente configurados a su lanzamiento comercial por nuestro proveedor de acceso a la red.

Las ofertas y tarifas respectivas de los servicios de telefonía e Internet al Hogar y/o cualquier otra se brindan de conformidad con las estructuras tarifarias y promociones registras ante el IFT. Estas se utilizan para proporcionar los servicios de telefonía e Internet al Hogar en términos de la oferta contratada, a efecto de asegurar la calidad de los servicios.

De no llevar a cabo esta práctica, se podría saturar la red y poner en riesgo el cumplimiento de los términos y condiciones de calidad de las ofertas de referencia y afectar a los usuarios de la red.

5. Calidad y Gestión de congestión.

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

La calidad de los servicios puede verse afectada por una mayor demanda de tráfico o de usuarios finales de la originalmente prevista. A tal efecto, se debe reportar de manera regular las proyecciones de tráfico. Con la finalidad de mantener la integridad de la red y no afectar a otros clientes, por ello nuestro proveedor de acceso a la red podrá suspender las activaciones en una determinada región o localidad, sin responsabilidad alguna.

La gestión de congestión consiste en que nuestro proveedor de acceso a la red ajustará los parámetros técnicos en el servicio de Internet al Hogar, por lo que puede implementar una reducción de velocidad de hasta 2.5 Mbps 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 eNB/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 en la red de nuestro proveedor de acceso. 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 en perjuicio de los usuarios finales.

6. Bloqueo.

Nuestro proveedor de acceso a la red no lleva a cabo el bloqueo de tráfico de datos en los servicios de telefonía e Internet al Hogar que tengan contratados los usuarios finales.

7. Priorización pagada.

Nuestro proveedor de acceso a la red no ofrece el servicio de priorización pagada y no cuenta con una oferta para tal efecto.

8. Datos patrocinados.

Nuestro proveedor de acceso a la red ofrece datos patrocinados en los siguientes casos cuando se presta el servicio de acceso a Internet:

- Acceso gratuito a la URL http://educacionconequidad.sep.gob.mx (con IP 168.255.101.55) para el programa **Aprende en Casa**. Aplica cuando el usuario este usando el servicio en algunos de los nodos-celdas determinadas conforme a las zonas solicitadas por el gobierno, en un horario de lunes a viernes de 8 A.M. a 4 P.M. con velocidad reducida de hasta 300 kbps.

- Acceso gratuito a las siguientes URLs definidas para COVID con velocidad reducida de hasta 300 kbps.

    - https://coronavirus.gob.mx
    - alfa.gob.mx
    - servicios.gob.mx
    - api.gob.mx
    - http://aprendeencasa.sep.gob.mx

- http://www.aprende.edu.mx
- https://telesecundaria.sep.gob.mx
- https://educacionbasica.sep.gob.mx

- URLs de nuestra empresa para realizar la activación del producto en usuarios finales, en atención a usuarios sin costo, así como portales de pagos a velocidad de hasta 128Kbps.
- URLs de nuestra empresa con texto plano para gestión de usuarios finales.

Glosario.

CG-NAT: se refiere a Carrier Grade Network Address Translation.

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

DNS: se refiere a Domain Name System

eNB: se refiere a Evolved Node B

IFT: Instituto Federal de Telecomunicaciones

ISP: se refiere a Internet Service Provider

URL: se refiere a Uniform Resource Locator

9. Recomendaciones para prevenir riesgos de violación a la Privacidad y Comunicaciones Privadas.

A todos nuestros usuarios finales, se les hacen las siguientes recomendaciones con la finalidad de evitar que se pongan en riesgo sus datos personales y comunicaciones privadas:

1. VIGILA LAS DESCARGAS Y ARCHIVOS ADJUNTOS FRAUDULENTOS

- Ten cuidado a la hora de descargarte archivos de Internet, en especial aquellos ejecutables tipo "*.exe"*, ya que pueden contener código malicioso y dañar tu equipo.
- Recuerda que también puedes encontrarte con este tipo de amenazas en forma de archivo adjunto en un correo electrónico.
- El consejo básico es: Si te encuentras frente a un archivo que no esperas, de alguien que no corresponde o de procedencia desconocida, no lo abras y mándalo a la papelera de inmediato.

2. DUDA DE E-MAILS EXTRAÑOS, PHISHING Y SPAM

- Como decíamos, el correo electrónico es una de las principales vías de entrada de amenazas de seguridad. Nadie está exento de poder recibir un mensaje sospechoso;
- Por tanto, ante cualquier mail extraño elimínalo y no abras ni descargues el archivo adjunto. Si es verdaderamente importante, te volverán a contactar por otra vía;
- Sospecha especialmente de que estás ante algo anómalo si el e-mail está mal redactado, desconoces el remitente o la dirección es sospechosa o está incompleta, si está escrito en un idioma que no es con el que habitualmente te comunicas con ese interlocutor, si te piden dinero por correo (aunque el remitente asegure ser tu banco), etc.
- Si acabas aterrizando en una web en la que debes introducir tus datos, fíjate antes que es https y que el enlace es correcto. De lo contrario, podría tratarse de phishing. Siempre que puedas, intenta acceder directamente a esa web desde tu navegador y no después de haber hecho clic en un enlace de un email o de otra fuente sospechosa.

3. MANTÉN SIEMPRE TU SISTEMA OPERATIVO ACTUALIZADO

- Esto es muy importante a tener cuenta ya que, al igual que los malware evolucionan constantemente, tu SO también debería actualizarse al mismo ritmo.

- Las actualizaciones del sistema operativo de tus dispositivos suelen traer parches para solucionar problemas técnicos o brechas de seguridad.

4. HAZ UNA BUENA GESTIÓN DE TUS CONTRASEÑAS

- Suelen ser también otra de las grandes brechas de seguridad.
- Podemos cometer varios errores con las contraseñas: desde poner una fácil de descifrar (año de nacimiento, número de teléfono, matrícula del coche,123456...), a poner la misma contraseña para todos los sitios.
- Es importante tener una contraseña única para cada sitio, que sea robusta con multitud de caracteres y cambiarla de forma periódica.
- También puedes crear contraseñas mediante generadores de claves de forma aleatoria (en los que se incluyen números, símbolos, letras en mayúscula y minúscula, etc).
- Por último, te recomendamos guardar tu contraseña en un gestor de contraseñas que te ayuda a tener contraseñas complejas sin tener que recordarlas.

5. RECUERDA, TU MÓVIL O TABLET TAMBIÉN DEBEN ESTAR PROTEGIDOS Y SON TAN VULNERABLES COMO UN EQUIPO DE COMPUTO

- No pases por alto este aspecto. ¿A caso no utilizamos nuestros dispositivos móviles tanto o más que un ordenador de mesa o portátil?
- Debemos tener en cuenta que nuestro móvil o tablet pueden ser víctimas de un virus y por eso mismo, debemos extremar precauciones cuando los usemos para navegar por internet o realizar alguna compra online.
- Igualmente, también es recomendable la instalación de un sistema antivirus que garantice el pago seguro y el acceso seguro a tu banca online.

6. USA LA CREACIÓN DE USUARIOS PARA DIFERENTES PERSONAS

- Si compartes un equipo con varias personas (en tu hogar u oficina de trabajo) es importante que crees cuentas de diferentes usuarios y configures los permisos según el principio de necesidad de saber: que cada usuario acceda a donde realmente necesita y no a lo de todos.
- Con ello, tus datos personales, historial de navegación, archivos, etc., quedarán reservados solo para ti mismo. Si se vulnera la seguridad de otro usuario, tu información quedará mejor resguardada.
- Como es evidente, también se debe configurar una contraseña (con las indicaciones que te hemos dado anteriormente) distinta y segura para cada usuario.

7. ACTIVA EL FIREWALL O CORTAFUEGOS

- Se trata de una de las herramientas a la hora de proteger nuestro dispositivo por defecto, está disponible en todos los sistemas operativos y es fácil de configurar, pudiendo escoger el nivel de protección que cada uno desea en cada momento.

8. REALIZA SIEMPRE COMPRAS EN SITIOS SEGUROS

- Las compras online pueden ser también otra vía de entrada a amenazas de seguridad, ya que pueden robarte datos y dinero.
- El consejo: no compres nada en una tienda online que no te parezca de confianza. Revisa que sea un lugar certificado y fiable.
- Presta atención al certificado SSL de una web (representado con un símbolo de un candado en la barra de navegación), y a que la web desde la que vas a hacer la compra tiene un dominio 'https'

9. CUIDADO CON LOS DISPOSITIVOS IOT (INTERNET OF THINGS = INTERNET DE LAS COSAS)

- Altavoces, Smart TV, relojes y pulseras inteligentes... Estos dispositivos también conocidos como wearables (si se llevan puestos) o dispositivos IoT (en general) pueden ser susceptibles de ser hackeados, pues ya se han dado casos de hackeos, filtraciones y escuchas a través de los mismos.
- El consejo es que siempre sigas las instrucciones del fabricante y actualices el sistema cuando sea necesario para evitar que pasen "cosas raras".
- La innovación tiene cosas positivas pero suele ir asociada a mayores riesgos ya que tienen menos medidas de seguridad por defecto. De ahí que en las empresas u organizaciones más innovadoras, necesiten de expertos en Ciberseguridad en IoT.

10. REVISA LAS APP Y EXTENSIONES AUTORIZADAS

- Mucho cuidado con extensiones del tipo "ver quién me ha dejado de seguir" o juegos de Facebook porque, de ortorgarles permisos a dichas extensiones, podemos estar expuestos a un filtrado de nuestros datos.
- Registrarse en webs o App con nuestros perfiles de Facebook, Google+ o Twitter es más rápido pero estamos facilitando información de dichas redes. Normalmente esta acción no implica que estemos dando nuestra contraseña a la página pero debemos estar atentos a quien le facilitamos información personal y qué medidas de ciberseguridad realmente tiene esa web o App para protegerla.

11. REALIZA COPIAS DE SEGURIDAD

- Ante cualquier riesgo o amenaza de ver comprometidos nuestros archivos (por robo o por daño), es interesante contar con una solución de *respaldo*.
- Realiza copias de seguridad de forma permanente, son la única medida eficaz (y gratis) en caso de que sufras un cibersecuestro de tu dispositivo (Ransomware).

12. CIERRA SESIÓN, SOBRE TODO EN SITIOS PÚBLICOS

- ¿Dejarías la puerta de tu casa abierta o las llaves de tu coche puestas? Bueno, depende del país en el que residas quizás no te ocurra nada, pero en lo que a Ciberseguridad se refiere, nunca dejes la sesión abierta en un ordenador público (de la oficina, de una biblioteca...). Recuerda cerrar todas las sesiones antes de desconectarte y apagar el ordenador.
- Asegúrate que no está seleccionada la opción de "Recordar contraseña", ya que aunque salgas de la sesión, cualquier que utilice dicho dispositivo podrá acceder de nuevo a tu sesión sin necesidad de conocer la contraseña.

13. SOSPECHA SIEMPRE DEL WIFI DEL AEROPUERTO (O DE CUALQUIER SITIO PÚBLICO)

- El cartel del "WiFi gratis" puede ser un gran reclamo para ti, pero también para quien intente quedarse con tus datos.
- Intenta evitar conectarte a una red abierta. Si no te queda otra, evita por encima de todo acceder a datos sensibles (bancos, correos, insertar contraseñas de redes sociales, etc). Todos los datos que circulen por esa red son plenamente visibles.
- Valora utilizar una conexión VPN (RED PRIVADA VIRTUAL) para que la información que transmitas vaya cifrada de punto a punto.

14. SI NO ESTÁS USANDO INTERNET, APÁGALO

- Si no estás usándolo, desconéctalo y reducirás posibilidades de sufrir un ataque informático. Tan sencillo como apagar el router o pulsar el botón de 'modo avión' y asegurarte una desconexión (casi) total de redes.

Aunado a las recomendaciones antes señaladas, y para complementar la información de protección en beneficio de nuestros usuarios a continuación les proporcionamos una ligas en las que se pueden revisar algunas recomendaciones que hace el Instituto Federal de Telecomunicaciones en materia de privacidad y seguridad en las comunicaciones privadas:

http://www.ift.org.mx/sites/default/files/contenidogeneral/usuarios-y-audiencias/informepoliticasdeprivacidad150520final.pdf

http://www.ift.org.mx/usuarios-y-audiencias/enemigos-de-tu-ciberseguridad

http://www.ift.org.mx/usuarios-y-audiencias/enemigos-publicos-del-celular

http://www.ift.org.mx/usuarios-y-audiencias/ciber-club-ift