CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE RED (ARTÍCULO 12 DE LOS LINEAMIENTOS PARA LA GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE LA RED)

El presente documento tiene como propósito informar a los usuarios del servicio de acceso a internet de YONDER MEDIA MOBILE MEXICO, S. DE R.L. DE C.V. (en lo sucesivo YONDER MEDIA MOBILE MEXICO) sobre sus derechos como usuarios de este servicio, en términos de la Ley Federal de Telecomunicaciones y Radiodifusión, y en 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 ("Políticas" y/o "Lineamientos") publicados el 05 de julio de 2021 en el Diario Oficial de la Federación. conforme a lo siguiente:

La presente Política de Gestión de Tráfico y Administración de Red de YONDER MEDIA MOBILE MEXICO está en todo momento encaminada a asegurar la calidad, capacidad y velocidad del servicio de acceso a Internet, así como a preservar la integridad y seguridad de la red.

El tráfico de datos sobre la cobertura ofrecida por YONDER MEDIA MOBILE MEXICO opera bajo esquema best effort, es decir, se ofrece la mejor calidad de servicio en el momento de conexión, en el entendido de que ésta puede variar por la demanda del servicio.

GLOSARIO

CG-NAT: se refiere a Carrier Grade Network Address Translation.
USUARIO: Concesionario de servicios de telecomunicaciones o comercializadora, que celebra un contrato con YONDER MEDIA MOBILE MEXICO, por virtud del cual utiliza la capacidad, infraestructura o servicios mayoristas de telecomunicaciones a través de la red del mayorista.
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 Aquellos concesionarios y autorizados que proporcionana los usuarios finales el servicio de acceso a Internet a través de una red pública de telecomunicaciones.
URL: se refiere a Uniform Resource Locator

1. DERECHOS DE LOS USUARIOS.

1.1 LIBRE ELECCIÓN.

El servicio de acceso a Internet que ofrece YONDER MEDIA MOBILE MEXICO permite que los usuarios 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 de referencia aprobadas a YONDER MEDIA MOBILE MEXICO por el Instituto Federal de Telecomunicaciones.

1.2 TRATO NO DISCRIMINATORIO.

YO MOBILE MEXICO se obliga a tratar de la misma manera el tráfico de los contenidos, aplicaciones o servicios de tipo similar en Internet entre los usuarios, absteniéndose de obstruir, interferir, inspeccionar, filtrar o discriminar contenidos, aplicaciones o servicios.

1.3 PRIVACIDAD Y SEGURIDAD SE LAS COMUNICACIONES.

A nivel técnico, YONDER MEDIA MOBILE MEXICO se encuentra obligado a asegurar la inviolabilidad de las comunicaciones privadas de los usuarios a través de la red de YONDER MEDIA MOBILE MEXICO y su privacidad. YONDER MEDIA MOBILE MEXICO no utiliza las técnicas de DPI/DFI para monitoreo de tráfico.

1.4. GESTIÓN DE TRÁFICO BASADA EN VOLUMEN DE DATOS CON UNA VIGENCIA DETERMINADA.

Consiste en ofrecer a los usuarios de YONDER MEDIA MOBILE MEXICO un volumen de datos con una vigencia determinada a velocidad best effort, una vez alcanzado el volumen de datos del producto contratado para un usuario final el Cliente puede contratar un nuevo producto y/o contratar un producto de consumo excedente con velocidad best effort de la misma manera.

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 en las ofertas de referencia por YONDER MEDIA MOBILE MEXICO se encuentran previamente configurados a su lanzamiento comercial. Aplica en las ofertas de referencia respectivas del

servicio de movilidad de conformidad con las estructuras tarifarias y promociones registradas ante el IFT.

Se utiliza para proporcionar el servicio de movilidad 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.

1.5. CALIDAD Y GESTIÓN DE CONGESTIÓN.

YONDER MEDIA MOBILE MEXICO garantiza la calidad del servicio de movilidad, por lo cual ofrece a sus usuarios 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 YONDER MEDIA MOBILE MEXICO.

La calidad del servicio puede verse afectada por una mayor demanda de tráfico o de usuarios finales de la originalmente prevista. Con la finalidad de mantener la integridad de la Red Compartida y no afectar a otros clientes, YONDER MEDIA MOBILE MEXICO podrá suspender las activaciones en una determinada región o localidad, sin responsabilidad alguna para YONDER MEDIA MOBILE MEXICO.

La gestión de congestión consiste en que YONDER MEDIA MOBILE MEXICO ajustará los parámetros técnicos en el servicio de movilidad, 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 eNB/sector.

Se utiliza para preservar la operación y calidad de la red, de tal manera que se garantice la mejor experiencia de los usuarios de YONDER MEDIA MOBILE MEXICO. 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.

1.6. DESARROLLO SOSTENIDO DE LA INFRAESTRUCTURA.

YONDER MEDIA MOBILE MEXICO, analizará y en su caso aplicará las acciones necesarias que le permita el crecimiento sostenido de la infraestructura de telecomunicaciones, de conformidad a lo propuesto por el IFT con la finalidad de promover un funcionamiento más eficiente y competitivo en el mercado de las telecomunicaciones.

1.7. TRANSPARENCIA.

YONDER MEDIA MOBILE MEXICO pone a disposición de sus usuarios, a través de su página de Internet la información relativa a la prestación de sus servicios, contenidas en el presente Código de Políticas de Gestión y Administración de Red.

1.8. INFORMACIÓN.

BLOQUEO
YONDER MEDIA MOBILE MEXICO no lleva a cabo el bloqueo de tráfico de datos en el servicio de movilidad que tengan contratados sus usuarios.

PRIORIZACIÓN PAGADA
YONDER MEDIA MOBILE MEXICO no ofrece el servicio de priorización pagada y no cuenta con una oferta de referencia para tal efecto.

2. POLÍTICAS

A continuación, se detallan las Políticas que utilizará YONDER para la eficiente prestación del Servicio, consistentes en:

2.1 Optimización del Tráfico.

Son acciones que realiza YONDER MEDIA MOBILE MEXICO con el objeto de mejorar la experiencia de navegación del usuario en coordinación con el Concesionario PSI, como la administración del tráfico o gestión de ancho de bandas de los medios, mismas se traducen en un uso más eficiente de la red. Además, beneficiará la operación de la red, ya que disminuirá la posibilidad de escenarios de congestión de tráfico, altas latencias y altos costos operativos en la red.

2.2 Administración de las Direcciones IP.

Una dirección IP es una dirección única que identifica a un dispositivo en Internet o en una red local; es un identificador que permite el intercambio de información en Internet. Las direcciones IP son asignadas por el organismo internacional, Internet Assigned Numbers Authority, quien administra dichas direcciones de manera eficiente para permitir el acceso a Internet de todos los usuarios a nivel global de manera equitativa.

La implementación de lo anterior generará:

• Ocupación adecuada de las direcciones IP públicas; y
• Disponibilidad de las direcciones IP públicas.

2.3 Administración de tráfico en casos de congestión.

El PSI podrá llevar a cabo acciones para la optimización del tráfico en caso de saturación de la red, haciendo uso adecuado de los recursos disponibles en un momento y ubicación determinados. Particularmente, ante situaciones que pudieran comprometer la calidad del Servicio.

Al implementarse la prestación del Servicio podría ser (sin intermitencia y baja latencia), entre otros.

3. RECOMENDACIONES AL USUARIO FINAL.

A continuación, se enlista una serie de recomendaciones para realizar una navegación más segura:

PROGRAMA DE SEGURIDAD EN INTERNET: Es valioso asegurarse que los equipos a través de los que accede al Servicio, cuenten con un programa (conocidos como navegadores o web browsers) que brinde protección al navegar en Internet, el cual incluya un antivirus actualizado a fin de prevenir ataques de programas maliciosos que puedan afectar al equipo o bien, sustraer información personal y/o confidencial; así como herramientas para prevenir anuncios no deseados; accesos no deseados o conexiones en segundo plano; seguimiento y almacenamiento de contraseñas, tecleo o información de tarjetas de crédito (Keylogger, Password Sniffing); obtención de información personal y/o confidencial (Phishing), entre otros.

EVITAR NAVEGACIÓN EN SITIOS NO CONOCIDOS: Al navegar en Internet asegúrate de validar que el sitio, servicio, contenido o aplicación visitado/utilizado cuente con certificados de seguridad y sellos de confianza emitidos por auditores y certificadores reconocidos.
Te recomendamos instalar complementos para navegadores web o aplicaciones móviles, así como, revisar las opciones de seguridad y privacidad del navegador que usas.

PROPORCIONA INFORMACIÓN SOLO CUANDO ESTÉS SEGURO: Recomendamos no proporcionar datos personales, números de cuenta, tarjetas bancarias, números telefónicos, NIP de seguridad, tokens, códigos de seguridad de tarjetas, entre otros, a menos de que estés plenamente convencido de la autenticidad del sitio y que las finalidades de uso sean las pertinentes. De igual forma, te recomendamos no proporcionar ni compartir información sensible (tarjetas de crédito, números confidenciales, contraseñas, pines, tokens, imágenes, fotografías etc.) en Internet que contenga información confidencial.

CONTROL PARENTAL: Instala y utiliza herramientas de control parental para monitorear y controlar las actividades de los menores de edad cuando hagan uso de Internet.

CONFIGURACIÓN DE PRIVACIDAD EN REDES SOCIALES: Revisa la configuración de seguridad en las redes sociales que uses y evita compartir información personal y/o confidencial.

DESCARGA PROGRAMAS INFORMÁTICOS: (software) y aplicaciones de sitios oficiales y confiables.

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.

Te sugerimos que, 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.

DUDA DE E-MAILS EXTRAÑOS, PHISHING Y SPAM

El correo electrónico es una de las principales vías de entrada de amenazas de seguridad, existe la posibilidad de recibir un mensaje sospechoso. Por tanto, ante cualquier mail extraño elimínalo y no abras ni descargues el archivo adjunto.
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).

Si te encuentras 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.

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.

HAZ UNA BUENA GESTIÓN DE TUS CONTRASEÑAS

Se recomienda hacer uso de contraseñas seguras que tengan al menos 8 caracteres. Te sugerimos utilizar una combinación de números, letras mayúsculas, minúsculas y símbolos. Cambia tu contraseña de manera frecuente.

Las contraseñas suelen ser también otra de las grandes brechas de seguridad, es importante tener una contraseña única para cada sitio, que sea robusta con multitud de caracteres y cambiarla de forma periódica.

Evita poner una contraseña fácil de descifrar (año de nacimiento, número de teléfono, 123456...), a poner la misma contraseña para todos los sitios.

Por último, te recomendamos guardar tu contraseña en un gestor de contraseñas que te ayuda a tener contraseñas complejas sin tener que recordarlas.

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

Considera que el teléfono 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, se recomienda la instalación de un sistema antivirus que garantice el pago seguro y el acceso seguro a tu banca online.

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 configurando una contraseña distinta y segura para cada usuario. Asimismo, configures los permisos según el principio de necesidad de saber que cada usuario acceda a donde realmente necesita y no a lo de todos, así 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.

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.

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.

Te sugerimos, no comprar 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'

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.

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.

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 backup.

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).

CIERRA SESIÓN, SOBRE TODO EN SITIOS PÚBLICOS.

Nunca dejes la sesión abierta en un ordenador público (de la oficina, de una biblioteca, cualquier lugar público) 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.

SOSPECHA SIEMPRE DEL WIFI DE CUALQUIER SITIO PÚBLICO.

Intenta evitar conectarte a una red abierta. Si no te queda otra opción, 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 para que la información que transmitas vaya cifrada de punto a punto.

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 unas 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:

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

https://ciberseguridad.ift.org.mx/

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

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

4. MARCO LEGAL APLICABLE

- Ley Federal de Telecomunicaciones y Radiodifusión

- 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.

5. ÚLTIMA ACTUALIZACIÓN: AGOSTO 2023.