Código de Políticas de Gestión de Tráfico y Administración de Red

El presente documento tiene como objetivo informar a los usuarios de acceso a internet de Viasat sobre sus derechos; de las políticas de gestión de tráfico y administración de la red de Viasat, que permiten garantizar la calidad del servicio, así como la integridad de la red. Asimismo, hacemos del conocimiento de los clientes de Viasat una serie de recomendaciones para fomentar la navegación segura, así como para la protección de los menores.

Derechos de los usuarios finales del servicio de acceso a Internet

Libre elección.

Los usuarios de los servicios de acceso a Internet podrán acceder a cualquier contenido, aplicación o servicio ofrecido por Viasat o por los autorizados a comercializar, dentro del marco legal aplicable, sin limitar, degradar, restringir o discriminar el acceso a los mismos.

Viasat no podrá limitar el derecho de los usuarios del servicio de acceso a Internet a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos que se conecten a su red, Viasat únicamente requerirá que éstos se encuentren homologados;

No discriminación.

Viasat como prestador del servicio de acceso a Internet se abstendrá de obstruir, interferir, inspeccionar, filtrar o discriminar contenidos, aplicaciones o servicio;

Privacidad.

Viasat preservará la privacidad de los usuarios y la seguridad de la red. Para obtener más información sobre las prácticas de privacidad de Viasat, consulte la política de privacidad aplicable a su servicio disponible en https://www.viasat.com/es-mx/privacidad/.

Transparencia e información.

Viasat como es su obligación publica en su página de Internet la información relativa a las características del servicio ofrecido, incluyendo las políticas de gestión de tráfico y administración de red autorizada por el Instituto, velocidad, calidad, la naturaleza y garantía del servicio.

Gestión de tráfico.

Viasat podrá tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red conforme a las políticas autorizadas por el Instituto, a fin de garantizar la calidad o la velocidad de servicio contratada por el usuario, siempre que ello no constituya una práctica contraria a la sana competencia y libre concurrencia.

Calidad.

Viasat deberá preservar los niveles mínimos de calidad que al efecto se establezcan en los lineamientos respectivos, y

Desarrollo sostenido de la infraestructura.

Viasat en atención a los lineamientos respectivos emitidos por Instituto Federal de Telecomunicaciones deberá fomentar el crecimiento sostenido de la infraestructura de telecomunicaciones.

Políticas de Gestión de Tráfico

La red está diseñada para garantizar que los usuarios, en general, no experimenten congestión. En condiciones normales de tráfico, no es necesario que Viasat utilice prácticas de gestión de la congestión. Dicho esto, si bien la capacidad de la red es abundante, no es ilimitada. Debido a una demanda anormal en ciertos momentos, la Red puede experimentar un cierto nivel de congestión, lo que requiere las prácticas de gestión de congestión descritas en esta Política.

El objetivo de Viasat es gestionar su Red para minimizar el impacto de la congestión en el tráfico. Durante períodos de congestión, las aplicaciones que consumen mucho ancho de banda, como la transmisión de video y la descarga de archivos, pueden disminuir su velocidad más que otras aplicaciones. Como resultado, la calidad del flujo de video puede reducirse y / o puede producirse un almacenamiento en búfer. Además, las descargas de archivos pueden tardar más en completarse durante los períodos de congestión. En situaciones de congestión más severa, es posible que sea necesario disminuir la velocidad todas las aplicaciones y, en tales casos, la descarga de las páginas web puede llevar más tiempo.

Viasat no bloquea intencionalmente ninguna forma particular de tráfico; sin embargo, en el caso de los puertos comúnmente conocidos por contener paquetes de datos maliciosos que se consideran un riesgo para la seguridad de la red, Viasat puede bloquear estos puertos para proteger la red.

Además, Viasat utiliza otras técnicas diseñadas para prevenir o reducir de manera preventiva los períodos de congestión de la red, mejorar la experiencia del usuario, mejorar la seguridad y mejorar la confiabilidad de la red. Por ejemplo, según el tipo de servicio que esté recibiendo, Viasat trabaja activamente para: (i) reducir la calidad de transmisión de video a resoluciones óptimas según el tipo de dispositivo utilizado para transmitir video (por ejemplo, pero no limitado a, reducir la resolución del video en dispositivos que no necesitan una resolución de video de alta calidad, como dispositivos con pantallas pequeñas); (ii) suspender cuentas para bloquear las transmisiones salientes de spam; (iii) gestionar el riesgo de que virus, gusanos e intrusiones similares dañen la Red; (iv) frustrar ataques de negación de servicio; y (v) reducir el riesgo de que un intruso obtenga acceso al sistema informático de un suscriptor.

Política de Uso Justo

El servicio contratado a Viasat para el acceso a Internet puede incluir una limitación con respecto al volumen de datos incluidos en el plan o paquete adquirido. Durante la vigencia del plan o paquete de servicios, el usuario tendrá acceso a la red a la velocidad de transferencia establecida. De acuerdo con los términos y condiciones de cada plan o paquete de servicios, una vez que el usuario haya alcanzado el volumen de datos incluido en su compra, el usuario / suscriptor podrá seguir disfrutando del servicio de Internet con una reducción en la velocidad de transferencia.

Si se suscribe a un plan de servicio con navegación y chat ilimitados, después de alcanzar su límite de datos en su plan o paquete, continuará teniendo acceso a la mayoría de las páginas web y servicios de chat de texto a las velocidades de transferencia establecidas. El resto de la actividad de

Internet, como la actividad de Internet incorporada en páginas web, correo electrónico, transmisión de video, chat de video, audio y juegos en línea, tendrá una velocidad de descarga de 128 Kbps. El acceso a las páginas web y al chat cuenta para su límite de datos contratado.

Recomendaciones a los usuarios finales

Mantenga sus computadoras y dispositivos móviles actualizados.

Instale en sus dispositivos la última versión del sistema operativo, navegador web y las mejores defensas contra virus, malware y otras amenazas en línea.

Elija contraseñas seguras.

Mantenga contraseñas seguras para todas sus aplicaciones y dispositivos; si está disponible, elija la verificación en dos pasos, también conocida como autenticación en dos pasos, un método que agrega una capa adicional de seguridad para proteger sus cuentas.

Cambie sus contraseñas periódicamente e inmediatamente después de enterarse de un intento de obtener acceso ilegal a sus dispositivos o cuentas.

Tenga cuidado con las estafas de suplantación de identidad (phishing).

Los intentos de suplantación de identidad (phishing) son intentos por medio de correo electrónico o mensajes de texto para convencer al usuario de que proporcione información personal que permitirá a los estafadores acceder al correo electrónico y cuentas bancarias u otra información confidencial.

Estos mensajes parecen provenir de una organización confiable como un banco o una organización gubernamental.

Por lo general, por medio de una situación que requiere su acción inmediata, lo invitan a hacer clic en un enlace o abrir un archivo adjunto.

Cómo protegerse del phishing

1. Proteja su computadora con software de seguridad.
2. Proteja su teléfono móvil configurando el software para que se actualice automáticamente.
3. Proteja sus cuentas mediante la autenticación de más de un paso.
4. Proteja sus datos haciendo una copia de seguridad. Realice una copia de seguridad de sus datos y asegúrese de que esas copias de seguridad no estén conectadas a su red doméstica. Puede copiar los archivos de su computadora a un disco duro externo o almacenamiento en la nube. También haga una copia de seguridad de los datos de su teléfono.

No haga pública su información personal.

Los piratas informáticos (hackers) buscan en las redes sociales información personal en los perfiles de usuario para descubrir contraseñas y posibles respuestas a preguntas de seguridad que puedan utilizarse para obtener acceso a sus cuentas. Evite publicar datos personales como cumpleaños, direcciones, etc. que puedan usarse para robar su identidad.

Tenga cuidado con los sitios web que visita.

Los sitios web que le permiten descargar imágenes, películas y aplicaciones gratuitas pueden contener trampas de software espía; compruebe la reputación de esos sitios antes de que su computadora o teléfono se infecte.

Compra de forma segura.

Antes de comprar en línea, asegúrese de que el sitio web utilice tecnología segura, verifique siempre que la dirección web comience con htpps y que el candado que aparece en la pantalla esté cerrado.

Lea las políticas de privacidad del sitio.

La política de privacidad le dice al cliente cómo el sitio protege y usa la información personal que recopila. Si no está de acuerdo o no comprende la política de un sitio, busque un sitio alternativo.

Marco legal aplicable

Ley Federal de Telecomunicaciones y Radiodifusión, artículo 145

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.

Última actualización:

Noviembre 2021.

Versión:1.0