CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE RED

SISTEMAS Y REDES DE MONITOREO S. A. DE C. V., ("SISTEMAS Y REDES DE MONITOREO S. A. DE C. V.") a fin de dar cumplimiento con lo establecido en la Ley Federal de Telecomunicaciones y Radiodifusión ("LFTR") y con base en los Lineamientos para la gestión de tráfico y administración de red a los cuales deberán sujetarse los concesionarios y autorizados que presten el servicio de acceso a Internet, presenta el siguiente Código de Políticas de Gestión de Tráfico y Administración de Red ("Código"), el cual informa a los usuarios finales (personas físicas o morales que contraten el servicio), las medidas implementadas para la gestión de tráfico así como sus derechos y las características obligatorias que como Prestadora de Servicios de Internet ("PSI") debe de ofrecer.

Por lo tanto, en términos de lo establecido en la LFTR los usuarios de SISTEMAS Y REDES DE MONITOREO S. A. DE C. V. tienen derechos que deben cumplirse.

1. – DERECHOS DE LOS USUARIOS

El servicio se sujetará a los principios señalados en el artículo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión:

I. Libre elección:

Los usuarios de SISTEMAS Y REDES DE MONITOREO S. A. DE C. V. tienen el derecho de acceder (según sea su esquema de contratación y pago) a cualquiera de los contenidos, aplicaciones y servicios que se encuentren disponibles en Internet, evitando con esto la fragmentación del mismo, esto quiere decir que en ningún caso SISTEMAS Y REDES DE MONITOREO S. A. DE C. V. como proveedor, podrá limitar, restringir, discriminar, obstruir, degradar, interferir, filtrar o bloquear el acceso a contenidos, servicios y aplicaciones a los usuarios finales, exceptuando aquellas situaciones catalogadas como indispensables (todas aquellas que representen un riesgo para la salud o sus comunicaciones entre otras y que por su naturaleza solo se haría un bloqueo de manera temporal).

Este derecho de los usuarios está relacionado con los dispositivos que estos elijan para acceder al uso de su servicio de Internet, por lo tanto, es primordial que estos comprueben que sus equipos reúnan las características técnicas necesarias para utilizar el servicio y acceder a él de una manera óptima, este último punto es responsabilidad del usuario.

II. No discriminación:

SISTEMAS Y REDES DE MONITOREO S. A. DE C. V. cumplirá con el

compromiso de no generar tratos discriminatorios entre usuarios finales, proveedores de aplicaciones, contenidos y servicios, tipos de tráficos similares, así como entre el tráfico propio y el de terceros que curse por la red de telecomunicaciones, con independencia del origen o destino de la comunicación. Por lo tanto, no priorizará o dará preferencia a contenidos, aplicaciones y/o servicios específicos.

III. Privacidad:

SISTEMAS Y REDES DE MONITOREO S. A. DE C. V. garantizará la seguridad de la red, a todos los usuarios, para asegurar la inviolabilidad y privacidad de sus comunicaciones privadas, por lo tanto, se compromete a no monitorear el contenido del tráfico que transita por su red, así como no almacenar información de los usuarios finales que no sea previamente autorizada y necesitada para proveer el servicio.

IV. Transparencia e información:

SISTEMAS Y REDES DE MONITOREO S. A. DE C. V. publicará de manera oportuna toda la información que describa el servicio ofrecido (calidad, velocidad, naturaleza, garantía, vigencia del servicio etc.…) esto incluirá las políticas de administración de red previamente autorizadas por el IFT, así como la gestión de tráfico.

V. Gestión de tráfico:

SISTEMAS Y REDES DE MONITOREO S. A. DE C. V. utilizará las medidas necesarias para el cumplimiento de las políticas de gestión de tráfico y administración de la red, estas políticas están enfocadas en garantizar la continuidad, velocidad, seguridad, capacidad y calidad del servicio contratado por el usuario. Estas políticas deben de abstenerse de caer en prácticas que afecten la sana competencia y libre concurrencia y estarán diseñadas para ayudar al usuario a tener la mejor experiencia en acceso y uso de su servicio.

VI. Calidad:

SISTEMAS Y REDES DE MONITOREO S. A. DE C. V. utilizará estrategias enfocadas a resguardar la operación y la calidad de la red con el fin de garantizar al usuario la mejor experiencia en el servicio, este se prestará en todo momento, haciendo atención a los niveles mínimos de calidad ofrecidos con base en la regulación aplicable en la materia.

VII. Desarrollo sostenido de la infraestructura:

El Instituto debe fomentar el crecimiento sostenido de la infraestructura de telecomunicaciones, con lo cual se promoverá un funcionamiento más eficiente y competitivo en el mercado de las telecomunicaciones a su vez, SISTEMAS Y REDES DE MONITOREO S. A. DE C. V. aplicará en su red los mismos parámetros para contribuir con el cumplimiento de su parte correspondiente en este crecimiento.

2. POLÍTICAS DE ADMINISTRACIÓN DE TRÁFICO Y ADMINISTRACIÓN DE RED

I. Asignación de direcciones IP privadas e IP públicas:

Una dirección IP es una dirección única que identifica a un dispositivo en Internet o en una red local, es decir, es un identificador que permite el intercambio de información en Internet, la asignación de IP privadas IPV4 se usa de manera conjunta con IP públicas para proporcionar al equipo terminal del usuario el acceso a Internet, las IP privadas se asignan al usuario para que tenga acceso a la red interna y las IP públicas son las que permiten el acceso a internet. Las IPs privadas IPv4 son asignadas a los usuarios a través de un NAT hacia IP públicas. Se ofrece como servicio adicional a los usuarios que necesiten contratar IPs públicas IPv4 fijas o exclusivas. La ventaja de tener una IP privada es que los usuarios estarían protegidos de ataques desde el internet, lo que no sucede con los usuarios de IP públicas fijas o exclusivas, ya que sus equipos pueden ser vistos desde internet. Sin la implementación de esta política seria imposible tener acceso al servicio de Internet.

II. Optimización de tráfico:

Con la finalidad de mejorar la experiencia del servicio y por ende la navegación del usuario, SISTEMAS Y REDES DE MONITOREO S. A. DE C. V. implementa diversas operaciones que ayudan a mejorar el uso de la red, estas pueden ir desde la gestión de ancho de bandas, administración de tráfico, almacenamiento temporal del contenido, entre otras. Estas acciones se realizan especialmente en los periodos de congestión de la red para preservar el ambiente que promueva una mejor experiencia para el usuario, basándose en la priorización del tipo

de tráfico que exista para optimizar el desempeño de los recursos a los que los usuarios acceden. Sin la implementación de esta política los usuarios tendrían una afectación generalizada en su servicio de Internet.

III. Administración de tráfico en casos de congestión:

SISTEMAS Y REDES DE MONITOREO S. A. DE C. V. realizará estrategias para el máximo aprovechamiento del tráfico en caso de que exista una saturación en la red, para ello tendrá que hacer un uso adecuado de los recursos disponibles, particularmente, ante situaciones que pudieran comprometer la calidad del Servicio.

IV. Bloqueo:

SISTEMAS Y REDES DE MONITOREO S. A. DE C. V. no implementa el bloqueo de tráfico de datos en los servicios, soló realiza prácticas de bloqueo de manera temporal en equipos que causen afectaciones en la red, en los servicios, o en las condiciones de seguridad en la Red Core.

De no implementar esta práctica, se podría saturar la red y poner en riesgo el cumplimiento de los términos y condiciones ofertados previamente al usuario. El bloqueo es la técnica que impide el acceso de los usuarios finales a un sitio web determinado o la utilización de un tipo de contenido o servicio particular, ya sea de manera temporal o permanente.

3. RECOMENDCIONES A USUARIOS

Las recomendaciones para que los usuarios finales minimicen los riesgos los riesgos que vulneren su privacidad, así como la de sus comunicaciones privadas son las siguientes:

1. Utilizar navegadores que cuenten con identificadores para ataques de phishing.

2. Utilizar equipos y software que estén actualizados en sus últimas versiones e instalar continuamente parches de seguridad en sistemas operativos y aplicaciones.

3. Utilizar un antivirus actualizado en los equipos con los que se acceda a la red global de internet.

4. Observar los enlaces y páginas que se pretenden abrir de tal forma que, se evite acceder a sitios que se vean sospechosos o que no sean confiables o donde se solicite información confidencial, personal o sensible.

5. Verificar que se está navegando en sitios web seguros y verificar que se tengan candados de seguridad tipo HTTPS://.

6. Evitar dar clic en correos electrónicos no solicitados o que provengan de fuentes desconocidas.

7. Evitar hacer caso de mensajes cuyo contenido sea atractivo, de urgencia o exagerado, por ejemplo, adjudicación de premios provenientes de concursos donde el usuario no participó.

8. Minimizar el registro con datos personales y evitar revelar contraseñas con sitios web que realmente utilice o frecuente, por ejemplo, correos electrónicos, banca electrónica, servicios públicos o cualquier otro.

9. Utilizar herramientas que permitan un borrado seguro de información en los equipos de cómputo que sean desechados por el usuario.

10. Actualizar periódicamente las contraseñas de sistemas y/o aplicaciones para prevenir que usuarios no autorizados tengan acceso a la información de los usuarios.

11. Utilizar contraseñas seguras haciendo uso de mayúsculas, minúsculas, caracteres y números en conjunto y en combinación.

12. Habilitar doble factor de autenticación en aquellos sitios en donde sea posible.

13. De ser necesario, comunicarse directamente con la institución a través de la información de contacto publicada en sitios oficiales.

14. Utilizar las páginas de origen de bancos e intermediarios de pago y nunca desde una liga.

15. Evitar dar clics o ingresar a ligas desconocidas o que no fueron solicitadas.

16. En caso de compartir el servicio y los equipos proveedores de internet con menores de edad, utilizar herramientas de control parental que ayuden a limitar y monitorear el contacto con riesgos en las actividades de los menores.

17. Hacer uno de la configuración de privacidad que ofrecen los sitios web visitados, así como leer y analizar las condiciones de uso de los servicios adquiridos.

18. Utilizar programas y aplicaciones oficiales ya sean adquiridos o de manera gratuita, así como revisar los permisos y accesos que estos requieran.

4. MARCO LEGAL APLICABLE

El presente Código se apega a lo establecido en el Artículo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión, así como 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, publicados en el Diario Oficial de la Federación el 5 de julio de 2021 y expedidos por el Instituto Federal de Telecomunicaciones.