CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO Y ADMINISTRACIÓN DE RED.

ENERGYNET

ENERGYNET SOLUCIONES Y REDES, S.A.S DE C.V.

ÍNDICE

OBJETIVO

El presente Código de Políticas de Gestión de Tráfico y Administración de Red tiene como objetivo principal poner a la disposición de los usuarios finales el conjunto de actividades, técnicas y procedimientos que el concesionario **ENERGYNET SOLUCIONES Y REDES, S.A.S DE C.V.** con nombre comercial **ENERGYNET,** utiliza para la operación y aprovechamiento de su red pública de telecomunicaciones así como del manejo, tratamiento y procesamiento del flujo de tráfico que cursa dentro de la misma red, este tipo de acciones son necesarias para el manejo del tráfico de la red, dar cumplimiento a las condiciones de contratación de los servicios con el usuario final y hacer frente a problemas de congestión, seguridad de la red y de la privacidad, entre otros.

ENERGYNET SOLUCIONES Y REDES, S.A.S DE C.V. tiene como objetivo mantener la permanencia de los servicios, asegurar la libre elección de los suscriptores, trato no discriminatorio, privacidad e inviolabilidad de las comunicaciones; de igual forma, mantener la calidad, capacidad y velocidad de los servicios contratados con base a estándares nacionales e internacionales, buenas prácticas en la industria de telecomunicaciones y normatividad aplicable.

Asimismo, la implementación continua de gestión de tráfico y administración conlleva beneficios respecto al funcionamiento continuo y eficiente de la red, pues permite a salvaguardar la seguridad e integridad de su red pública de telecomunicaciones (por ej., ante ataques maliciosos que puedan en consecuencia vulnerar a **ENERGYNET SOLUCIONES Y REDES, S.A.S DE C.V.** y a la gama de servicios que ofrecen tanto a nivel mayorista como minorista), ofrecer distintas gamas de servicio dependiendo de las necesidades de los usuarios, así como garantizar los niveles de calidad de servicio que le son contratados.

Lo anterior con apego a lo señalado en los artículos 1, 2 fracción VII y 12 de 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* correlativo con el artículo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión.

CONCESIONARIO PRESTADOR DEL SERVICIO.

ENERGYNET SOLUCIONES Y REDES, S.A.S DE C.V. es titular de una concesión única para uso comercial emitido por el Instituto Federal de Telecomunicaciones para proveer servicios de telecomunicaciones y radiodifusión específicamente el servicio de acceso a internet, ofreciendo a los usuarios finales distintos paquetes de datos. Los servicios que brinda están debidamente autorizados por el Instituto Federal de Telecomunicaciones (en adelante IFT).

ENERGYNET SOLUCIONES Y REDES, S.A.S DE C.V. al implementar las políticas de gestión de tráfico y administración de red, puede situarse en casos fortuitos o de fuerza mayor que requieran de manera excepcional que se limite, degrade, restrinja, discrimine, obstruya, interfiera, filtre o bloqueé el acceso a los contenidos, aplicaciones o servicios, para asegurar con ello el funcionamiento, seguridad e integridad de la red, así como la prestación del servicio de acceso a Internet a los usuarios. Al respecto, se considera razonable y justificado que políticas que resulten en tales afectaciones puedan ser implementadas únicamente de manera temporal en las siguientes situaciones:

a) Cuando exista un riesgo a la integridad y seguridad de la red o a las comunicaciones privadas de los usuarios. Por ejemplo, ante ataques o situaciones técnicamente comprobables que impliquen la interrupción de la capacidad de comunicación del servicio de acceso a Internet o pretendan obtener información de la comunicación de los usuarios.
b) Cuando exista congestión excepcional y temporal, entendida como aquella de corta duración y que implica un incremento repentino en el número de usuarios o en el tráfico que transita por la red. Es relevante señalar que las congestiones temporales son distintas a aquellas que pueden presentarse en determinadas franjas horarias y de manera recurrente, las cuales pueden requerir de otros mecanismos de gestión e, incluso, ser un indicador de la necesidad de ampliar la capacidad de las redes para cumplir con la calidad contratada por los usuarios. Al respecto, es relevante reiterar que las acciones que tome **ENERGYNET SOLUCIONES Y REDES, S.A.S DE C.V.** ante una congestión temporal o

excepcional no podrán implicar que exista discriminación entre tipos de tráfico similares.

c) Cuando se presenten situaciones de emergencia y desastre, entendidas en términos de lo señalado en la Ley General de Protección Civil, que resulten en afectaciones a la red de **ENERGYNET SOLUCIONES Y REDES, S.A.S DE C.V.** Al respecto, se enfatiza que la aplicación de políticas que resulten en afectaciones al servicio de acceso a Internet podrá realizarse en tanto resulte indispensable para atender la situación.

Lo anterior, como ya se ha explicado, sin perjuicio de las obligaciones que deban cumplir los PSI respecto a otras disposiciones. El usuario final podrá recibir asesoría y atención mediante el número telefónico **783-153-00-08** asimismo podrá enviar sus preguntas al correo electrónico atencionaclientes@energynet.com.mx con atención las 24 horas del día los 365 días del año además de la información pública de los servicios que puede ser consultada en la página web Energynet.com.mx. Por otra parte, el domicilio de atención a clientes se ubica en Calle 3, sin número, Ejido Juan Lucas C.P. 92860, Municipio de Tuxpan, Veracruz de Ignacio de la Llave.

DERECHOS DE LOS USUARIOS FINALES DEL SERVICIO DE ACCESO A INTERNET

ENERGYNET SOLUCIONES Y REDES, S.A.S DE C.V. respetará en todo momento los derechos de los usuarios finales que consumen el servicio de acceso a internet dentro de su red pública de telecomunicaciones. Dichos derechos son aquellos que se enlistan a continuación:

I. **LIBRE ELECCIÓN.** El usuario final podrá acceder a cualquier contenido, aplicación o servicio ofrecido por el proveedor del servicio de internet dentro del marco legal aplicable, sin limitar, degradar, restringir o discriminar el acceso a los mismos. Los usuarios pueden acceder e intercambiar contenido y tráfico de manera abierta por internet, haciendo uso de dispositivos homologados en el país.

II. **NO DISCRIMINACIÓN.** El proveedor del servicio de internet se abstendrá de obstruir, interferir, inspeccionar, filtrar o discriminar contenidos, aplicaciones o servicio al usuario final, salvo en el caso que el mismo usuario solicite un servicio

adicional que provea dichas características (ej. bloqueo de contenidos, servicios y mecanismos de control parental, entre otros).

III. **PRIVACIDAD.** El proveedor del servicio de internet deberá preservar la privacidad del usuario final y la seguridad de la red. El proveedor cuenta con un Aviso de Privacidad donde el cliente puede conocer el procedimiento bajo el cual es tratada su información, conforme a la normatividad aplicable.

IV. **TRANSPARENCIA E INFORMACIÓN**. El proveedor del servicio de internet deberá publicar en su página de internet la información relativa a las características del servicio ofrecido como es la velocidad, calidad, la naturaleza y garantía del servicio así de indicar las políticas de administración de la red y gestión de tráfico.

V. **GESTIÓN DE TRÁFICO**. El proveedor del servicio de internet podrá tomar las medidas o acciones necesarias para la adecuada gestión de tráfico y administración de la red a fin de garantizar la calidad o la velocidad de servicio contratada por el usuario final, siempre que ello no constituya una práctica contraria a la sana competencia y libre concurrencia;

VI. **CALIDAD.** El proveedor del servicio de internet deberá preservar los niveles mínimos de calidad que al efecto se establecen dentro de los *Lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores del servicio fijo* emitidos por el IFT y publicados el día veinticinco de febrero de dos mil veinte así de las demás disposiciones administrativas y técnicas aplicables que emita o haya emitido la autoridad competente.

VII. **DESARROLLO SOSTENIDO DE LA INFRAESTRUCTURA**. En los lineamientos respectivos, el IFT fomentará el crecimiento sostenido de la infraestructura de telecomunicaciones, por lo tanto, el proveedor del servicio de internet se compromete a desarrollar, mantener vigente y operativa su red, basándose en la estrategia del negocio y en la disponibilidad física y técnica de dicha red, manteniendo en todo momento el objetivo de la satisfacción de sus clientes.

POLÍTICAS DE GESTIÓN Y ADMINISTRACIÓN DE TRÁFICO DEL PROVEEDOR DEL SERVICIO DE INTERNET

A continuación, se explicarán cada una de las políticas de gestión y administración de tráfico que **ENERGYNET SOLUCIONES Y REDES, S.A.S DE C.V.** aplica dentro de su red pública de telecomunicaciones con la finalidad de proveer un servicio eficiente y de calidad, siendo dicha explicación de fácil entendimiento para los usuarios finales.

GESTIÓN DE CONGESTIÓN / OPTIMIZACIÓN DE TRÁFICO	
CONCEPTO	Se trata de aplicar medidas de gestión del tráfico en áreas específicas de la red como respuesta a cambios imprevistos en el entorno de la red. Estas medidas son implementadas por los responsables de administrar los equipos centrales de la red, utilizando herramientas administrativas disponibles en el software. Una de estas técnicas consiste en generar reglas de prioridad basadas en direcciones IP
CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.	Los controles de congestión se aplican en los siguientes casos comunes: 1. Fallas técnicas en la red: Cuando ocurren problemas técnicos o interrupciones en la infraestructura de la red, se implementan los controles de congestión para mitigar los efectos adversos y mantener un flujo de datos estable. 2. Fluctuaciones imprevisibles en el flujo de tráfico de la red: Si hay un aumento inesperado en el consumo de datos por parte de los usuarios finales, lo cual genera congestión en la red, se utilizan los controles de congestión para equilibrar el tráfico y evitar interrupciones en el servicio. 3. Cualquier otra situación de funcionamiento incorrecto en la red o posibles escenarios de los casos mencionados anteriormente, con el objetivo de prevenir su aparición y minimizar sus impactos. La utilidad de los controles de congestión radica en equilibrar el tráfico en secciones específicas de la red, aliviando la congestión en las áreas afectadas y logrando un flujo de datos eficiente y estable en la red.

	Es importante destacar que la implementación de estos controles no implica el bloqueo o discriminación de contenido, aplicaciones o servicios de Internet. Su objetivo principal es optimizar el rendimiento y la estabilidad de la red, sin afectar el acceso a ningún tipo de contenido, aplicación o servicio en particular.
IMPACTO EN EL SERVICIO DE INTERNET AL USUARIO FINAL.	La falta de aplicación de controles de congestión en la red puede tener las siguientes consecuencias: 1. Posible reducción en la velocidad del servicio de acceso a Internet contratado por el usuario final: En momentos de congestión, la velocidad de conexión puede disminuir temporalmente, afectando la experiencia del usuario. Sin embargo, esta reducción suele ser de corta duración y se restablecerá rápidamente una vez que se resuelva la congestión. 2. La calidad del servicio permite priorizar el tráfico de diferentes servicios: La implementación de controles de congestión facilita la priorización del tráfico en la red, asegurando que los servicios más importantes lleguen al usuario final de manera eficiente. Esto mejora la productividad del cliente final al utilizar el servicio, ya que se garantiza un acceso fluido y sin interrupciones a los servicios críticos. En resumen, los controles de congestión en la red son importantes para evitar colapsos, mejorar la eficiencia del flujo de datos y priorizar los servicios esenciales para los usuarios finales, lo cual tiene un impacto positivo en la productividad y experiencia del cliente.
POSIBLES AFECTACIONES EN CASO DE NO APLICARSE	Si no se aplican los controles de congestión en la red, se pueden experimentar las siguientes afectaciones: A la red: - Colapso de la red: La falta de controles de congestión puede llevar a una expansión descontrolada de la congestión de datos en todas las secciones de la red. Esto puede provocar un colapso generalizado, con interrupciones del servicio e inestabilidad en la transmisión de datos.

	Al usuario final o en sus comunicaciones: - Reducción significativa de la velocidad de acceso a Internet: Sin controles de congestión, la saturación de datos en la red puede ocasionar una disminución considerable en la velocidad de acceso a Internet contratada por el usuario final. Esto significa que las actividades en línea, como la navegación web, la transmisión de contenido multimedia o la descarga de archivos, se verán considerablemente más lentas. - Posible falta de servicio: En situaciones de congestión extrema, donde los recursos de la red se encuentran completamente saturados, el acceso a Internet contratado por el usuario final puede llegar a ser nulo. Esto significa que el servicio puede volverse inaccesible, dejando al usuario sin conexión a Internet. En resumen, la falta de aplicación de controles de congestión puede llevar a un colapso en la red, lo cual afectaría negativamente la velocidad de acceso a Internet del usuario final y, en casos extremos, podría resultar en la falta de servicio.

BLOQUEO DE CONTENIDO	
CONCEPTO	Consiste en restringir o bloquear el acceso del usuario final a un sitio web específico, así como limitar el uso de ciertos tipos de contenido o servicios durante un período determinado.
CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.	La técnica de restricción de contenido se aplica en los siguientes casos: 1. A solicitud expresa y consentida del usuario final: El proveedor del servicio de Internet restringe el contenido específico indicado por el usuario. 2. Riesgo técnico comprobable para la integridad y seguridad de la red: Se restringe contenido, aplicación o servicio que represente un riesgo para la red, la privacidad y la seguridad de los usuarios finales. 3. Contenido considerado ilícito por autoridad competente: Se restringe contenido, aplicación o servicio identificado como

	ilícito por una orden legal emitida por una autoridad competente. En resumen, la restricción de contenido se aplica a petición del usuario, para proteger la integridad de la red y la seguridad de los usuarios, y para cumplir con la normativa legal.
IMPACTO EN EL SERVICIO DE INTERNET AL USUARIO FINAL.	Durante el período en el que persista la situación que dio origen al bloqueo, el usuario no podrá acceder al contenido, aplicación o servicio que ha sido bloqueado.
POSIBLES AFECTACIONES EN CASO DE NO APLICARSE	Si no se bloquea el contenido que pueda afectar la integridad y seguridad de la red, así como el contenido ilícito, se pueden producir las siguientes consecuencias: A la red: - Compromiso del tráfico de la red: El contenido no bloqueado puede perturbar y comprometer el flujo normal de tráfico dentro de la red. Esto puede conducir a la propagación de virus, malware u otras amenazas provenientes de dicho contenido, poniendo en riesgo la integridad y seguridad de la red en su conjunto. Al usuario final o en sus comunicaciones: - Fuga de datos privados: La falta de bloqueo de contenido peligroso puede aumentar el riesgo de que los datos privados de los usuarios finales se filtren o sean comprometidos. Esto podría resultar en la pérdida de información confidencial, como contraseñas, datos personales o información financiera. - Interceptación de comunicaciones: La ausencia de bloqueo de contenido ilícito puede facilitar la interceptación de las comunicaciones de los usuarios finales por parte de terceros no autorizados. Esto compromete la privacidad de las comunicaciones y puede exponer información sensible. En resumen, si no se bloquea el contenido que amenaza la integridad y seguridad de la red, así como el contenido ilícito, existe un riesgo tanto para la red en sí misma, con posibles infecciones y compromisos de seguridad, como para los usuarios finales, con la posibilidad de fuga de datos privados y la interceptación de sus comunicaciones.

PRIORIZACIÓN DE DATOS	
CONCEPTO	Se trata de la práctica de priorizar la transmisión de ciertos tipos de datos sobre otros en una red. Estas prioridades se establecen en base a consideraciones técnicas y su implementación generalmente recae en la decisión del proveedor del servicio de Internet.
CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.	Esta práctica se aplica de manera continua durante la provisión del servicio de Internet al usuario final. Su objetivo es lograr una transmisión de datos más eficiente sin degradar la calidad del resto del tráfico. Además, permite implementar funciones de balanceo de carga, mejorar la eficiencia en el funcionamiento de la red y brindar soluciones de seguridad.
IMPACTO EN EL SERVICIO DE INTERNET AL USUARIO FINAL.	En todo momento durante la provisión del servicio de Internet al usuario final, se implementa esta práctica con el objetivo de mejorar la eficiencia en la transmisión de datos sin afectar la calidad del resto del tráfico. Además, permite realizar el balanceo de carga, mejorar el rendimiento de la red y ofrecer soluciones de seguridad.
POSIBLES AFECTACIONES EN CASO DE NO APLICARSE	**A LA RED.** La falta de aplicación de esta práctica puede dar lugar a eventos de congestión en diferentes áreas de la red, lo que resultaría en un tráfico de datos deficiente. **AL USUARIO FINAL O EN SUS COMUNICACIONES.** Aunque inicialmente no afectaría la velocidad o calidad del servicio contratado por el usuario final, podría limitarse la calidad del servicio, lo que impediría que el usuario obtenga el máximo provecho y una experiencia óptima al utilizar los servicios proporcionados por el proveedor.

SEGURIDAD DE LA RED	
CONCEPTO	Esta práctica implica proteger y salvaguardar la seguridad e integridad de la red del proveedor de servicios de Internet mediante la implementación de técnicas informáticas. Esto se logra mediante la creación de políticas o reglas en el firewall (cortafuegos), con el objetivo de aislar a los clientes de posibles ataques tanto desde el exterior como desde el interior de la red.
CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.	Esta práctica se aplica para proteger la red del proveedor de servicios de Internet de ataques externos e internos que

	buscan perturbar su funcionamiento eficiente. Se utilizan técnicas informáticas, como reglas en el firewall, para evitar la alteración, degradación o corrupción de la red por virus, malware, spyware y ransomware. El proveedor trabaja para anular y eliminar los ataques, garantizando la seguridad de la red.
IMPACTO EN EL SERVICIO DE INTERNET AL USUARIO FINAL.	En caso de un ataque, es posible que la velocidad de navegación del usuario final disminuya o que no tenga acceso a cierto contenido, aplicación o servicio. Sin embargo, el proveedor del servicio de Internet se compromete a tomar todas las medidas necesarias para minimizar el tiempo de impacto. Se realizarán todas las acciones posibles para restaurar rápidamente la velocidad de navegación y restablecer el acceso al contenido afectado.
POSIBLES AFECTACIONES EN CASO DE NO APLICARSE	**A LA RED.** La falta de protección y seguridad de la red puede poner en riesgo el tráfico de datos, permitiendo la propagación de virus y afectando la estabilidad del servicio de Internet. **AL USUARIO FINAL O EN SUS COMUNICACIONES.** Como resultado, el usuario final puede experimentar una disminución en la velocidad de navegación y correr el riesgo de que terceros no autorizados accedan a sus datos privados y a sus comunicaciones.

¿QUÉ MEDIDAS IMPLEMENTA PARA GARANTIZAR LA SEGURIDAD DE LA RED?	Implementamos procedimientos tecnológicos, físicos y administrativos para proteger su información personal de la pérdida, mal uso, y del acceso, divulgación, alteración y destrucción no autorizada, tomando en cuenta los riesgos involucrados en el procesamiento y la naturaleza de la información personal.
¿CÓMO DETECTA INVASIONES EN SU RED?	En nuestro NOC contamos con un router de borde el cual reporta mediante un log de eventos que incluye ataques maliciosos a nuestra red, así como el intento de acceso no autorizado.

¿CUÁLES SON LAS RECOMENDACIONES LE DA A SUS CLIENTES PARA MANTENER LA PRIVACIDAD DE SUS DATOS?	Las recomendaciones para que los usuarios finales minimicen los riesgos a su privacidad y la de sus comunicaciones privadas son las siguientes: 1. Al conectarse a internet ser recomienda ocupar equipos y software que estén actualizados en sus últimas versiones e instalar parches seguridad en sistemas operativos y aplicaciones. 2. Utilizar contraseñas seguras, incluyendo mayúsculas, minúsculas, números y caracteres especiales. 3. Evitar ingresar a sitios desconocidos, que se vean sospechosas o que no sean confiables. 4. Minimizar el registro con datos personales en páginas web y aplicaciones que realmente utilice y le sean útiles. 5. Verificar que las páginas visitadas tengan el candado de seguridad tal como HTTPS://, especialmente si se envía información sensible como tarjetas de crédito. 6. Utilizar un antivirus actualizado en el dispositivo terminal que se utiliza para acceder a internet. 7. Cambiar las contraseñas de sus servicios en línea con frecuencia. 8. Evitar abrir y/o responder mensajes o correos de origen desconocido, sobre todo los que requieran sus datos personales.
¿CÓMO GARANTIZA LA PRIVACIDAD DE LOS DATOS DE SUS CLIENTES?	En nuestro router de bord se tiene implementado mediante software un Firewall, el cual no permite la entrada de información maliciosa o intentos no autorizados de acceso a la red.

RECOMENDACIONES PARA LOS USUARIOS FINALES CON LA FINALIDAD DE MINIMIZAR RIESGOS DE PRIVACIDAD

ENERGYNET SOLUCIONES Y REDES, S.A.S DE C.V. recomienda a sus usuarios finales, así como al público en general, a seguir las siguientes indicaciones para navegar dentro del internet con mayor seguridad y así obtener una protección más adecuada y amplia de nuestros datos personales.

Las recomendaciones son las que se detallarán a continuación:

1. No compartir información, no proporcionar contraseñas, y cambiar frecuentemente las contraseñas. Para impedir que invadan la privacidad del usuario o roben datos

importantes guardados sobre todo en las redes sociales y/o foros públicos en los que navegue.

2. *Evita acceder a contenidos, aplicaciones o servicios no confiables o de dudosa reputación.* Los sitios web que se encuentran dentro de la red de internet son susceptibles de encontrarse infectados o controlados por agentes externos que buscan acceder, robar e inclusive eliminar datos de tus dispositivos. Para evitar ser objeto de pérdida o robo de información, utiliza contraseñas o bloqueos en tus dispositivos por medio de códigos alfanuméricos, no accedas a contenido publicitario que contengan promociones gratuitas y accede a sitios programados con seguridad (dominio y protocolo HTTPS).

3. *Instala antivirus en tus equipos de navegación.* Debido a que existen diversos tipos de softwares maliciosos cuyo objetivo es impenetrar en tus dispositivos para extraer tu información privada, se recomienda la utilización de antivirus que son programas digitales que brindan una mayor seguridad y protección a tus equipos ante cualquier tipo de amenaza cibernética.

4. *Actualiza tu sistema operativo, programas y aplicaciones instaladas en tus dispositivos.* Los desarrolladores fabricantes de los programas y aplicaciones se encuentran constantemente reforzando la estabilidad, así como la seguridad del software con la finalidad de evitar vacíos de que puedan ser aprovechados por los atacantes para la obtención de información; de lo anterior se sugiere actualizarlos de manera periódica y así garantizar una adecuada protección a sus dispositivos, así como de su información.

5. *Respalda tu información.* En caso de algún daño que impida el acceso a la información dentro de un dispositivo, se recomienda que previo a dicho suceso efectúe una copia de seguridad o respaldo de sus datos dentro de algún medio de almacenamiento como puede ser un disco duro o por medio de servicio de la nube ofrecido por algún sitio web confiable.

MARCO LEGAL APLICABLE

- Constitución Política de los Estados Unidos Mexicanos, artículos 1,6,7,28 y demás aplicables.
- Ley Federal de Telecomunicaciones y Radiodifusión artículos 145, 146 y demás aplicables.
- 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.
- Lineamientos que fijan los índices y parámetros de calidad a que deberán sujetarse los prestadores del servicio fijo

VERSIÓN Y FECHA ÚLTIMA DE ACTUALIZACIÓN

Última actualización	07 de junio del 2023
Versión	**1.0**
Elaboró	**ENERGYNET SOLUCIONES Y REDES, S.A.S DE C.V.**