

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

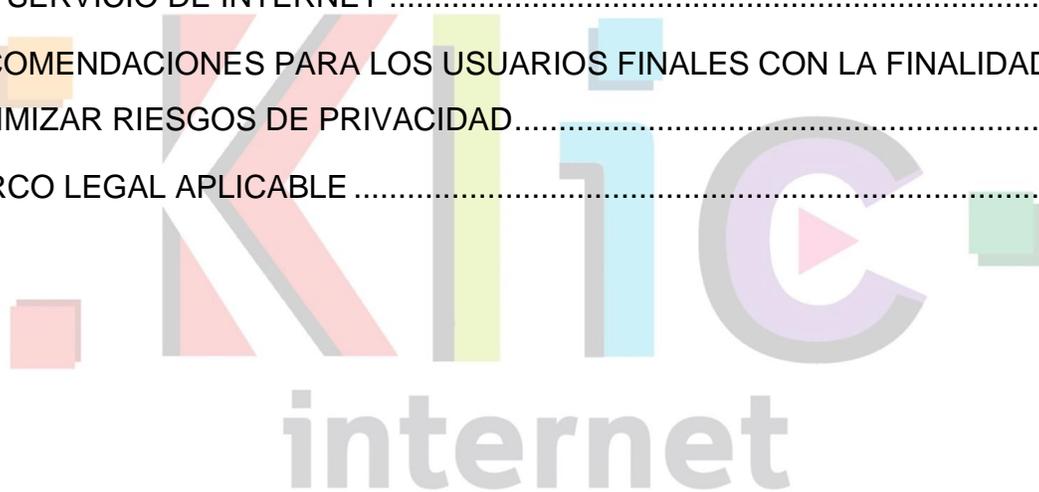


ERICK ZAUL MENA MUÑOZ



ÍNDICE

OBJETIVO.....	2
CONCESIONARIO PRESTADOR DEL SERVICIO.....	3
DERECHOS DE LOS USUARIOS FINALES DEL SERVICIO DE ACCESO A INTERNET	4
POLÍTICAS DE GESTIÓN Y ADMINISTRACIÓN DE TRÁFICO DEL PROVEEDOR DEL SERVICIO DE INTERNET	6
RECOMENDACIONES PARA LOS USUARIOS FINALES CON LA FINALIDAD DE MINIMIZAR RIESGOS DE PRIVACIDAD.....	6
MARCO LEGAL APLICABLE	14



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 **ERICK ZAUL MENA MUÑOZ** con nombre comercial **KLIC INTERNET**, 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.

ERICK ZAUL MENA MUÑOZ 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 **ERICK ZAUL MENA MUÑOZ** 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.

ERICK ZAUL MENA MUÑOZ 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).

ERICK ZAUL MENA MUÑOZ 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 bloquee 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 **ERICK ZAUL MENA MUÑOZ** 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 **ERICK ZAUL MENA MUÑOZ**. 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 los números telefónicos **4761271336 / 4772437423** asimismo podrá enviar sus preguntas al correo electrónico Atencion@klicinternet.com 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 <https://klicinternet.com/>. Por otra parte, el domicilio de atención a clientes se ubica en Calle Santa María, número 502-1, colonia Nueva Santa María, C.P. 36390, Municipio San Francisco del Rincón, Estado de Guanajuato.

DERECHOS DE LOS USUARIOS FINALES DEL SERVICIO DE ACCESO A INTERNET

ERICK ZAUL MENA MUÑOZ 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 **ERICK ZAUL MENA MUÑOZ** 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	<p>Consiste en la implementación de controles de congestión en ciertas partes de la red, derivadas dichas implementaciones ante cambios inesperados en el entorno de la red. En este caso se aplica la política QoS (Quality of Service) en español calidad de servicio. Se asegura la libre elección del usuario en el acceso a contenidos y servicios, sin restricciones arbitrarias. Se implementan técnicas para gestionar la congestión y priorizar ciertos tipos de tráfico de manera temporal y excepcional. Se preserva la privacidad de los usuarios y se fomenta la transparencia en la información proporcionada. El código cumple con la normativa vigente y promueve una red confiable y competitiva.</p>
CASOS EN QUE SE APLICA Y PARA QUÉ SE UTILIZA.	<p>El Código de Políticas de Gestión de Tráfico y Administración de Red de “Klic Internet” se aplica en diversas situaciones para asegurar una gestión eficiente y equitativa de la red. Estos son algunos casos en los que se utiliza:</p> <p>Garantizar la calidad del servicio: Se utiliza para asegurar que los usuarios finales experimenten una conexión de internet con la calidad, capacidad y velocidad contratadas, evitando afectaciones en la experiencia de navegación.</p> <p>Preservar la integridad y seguridad de la red: El código se aplica para mantener la estabilidad y seguridad de la red frente a posibles ataques externos o internos que puedan afectar su funcionamiento.</p> <p>Neutralidad de red: Se utiliza para garantizar que los usuarios puedan acceder a cualquier contenido, aplicación o servicio disponible en internet sin que se dificulte, limite, degrade, restrinja o discrimine su acceso.</p> <p>Gestión de congestión: En situaciones de alta demanda o congestión excepcional en la red, se implementan medidas</p>



	<p>para equilibrar el tráfico y evitar afectaciones en la velocidad de transmisión de datos.</p> <p>Priorización de tráfico: En ciertas circunstancias, se pueden priorizar ciertos tipos de tráfico para optimizar el desempeño de recursos y garantizar una mejor experiencia en aplicaciones críticas, como servicios de voz o navegación segura.</p> <p>Situaciones de emergencia y desastres: En casos de emergencias o desastres que pongan en riesgo la operación de la red, se pueden aplicar medidas temporales y excepcionales para mantener la integridad de la infraestructura.</p>
<p>IMPACTO EN EL SERVICIO DE INTERNET AL USUARIO FINAL.</p>	<p>Las políticas de gestión de tráfico y administración de red se aplican para asegurar la calidad, capacidad y velocidad del servicio de acceso a Internet que ofrece “Klic Internet”. Estas políticas buscan preservar la integridad y seguridad de la red, así como garantizar una experiencia de navegación óptima para los usuarios.</p> <p>Las afectaciones en la red pueden ser ocasionadas por congestión, latencia y velocidad reducida durante momentos de alta demanda. También, en casos excepcionales, se pueden aplicar medidas temporales para bloquear o restringir ciertos contenidos o servicios que representen riesgos para la red.</p> <p>Para gestionar el tráfico, se clasifica en diferentes categorías según su prioridad: tráfico prioritario para servicios críticos como VoIP y videoconferencias, tráfico de mediana prioridad para streaming y aplicaciones multimedia, y tráfico de baja prioridad para descargas masivas.</p> <p>La implementación adecuada de estas políticas asegura un equilibrio en el uso de recursos y una experiencia de navegación satisfactoria para todos los usuarios de “Klic Internet”. Además, se promueve la transparencia, la privacidad y la no discriminación en el acceso a contenidos y servicios en línea.</p>



<p>POSIBLES AFECTACIONES EN CASO DE NO APLICARSE</p>	<p>En resumen, la falta de implementación de las políticas de gestión de tráfico y administración de red por parte de “Klic Internet” podría ocasionar las siguientes afectaciones:</p> <p>Afectaciones a la red del prestador de servicios:</p> <ol style="list-style-type: none">1. Congestión y bajo rendimiento generalizado debido a una distribución ineficiente del tráfico.2. Mayor vulnerabilidad a ataques cibernéticos y amenazas de seguridad.3. Ineficiencia en el uso de recursos de la red.4. Afectaciones al usuario final y sus comunicaciones:5. Disminución de la velocidad de navegación, descargas y transmisión de contenido.6. Interrupciones frecuentes y cortes en el servicio de internet.7. Riesgo para la privacidad y seguridad de las comunicaciones en línea. <p>Por lo tanto, la implementación adecuada de las políticas de gestión de tráfico y administración de red es esencial para garantizar un servicio de calidad, estable y seguro para los usuarios de “Klic Internet”.</p>
<p>¿QUÉ MEDIDAS IMPLEMENTA PARA GARANTIZAR LA SEGURIDAD DE LA RED?</p>	<p>“Klic Internet” implementa diversas medidas para garantizar la seguridad de su red. Algunas de estas medidas son:</p> <ol style="list-style-type: none">1. Firewalls y sistemas de detección de intrusos: “Klic Internet” utiliza firewalls y sistemas de detección de intrusos para monitorear y filtrar el tráfico de la red, identificando y bloqueando posibles amenazas o intentos de acceso no autorizado.2. Encriptación de datos: Para proteger la privacidad de los usuarios, “Klic Internet” emplea protocolos de encriptación como SSL/TLS para asegurar que la información transmitida a través de la red esté protegida y sea inaccesible para terceros no autorizados.3. Protección contra ataques DDoS: “Klic Internet” implementa medidas para mitigar y resistir ataques de



	<p>denegación de servicio distribuido (DDoS), que pueden afectar el rendimiento y disponibilidad de la red.</p> <ol style="list-style-type: none">4. Monitoreo y análisis de tráfico: Se realizan constantes monitoreos y análisis del tráfico de la red para identificar posibles anomalías o actividades sospechosas, permitiendo una respuesta rápida ante cualquier incidente de seguridad.5. Actualizaciones y parches: “Klic Internet” se asegura de mantener su infraestructura actualizada con las últimas correcciones de seguridad y parches para evitar vulnerabilidades conocidas.6. Autenticación y control de acceso: Se implementan sistemas de autenticación seguros y controles de acceso para proteger el acceso a áreas críticas de la red y recursos sensibles.7. Políticas de seguridad interna: “Klic Internet” establece políticas y procedimientos internos de seguridad para el personal, con el fin de prevenir accesos no autorizados y garantizar la confidencialidad de la información de los clientes.8. Respuesta ante incidentes de seguridad: Se establece un plan de respuesta a incidentes de seguridad para abordar rápidamente cualquier situación de emergencia y minimizar el impacto en la red y en los usuarios.
<p>¿CÓMO DETECTA INVASIONES EN SU RED?</p>	<p>“Klic Internet” utiliza una variedad de herramientas y tecnologías para detectar invasiones en su red y responder rápidamente a posibles amenazas. Algunos de los métodos de detección utilizados incluyen:</p> <ul style="list-style-type: none">• Sistemas de Detección de Intrusos (IDS): “Klic Internet” emplea IDS para monitorear el tráfico de la red en busca de patrones y comportamientos sospechosos que puedan indicar actividades maliciosas o intentos de intrusión.• Análisis de registros (Logs): Se realiza un análisis constante de los registros de actividad de la red para identificar eventos anómalos, como intentos de acceso no autorizado o actividades inusuales.



	<ul style="list-style-type: none">• Firma de patrones: “Klic Internet” utiliza bases de datos actualizadas de firmas de patrones conocidos de ataques y malware, lo que permite detectar rápidamente actividades maliciosas conocidas.• Anomalías de tráfico: Se monitorea el tráfico de la red en busca de variaciones significativas o inusuales que puedan indicar un posible ataque o intrusión.• Inteligencia de amenazas: “Klic Internet” se mantiene informado sobre las últimas amenazas y tácticas utilizadas por los ciberdelincuentes, lo que les permite anticipar y defenderse contra nuevas formas de ataque.• Colaboración con proveedores de seguridad: La compañía trabaja en colaboración con proveedores de seguridad y organizaciones de la industria para compartir información sobre amenazas y tendencias de seguridad.• Monitorización de comportamiento: Se examinan patrones de comportamiento de usuarios y dispositivos para detectar posibles comportamientos maliciosos o inusuales.
<p>¿CUÁLES SON LAS RECOMENDACIONES LE DA A SUS CLIENTES PARA MANTENER LA PRIVACIDAD DE SUS DATOS?</p>	<p>“Klic Internet” proporciona a sus clientes una serie de recomendaciones para mantener la privacidad y seguridad de sus datos mientras utilizan el servicio de acceso a Internet. Algunas de estas recomendaciones incluyen:</p> <ul style="list-style-type: none">• Proteger el enrutador: Cambiar regularmente la contraseña del Wi-Fi y utilizar protocolos de seguridad como WPA2 para evitar el acceso no autorizado a la red doméstica.• Navegar en sitios seguros: Asegurarse de que los sitios web sean de confianza, verificando que la URL comience con "https" y que haya un candado con un certificado válido de una entidad confiable.• Utilizar contraseñas fuertes: Utilizar frases como contraseñas que incluyan una combinación de números, letras y símbolos para proteger cuentas de correo electrónico, redes sociales y dispositivos electrónicos.• Mantener el software actualizado: Instalar y mantener actualizado un antivirus y actualizar regularmente las aplicaciones y el sistema operativo para garantizar una navegación más segura.• Cuidado con los enlaces sospechosos: Tener especial precaución con los enlaces recibidos en correos electrónicos y redes sociales, evitando hacer clic en



	<p>enlaces que puedan llevar a sitios no deseados o peligrosos.</p> <ul style="list-style-type: none">• Evitar compartir información sensible: No proporcionar datos personales o sensibles en redes sociales o correos electrónicos, ya que las entidades legítimas como entidades bancarias no solicitarán esa información a través de medios electrónicos.• Usar herramientas de detección de sitios sospechosos: Utilizar herramientas que detecten sitios sospechosos o peligrosos para evitar interactuar con contenido malicioso.• Mantener dispositivos en buen estado: Asegurarse de que los equipos terminales estén en óptimas condiciones y con software legítimo y autorizado.• Colaborar con la atención al cliente: Reportar cualquier incidente o actividad sospechosa a la atención al cliente de “Klic Internet” para una rápida intervención y resolución.
<p>¿CÓMO GARANTIZA LA PRIVACIDAD DE LOS DATOS DE SUS CLIENTES?</p>	<p>“Klic Internet” garantiza la privacidad de los datos de sus clientes a través de diversas medidas y prácticas de seguridad implementadas en su red y servicios. Algunas de las formas en que garantiza la privacidad de los datos son:</p> <ul style="list-style-type: none">• Políticas de privacidad: “Klic Internet” cuenta con políticas de privacidad claras y transparentes que describen cómo se recopilan, utilizan, protegen y comparten los datos de los clientes. Estas políticas cumplen con las leyes y regulaciones de protección de datos aplicables.• Encriptación de datos: “Klic Internet” utiliza técnicas de encriptación seguras para proteger la transmisión de datos entre los usuarios y sus servicios en línea. Esto ayuda a evitar el acceso no autorizado a la información durante su tránsito por la red.• Protección de la red: La infraestructura de la red de “Klic Internet” está diseñada para prevenir intrusiones y ataques cibernéticos. Se implementan cortafuegos y sistemas de detección de intrusiones para monitorear y proteger la red de posibles amenazas.• Acceso seguro a la cuenta: Los clientes de “Klic Internet” tienen acceso seguro a sus cuentas a través de credenciales de inicio de sesión únicas y contraseñas. Se promueve el uso de contraseñas fuertes y se recomienda el cambio periódico de las mismas.



	<ul style="list-style-type: none">• Auditorías y monitoreo: “Klic Internet” realiza auditorías y monitoreo de la seguridad de la red y los sistemas para identificar y abordar posibles vulnerabilidades o incidentes de seguridad.• Consentimiento informado: Antes de recopilar y utilizar datos personales, “Klic Internet” obtiene el consentimiento informado de sus clientes y les proporciona información sobre cómo se utilizarán sus datos.• Protección de datos sensibles: “Klic Internet” aplica medidas adicionales de seguridad para proteger datos sensibles, como información financiera o datos de tarjetas de crédito, y solo retiene estos datos el tiempo necesario para cumplir con los fines específicos.• Formación y concientización: El personal de “Klic Internet” recibe capacitación en temas de seguridad y privacidad de datos para garantizar que se sigan las mejores prácticas y se mantengan altos estándares de protección.
--	--

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

ERICK ZAUL MENA MUÑOZ 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	03 de agosto del 2023
Versión	1.0
Elaboró	ERICK ZAUL MENA MUÑOZ