

## CÓDIGO DE POLÍTICAS DE GESTIÓN DE TRÁFICO, ADMINISTRACIÓN Y NEUTRALIDAD DE RED

### OBJETIVO

El presente Código tiene por objetivo informar a los usuarios del servicio de acceso a Internet provisto por EURONET TELECOMUNICACIONES S.A de C.V. (en adelante **LULUNET**) sobre nuestros Principios de Neutralidad de Red y del Código de Políticas de Gestión de Tráfico y Administración de Red regulados por el artículo 145 de la Ley Federal de Telecomunicaciones y Radiodifusión, y el artículo 12 de los Lineamientos para la Gestión de Tráfico y Administración de Red emitidos por el Instituto Federal de Telecomunicaciones (Instituto) por medio del Acuerdo P/IFT/EXT/280621/13.

Por consiguiente, a continuación, se describen los principios y políticas que rigen el servicio de **LULUNET**.

### I. DERECHOS DE LOS USUARIOS

#### **Libre elección:**

Los usuarios del Servicio de acceso a Internet (Servicio) de **LULUNET** podrán acceder a cualquier contenido, aplicación o servicio ofrecido por éste, dentro del marco legal aplicable, sin limitar, degradar, restringir o discriminar el acceso a los mismos.

**LULUNET** 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, siempre y cuando éstos se encuentren homologados, reuniendo las condiciones técnicas necesarias para poder acceder al servicio, aplicación o contenido deseado, que sea ofrecido en Internet. Lo anterior, conforme a los términos, condiciones y estructuras tarifarias contenidas en las ofertas inscritas en el Instituto (Instituto Federal de Telecomunicaciones).

### No discriminación:

**LULUNET** se abstendrá de obstruir, interferir, inspeccionar, filtrar o discriminar los contenidos, las aplicaciones o el propio Servicio; tratando de la misma manera el tráfico de los que sean similares entre sí, en beneficio de los usuarios finales.

### Privacidad:

**LULUNET** procurará la preservación de la privacidad de los usuarios y la seguridad de la red, asegurando la inviolabilidad de sus comunicaciones privadas. Para tal efecto, el Aviso de Privacidad puede ser consultado en <https://www.lulunet.mx/aviso-privacidad>

### Transparencia e información:

**LULUNET** publica y actualiza en su página de internet (<https://lulunet.mx/>), 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; cuestiones que pueden ser consultadas en el Código de Prácticas Comerciales en el vínculo [CÓDIGO DE PRÁCTICAS COMERCIALES](#)

### Gestión de tráfico:

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

### **Calidad:**

**LULUNET** se compromete a preservar los niveles mínimos de calidad que al efecto se establezcan en los lineamientos respectivos..

### **Desarrollo sostenido de infraestructura:**

En beneficio de los Usuarios Finales, el Instituto fomenta el crecimiento sostenido de la infraestructura de telecomunicaciones.

## **II. POLÍTICAS DE GESTIÓN Y ADMINISTRACIÓN DE TRÁFICO**

Las políticas de gestión de tráfico y administración de red son un conjunto de técnicas utilizadas por los proveedores del servicio de acceso a Internet para el manejo, tratamiento y procesamiento del flujo de tráfico cursado por una red pública de telecomunicaciones.

Las técnicas de gestión implementadas por **LULUNET**, en todo momento se encaminan a asegurar la calidad, capacidad y velocidad del servicio de acceso a Internet provisto a los Usuarios, y al mismo tiempo preservar la integridad y la seguridad de la red.

Las políticas utilizadas en ningún momento impedirán, limitarán, degradarán, restringirán o discriminarán el libre acceso a cualquier contenido, aplicación o servicio, y tampoco violarán la privacidad o intervendrán las comunicaciones de los Usuarios.

### **Administración de tráfico en congestión:**

A fin de garantizar la calidad o la velocidad de servicio contratada por el usuario **LULUNET** utilizará un conjunto de actividades, métodos, procedimientos y herramientas para la operación y el aprovechamiento de los recursos y capacidades de su red; utilizando además las técnicas necesarias para el manejo, tratamiento y procesamiento del flujo de tráfico cursado por su red pública de telecomunicaciones.

**LULUNET** garantiza la calidad de sus servicios, por lo cual ofrece una tasa de transmisión descendente de por lo menos 4 Mbps y una tasa de transmisión ascendente de por lo menos 1 Mbps en el borde de la cobertura exterior durante hora pico.

La calidad de los servicios ofrecidos puede verse afectada por una mayor demanda de tráfico o de usuarios finales de la originalmente prevista. A tal efecto, se debe reportar de manera regular las proyecciones de tráfico.

La gestión de congestión consiste en que nuestro proveedor de acceso a la red ajustará los parámetros técnicos en el Servicio, por lo que puede implementar una reducción de velocidad de hasta 2.5 Mbps 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 del conjunto de usuarios finales en la red de nuestro proveedor de acceso. 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 en perjuicio de los usuarios finales.

Derivado de la implementación de las medidas mencionadas, podría generar que los tiempos de respuesta en el acceso y/o descargas de contenidos se mantenga o disminuya, y con ello, los usuarios pudieran experimentar una mejora en la navegación.

### **Política de enrutamiento:**

La administración del tráfico en la red de **LULUNET** se hace mediante equipos enruteadores, consistente en una red IP (protocolo de Internet) que utiliza los diversos protocolos para proporcionar mayor seguridad. Los routers guían y dirigen los datos de red mediante paquetes y priorizan los datos y eligen la mejor ruta para cada transmisión.

Por lo tanto, **LULUNET** garantiza utilizar la mejor ruta a los destinos de internet, actuando de forma automática, para evitar pérdidas del servicio cuando se presentan eventos que pudieran afectarlas.

## **Administración de 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 IAR (Internet Addresses y Resources México), quien administra dichas direcciones de manera eficiente para permitir el acceso a Internet de todos los usuarios a nivel global de manera equitativa.

Toda vez que se trata de insumos finitos, la administración de direcciones IP, se realiza de la siguiente manera:

- a) Asignación dinámica y compartida de las direcciones IP “públicas” de los tipos IPv4 e IPv6 para todos los usuarios del Servicio, lo que implica que una misma dirección puede ser compartida para una multiplicidad de direcciones IP privadas.
- b) Asignación dinámica o estática de direcciones IP “privadas” son utilizadas para con las que se presta el Servicio.
- c) La navegación en Internet genera lo que se conoce comúnmente como sesiones, las cuales emplean las direcciones IP privadas; el Proveedor podrá gestionar la cantidad de direcciones simultáneas disponibles al usuario.

La implementación de lo anterior generará:

1. Ocupación adecuada de las direcciones IP públicas.
2. Disponibilidad de las direcciones IP públicas.

## **Interconexión entre redes:**

Es la conexión directa entre redes de internet consiste en conectar redes independientes con el fin de intercambiar información de manera directa entre los usuarios o servicios de ambas redes evitando la necesidad de utilizar a un tercero para el intercambio de tráfico a través de una red de tránsito.

## **Bloqueo:**

**LULUNET** no lleva a cabo el bloqueo de tráfico de datos en los Servicios que tengan contratados los usuarios finales.

El bloqueo es la técnica que impide el acceso de los Usuarios a un sitio web determinado o la utilización de un tipo de contenido o servicio particular, ya sea de manera temporal o permanente.

**LULUNET** podrá bloquear el acceso en caso de existir riesgo a la integridad de la red y a las comunicaciones legítimas de los Usuarios dada a la existencia de máquinas que tienen gusanos, virus u otro malware que genere grandes cantidades de correo electrónico no deseado.

## **Beneficios a los Usuarios:**

Las políticas de administración y gestión de tráfico enunciadas ofrecen como beneficio a los Usuarios finales:

- Reducción del tiempo de respuesta en la entrega de contenido hacia los usuarios.
- Optimización en consumo de ancho de banda del operador hacia la red de tránsito.
- Reducción de costos operativos en enlaces hacia red de tránsito.
- Mayor fiabilidad de la red.
- Mayor seguridad al navegar por la web.
- Disminución de la brecha digital

Asimismo, no implementar tales políticas traería como consecuencia:

- Incremento del tiempo de respuesta en el envío y recepción de contenido.
- Aumento de los costos operativos en enlaces hacia red de tránsito.
- Degradación de la experiencia de usuario

- Baja confiabilidad de la red.
- Mayor inseguridad al navegar por la web.
- Aumento de la brecha digital

### **III. RECOMENDACIONES DE USO**

Para favorecer y fomentar la seguridad al navegar por Internet así como minimizar riesgos a la privacidad de los Usuarios, **LULUNET** hace las siguientes recomendaciones:

#### **1. Utilizar un navegador seguro:**

Asegurarse que los equipos a través de los que accede al Servicio, cuenten con un programa (web browser o navegador) que brinde protección al navegar en Internet, el cual incluya un antivirus actualizado a fin de prevenir ataques de programas maliciosos (Malwares) que puedan afectar al equipo o bien, sustraer información personal y/o confidencial; así como herramientas para prevenir anuncios no deseados (Adware); accesos no deseados o conexiones en segundo plano (Backdoor); 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. Mientras más completa sea la solución que adquieras, mayor será su nivel de protección.

#### **2. Mantener el sistema operativo actualizado:**

Las actualizaciones del sistema operativo de tus dispositivos suelen implementar parches para solucionar problemas técnicos o brechas de seguridad, lo que brindará mayor protección en contra de nuevos malwares.

#### **3. Instalar un Firewall:**

El Firewall, también conocido como Cortafuegos es una herramienta que protege al dispositivo utilizado para navegar en Internet y se encarga de bloquear los accesos no autorizados a nuestra red; son fáciles de descargar e instalar y existen varias opciones para todos los sistemas operativos.

#### **4. Instalar un Antivirus:**

Los antivirus son programas cuyo objetivo es detectar y eliminar virus informáticos o malwares al navegar por la web y descargar datos, además algunos de ellos son capaces de buscar y detectar virus para bloquearlos, así como desinfectar archivos y prevenir una infección de estos, por lo que contar con dicho programa ofrecerá mayor protección y seguridad al utilizar el Internet; son fáciles de descargar e instalar y existen varias opciones para todos los sistemas operativos.

#### **5. No navegar en sitios desconocidos:**

Al navegar en Internet asegúrese de validar que el sitio, servicio, contenido o aplicación visitado o utilizado cuente con certificados de seguridad y sellos de confianza emitidos por auditores y certificadores reconocidos. Recomendamos instalar complementos para navegadores web, así como, revisar las opciones de seguridad y privacidad del navegador que utiliza.

#### **6. No proporcionar información sensible en sitios inseguros:**

Se recomienda no proporcionar datos personales, números de cuenta, tarjetas bancarias, números telefónicos, NIP's de seguridad, tokens, códigos de seguridad de tarjetas, contraseñas, pins, tokens, imágenes, fotografías, etc., a menos de que estés plenamente convencido de la autenticidad del sitio y que las finalidades de uso sean las pertinentes.

#### **7. Configurar el control parental:**

Instalar y utilizar herramientas de control parental para monitorear y controlar las actividades de los menores de edad cuando hagan uso de Internet y procurar sensibilizarlos acerca de los riesgos a los que se pueden enfrentar en Internet.

#### **8. Actualizar frecuentes contraseñas:**

Se recomienda cambiar contraseñas frecuentemente haciendo uso de contraseñas seguras que tengan al menos 8 caracteres y que tengan una combinación de números, letras mayúsculas, minúsculas y símbolos.

Además se aconseja no establecer la misma contraseña para diversos perfiles y cuentas, sino utilizar una única para cada sitio.

## **9. Crear usuarios distintos:**

En caso de que varias personas utilicen el mismo dispositivo para navegar en la web, se recomienda que cada una cuente con un usuario y contraseña para ello, lo que brindará mayor seguridad para el tratamiento de datos personales y uso de archivos.

## **10. Configurar adecuadamente la privacidad en redes sociales:**

Revisa la configuración de seguridad en las redes sociales que uses y evita compartir información personal y confidencial.

## **11. Cerrar sesión:**

Finalizar la sesión de las cuentas o perfiles cuando no estén siendo utilizados y antes de apagar los dispositivos; fomentará la protección de tu privacidad, en especial si se accede desde dispositivos públicos.

## **12. Cuidar los permisos en las aplicaciones:**

Al instalar aplicaciones en los dispositivos, algunas aplicaciones solicitar permisos para acceder a carpetas como la galería de fotos y vídeos, así como para acceder al hardware del dispositivo como la cámara y micrófono, por lo que es importante permitir dicho acceso sólo a aplicaciones de confianza y descargadas desde plataformas oficiales, y en su caso administrar las aplicaciones que tienen tales permisos desde la configuración del dispositivo.

## **13. Realizar descargas de sitios oficiales y confiables:**

Para descargar software, aplicaciones y archivos de forma segura se recomienda no modificar la configuración de fábrica de los equipos; descargar software y aplicaciones solo de sitios web y tiendas oficiales; verificar los permisos y accesos requeridos por el software o aplicación antes de otorgarlos.

## **14. Evitar acceder desde puntos Wi-Fi inseguros:**

Evitar conectarse desde conexiones Wi-Fi desconocidas o de red abierta, puesto que mediante éstas es sumamente fácil acceder a datos sensibles y confidenciales, por lo que se recomienda utilizar una conexión VPN para que la información que transmitas vaya cifrada de punto a punto.

## **15. Desconectar Internet:**

Si no se está haciendo uso del Internet, es aconsejable desconectarlo o apagarlo, pues así se reducen las posibilidades de sufrir un ataque informático.

## **16. Copias de seguridad:**

Para evitar la pérdida de información valiosa ya sea por robo, extravío o avería del dispositivo, se recomienda contar con un backup, también conocido como copia de seguridad. Esto se puede hacer de manera externa, respaldando la información de interés en algún hardware de sistema cerrado, o bien, desde el backup que ofrece la propia aplicación en uso o desde la nube personal de Usuario.

Actualizado al día 1° de Febrero 2025.