

POLITICAS DE USO ACEPTABLE ETB - PUA

Introducción:

ETB en su calidad de proveedor de redes y servicios entre ellos: Voz, Voz Móvil, Internet Móvil, Servicios de Red Inteligente, servicios de datos, Internet Banda Ancha y sus servicios de valor asociado como correo electrónico, PWP (páginas web personales), Disco Duro Virtual, Guardián de Contenido, McAfee, tienda virtual y chat para soporte, entre otros; se permite adicionar las políticas de uso aceptable (en adelante denominada PUA) a las condiciones bajo las cuales **ETB** presta dichos servicios, en el sentido de incluir como prohibiciones las que se señalan en el presente documento.

Este documento PUA pretende proteger a ETB y a sus clientes de ataques a sus sistemas, equipos y redes, así como coordinar y mantener los protocolos y lineamientos aceptados internacionalmente para el uso correcto y apropiado de los servicios.

ETB se reserva el derecho de modificar la presente política en cualquier momento, la cual será efectiva una vez esta sea comunicada en este URL y es responsabilidad del usuario consultarla de manera periódica.

Propósito:

Este documento es enunciativo ya que no abarca todos los aspectos en los cuales se podrá incurrir. En este orden de ideas, toda actividad que viole la ley, las regulaciones o las normas que apliquen para los servicios de Voz, Larga Distancia, Servicios de Red Inteligente, Voz Móvil, Internet Móvil e Internet Banda Ancha (por ejemplo: marcos de seguridad y recomendaciones definidos por la UIT, CRC, etc.), o que perjudique el desempeño de la red, la imagen o las relaciones con los clientes de ETB, así no se mencionen o se incluyan dentro de este documento, se asumen como parte de estas políticas, dado que su fin es preservar la integridad y disponibilidad de los servicios y de sus usuarios. El documento PUA está ligado a las Condiciones de Prestación del Servicio (http://www.etb.com.co/guiadeconsulta/contratos_opcion.asp) y otras políticas de ETB.

Alcance:

El documento PUA está dirigido a clientes de **ETB**, personas naturales o jurídicas, que contratan servicios para conectarse a los servicios de Voz, Larga distancia, Servicios de Red Inteligente, Voz Móvil, Internet Móvil, Internet Banda Ancha o servicios de datos que ofrece **ETB**. Cualquier actividad prohibida que se lleve a cabo, en la cual participe un tercero en nombre de o en beneficio de un cliente de **ETB** o cualquier cliente o usuario final de un cliente de **ETB**, será considerada una actividad prohibida que se lleve a cabo por el cliente de **ETB**. Cualquier vulneración a la ley o a las condiciones previstas, se constituye en VIOLACIÓN de lo estipulado por el cliente para la utilización de los servicios, que por su potencial repercusión requieren de la toma de medidas inmediatas, en consecuencia el cliente acepta y reconoce que **ETB** está facultada para suspender o terminar la prestación del servicio sin necesidad de requerimiento previo, sin perjuicio de lo anterior, **ETB** podrá, en los casos en que lo considere pertinente, informar al cliente sobre la realización de conductas prohibidas y solicitarle que se abstenga de realizarlas. En estos casos, se contactará al cliente vía telefónica o por medio de las cuentas de correo electrónico inscritas o conocidas por **ETB** de ser posible. Lo anterior, sin perjuicio de las acciones judiciales y denuncias que **ETB** y terceros afectados puedan emprender contra el usuario en Colombia o en cualquier otra jurisdicción. En cualquiera de los eventos anteriores **ETB** podrá dar por terminado el **CONTRATO** unilateralmente y sin que medie declaración judicial. **EL CLIENTE** es el único responsable de los perjuicios o daños que cause por el incumplimiento de sus obligaciones.

Usos indebidos:

De manera enunciativa señalamos algunos usos indebidos que no están autorizados ni permitidos y que su ejecución por parte del usuario originará la terminación o suspensión del servicio por parte de **ETB**, con justa causa al constituirse como violación de las condiciones de uso de los servicios prestados por **ETB**:

- i.** Interceptación de llamadas sin orden legal autorizada, así como el uso total o parcial de la información obtenida de esta forma.
- ii.** Conexiones no formales en strip o redes internas del predio sobre el servicio de otro usuario.
- iii.** Grabación total o parcial de llamadas, así como el uso total o parcial de la

información obtenida de esta forma.

- iv. Realizar conexiones, acometidas o líneas, tales como acometidas fraudulentas, traslados no autorizados, derivaciones externas, derivaciones sobre la línea de otro CLIENTE o USUARIO, entre otros, o por utilizar equipos o instalaciones que no cumplan con las normas técnicas y las condiciones de homologación que determine la autoridad competente.
- v. Utilizar los servicios para actividades ilegales (extorsión, matoneo, llamada millonaria, entre otros).
- vi. Efectuar llamadas a los servicios de urgencia y/o emergencia que no se adecuen al propósito de los mismos.
- vii. Realizar uso de cualquier modalidad tendiente a violar en forma directa o indirecta el régimen de telecomunicaciones y, en especial el marco general de la prestación de SERVICIOS o actividad inherente o complementaria a éstos. Se entiende que tienen la naturaleza de métodos de comunicación no autorizados entre otros (i) el enrutamiento directo del tráfico de larga distancia simulándolo como tráfico de telefonía fija local (by pass); (ii) el Call Back; (iii) la utilización del SERVICIO para una actividad diferente a la contratada con ETB; (iv) la reventa de SERVICIOS y planes contratados para uso personal no autorizados por ETB; (v) la distorsión del tráfico; (vi) la alteración de las señales de los equipos terminales o abonados; (vii) la alteración de cualquier equipo, sistema o dispositivo de acceso de tal forma que se modifique la medición del consumo facturable de los SERVICIOS o se sustraiga su pago; (viii) el hacerse a códigos de acceso o números de identificación personal sin autorización; (ix) el acceso a SERVICIOS SUPLEMENTARIOS o a CATEGORÍAS DE PROGRAMACIÓN sin previa autorización de ETB; (x) la interceptación de comunicaciones sin orden de autoridad competente; (xi) el acceso a los servicios para realizar denuncias o manifestaciones tendenciosas, falsas, engañosas, ficticias o contrarias a la moral y a las buenas costumbres, o (xii) cualquier modalidad similar o de uso ilegal de la red de telecomunicaciones y de fraude en su utilización.
- viii. Influir injusta o ilegalmente o en forma indebida o inadecuada directa o indirectamente en los sistemas, redes, aplicativos y demás elementos involucrados en la transmisión o recepción de información, incluyendo los terminales de los usuarios.
- ix. Violar o intentar violar sistemas de seguridad o red de **ETB** o de cualquier tercero. Intentar acceder sin autorización a los sitios o servicios de **ETB** o de otro
- x.

operador, mediante la utilización de herramientas intrusivas (hacking), descifre de contraseñas, descubrimiento de vulnerabilidades o cualquier otro medio no permitido o ilegítimo.

- xi.** Cargar archivos que contengan virus, software malicioso, malware, generadores de phishing, gusanos (“worms”), bombas de correo (“mail-bombing”), archivos dañados o cualquier otro programa o software similar que pueda perjudicar el funcionamiento de los equipos de la red de **ETB** o de propiedad de terceros.
- xii.** Obtener información de los usuarios de Internet para fines comerciales no autorizados previamente, mediante publicidad engañosa o artilugios de cualquier índole, divulgarla o ponerla a disposición de entidades o procesos no autorizados.
- xiii.** Presentar, alojar o transmitir información, imágenes o textos que en forma directa o indirecta se relacionen con actividades sexuales con menores de edad. El **CLIENTE** declara que conoce lo dispuesto en la Ley 679 de 2001 y el Decreto 1524 de 2002, de acuerdo con lo cual se prohíbe expresamente el alojamiento de contenidos de pornografía infantil, y en esa medida los proveedores o servidores, administradores y usuarios de redes globales de información no podrán: (i) Alojar en su propio sitio imágenes, textos, documentos o archivos audiovisuales que impliquen directa o indirectamente actividades sexuales con menores de edad. (ii) Alojar en su propio sitio material pornográfico, en especial en modo de imágenes o videos, cuando existan indicios de que las personas fotografiadas o filmadas son menores de edad. (iii) Alojar en su propio sitio vínculos o "links", sobre sitios telemáticos que contengan o distribuyan material pornográfico relativo a menores de edad. Adicionalmente, y sin perjuicio de la obligación de denuncia consagrada en la ley para todos los residentes en Colombia, los administradores y usuarios de redes globales de información deberán (i) denunciar ante las autoridades competentes cualquier acto criminal contra menores de edad de que tengan conocimiento, incluso de la difusión de material pornográfico asociado a menores. (ii) Combatir con todos los medios técnicos a su alcance la difusión de material pornográfico con menores de edad. (iii) Abstenerse de usar las redes globales de información para divulgación de material ilegal con menores de edad. (iv) Establecer mecanismos técnicos de bloqueo por medio de los cuales los usuarios se puedan proteger a sí mismos o a sus hijos de material ilegal, ofensivo o indeseable en relación con menores de edad. El incumplimiento de las obligaciones y prohibiciones mencionadas,

acarreará además de las sanciones penales a que haya lugar: (i) la terminación del presente contrato, (ii) la imposición por parte del Ministerio de Tecnologías de la Información y las Comunicaciones de multas hasta de cien (100) salarios mínimos legales mensuales vigentes, y (iii) la suspensión o cancelación de la correspondiente página electrónica. Asimismo, EL USUARIO deberá implementar sistemas internos de seguridad para su red, encaminados a evitar el acceso no autorizado a su red, la realización de spamming, o que desde sistemas públicos se tenga acceso a su red, con el fin de difundir en ella contenido relacionado con pornografía infantil; (iv) utilizar el SERVICIO para el acceso y uso de contenidos ilícitos o que violen las normas sobre derechos de autor, cuyas consecuencias se prevé en las leyes sobre la materia.

- xiv. Anunciar, enviar, presentar o transmitir contenido de carácter ilegal, atentatorio a la dignidad del ser humano, que tenga la potencialidad de ser peligroso, genere pánico económico, social, de salubridad, etc.
- xv. Vulnerar derechos de propiedad industrial, derechos de autor, o copyright protegidos por las leyes nacionales, extranjeras y acuerdos o tratados internacionales sobre la materia.
- xvi. Violar las comunicaciones y la intimidad de las personas.
- xvii. Crear identidades falsas con el propósito de confundir a terceros.
- xviii. Usar los sitios o servicios que puedan dañar, deshabilitar, sobrecargar o deteriorar algún sitio o servicio prestado por **ETB** o cualquier otro operador.
- xix. Enviar correo basura, Spam (por sus siglas en inglés) indiscriminado, o encadenado no autorizado o consentido previamente por los destinatarios.
- xx. Monitorear tráfico de cualquier red o sistema sin la debida autorización del usuario o administrador de la red.
- xxi. Realizar ataques de denegación de servicio (DoS) que causen daño o inutilización de los servicios prestados por **ETB** u otros operadores.

Control de contenidos:

Al hacer uso del servicio Control de Contenidos <http://www.etb.com.co/guardian/>, el **CLIENTE** declara que conoce y acepta las condiciones de uso del servicio de acceso a Internet de **ETB**, en especial las que le imponen la obligación de responsabilidad a su cargo sobre la utilización del servicio, recibo, envío y alojamiento de imágenes y/o textos que en forma directa o indirecta se encuentren relacionados con actividades delictivas,

pornografía infantil, plagio, entre otras. La instalación y uso del servicio de Guardián de Contenidos es una herramienta gratuita que **ETB** coloca a disposición del **CLIENTE** y que no exime a éste de las responsabilidades aludidas. El **CLIENTE** conoce y acepta que el servicio de Guardián de Contenidos no tiene una efectividad de uso del 100% y en consecuencia expresamente exonera a **ETB** por las fallas que el mismo presente y en general por las manipulaciones del programa que permitan su desactivación o efectividad total o parcial.

Correo y Política antispam:

Es un deber de los usuarios de **ETB** utilizar el servicio de correo electrónico de manera adecuada y responsable. El Spamming es una actividad ilegal que no es permitida ni tolerada por **ETB**.

- Se define Spamming como la acción de enviar correo electrónico SPAM.
- Se define SPAMMER como aquel que envía correo SPAM.
- Se define correo SPAM como el envío de cualquier correo electrónico, masivo o no, a personas (usuarios de ETB y usuarios de otras redes) que incluyen temas tales como pornografía, publicidad, venta de productos, entre otros, los cuales no han sido solicitados por el(los) destinatario(s).

Cuando se habla de “envío masivo o individualizado de correo electrónico”, **ETB** lo entiende como el envío de uno o más correos a usuarios que no lo han solicitado, indiferentemente de que las direcciones de correo electrónico de los destinatarios se encuentren en el campo PARA, CC o BCC, del correo electrónico generado. Para determinar si un cliente de **ETB** está enviando correo SPAM, **ETB** se apoyará en los reportes enviados por entidades internacionales o terceros, así como en los reportes generados por la herramienta antispam con la que cuenta **ETB**.

Los usuarios que tienen listas con direcciones de correo electrónico, las cuales han sido previamente inscritas y autorizadas por sus responsables para enviarles correos electrónicos, deberán informar a los destinatarios el derecho que tienen a solicitar su retiro de la lista (opción “unsubscribe”) y deberán adoptar las medidas necesarias para evitar que sigan enviando este tipo de correos una vez el cliente lo haya solicitado. La opción de retiro de la lista de correo, no exime al generador de su responsabilidad, ya que si el correo ha sido enviado a una dirección que no lo ha solicitado será catalogado como SPAMMER.

Los clientes de **ETB** son los únicos responsables de los mensajes y del contenido que anuncian, distribuyen o de otro modo facilitan utilizando las conexiones y servicios que ofrece **ETB**. Es responsabilidad del cliente asegurar y configurar de forma adecuada los equipos y servicios que va a conectar a Internet. **ETB** no se responsabiliza por equipos del cliente. En este orden de ideas, los clientes deben abstenerse de realizar, entre otras, las siguientes prácticas:

- i. Hacer Spamming de cualquier naturaleza que no haya sido autorizados por el(los) destinatario(s) o que pudieran originar cualquier clase de incomodidad o queja por parte del mismo.
- ii. Continuar enviando correo a destinatarios que le hayan solicitado que no desean continuar recibiendo esta clase de correos.
- iii. Utilizar cualquier servicio prestado por **ETB** para la composición, almacenamiento, distribución, colección o envío masivo de correo electrónico. Se incluye cualquier forma de correo que no hayan sido solicitado, así como transmitir correos a terceras personas sin su consentimiento que fueran obscenos, molestos, injuriosos, difamatorios, abusivos, amenazantes o que pongan en peligro la estabilidad de la red de **ETB** o de cualquier otra red.
- iv. Promover directa o indirecta la proliferación de correo spam, incluyendo las casillas de correo, software para realizar spam y hosting de sitios web para realizar spam.
- v. Utilizar un servidor de correo para retransmitir correo sin el permiso expreso del sitio (Relaying). Entiéndase Relaying como la acción de utilizar un servidor como medio de difusión de correo electrónico en el cual, el remitente o el destinatario no son usuarios de dicho servidor.

Para mayor información favor consultar <http://www.zonasegura.etb.com.co/>.

Condiciones de uso de Planes Ilimitados de Larga Distancia

i. Segmento Empresas

- Estos planes no aplican para clientes de Reventa, Grandes Clientes, Call Center o clientes que incluyan dentro de su operación cualquier actividad de telemarketing (generación de llamadas masivas), por ejemplo: oficinas de

cobranzas, ventas, áreas de servicio al cliente, agencias de investigación de mercado y otras actividades relacionadas, entre otros.

Se considerará fraude o mal uso del servicio, el incumplimiento de las condiciones del plan de “7 Sin Límites” o si el servicio se emplea para terminación ilegal de tráfico o alguna práctica restrictiva por la regulación que esté vigente.

- En el caso que ETB determine que el cliente está realizando un uso indebido del servicio de larga distancia a través de los planes de “7 Sin Límites”, ETB se reserva el derecho de realizar la cancelación inmediata de los planes sobre los cuales se están incumpliendo las condiciones descritas anteriormente o la cancelación de todos los planes activos que tenga el cliente. De igual forma, se realizará el cobro de todos los minutos adicionales que se presenten en el tráfico de LD Nacional, según los máximos permitidos por plan indicados en la tabla anterior, a las tarifas plenas vigentes (ver circular externa No. 14).

ii. Segmento Hogares

- Las líneas telefónicas inscritas en el plan “7 Sin Límites” que registren más de veinte (20) números telefónicos distintos a nivel nacional o internacional, en un mes de facturación, se les cancelará el plan después de ser notificado por parte de la Empresa.
- Los Planes están dirigidos exclusivamente al segmento residencial para su uso convencional, de modo que, en caso de establecerse por parte de ETB que está siendo explotado, comercializado o utilizado para una actividad comercial por el cliente, se suspenderá o terminará unilateralmente por justa causa, siguiendo el procedimiento previsto en el contrato de condiciones uniformes de ETB. En estos casos ETB refacturará y cobrará los consumos realizados a través del Plan a la tarifa plena vigente para cada destino, sin perjuicio de las demás acciones legales e indemnizaciones que en su favor pueda reclamarle al cliente.

Recomendaciones para disminuir la posibilidad de fraude hacia clientes de Enlaces de Voz

No mantenga contraseñas por defecto suministradas por su proveedor para la administración de la planta telefónica, utilice contraseñas seguras y robustas para el acceso a la planta y autenticación de dispositivos SIP.

Compruebe periódicamente (a diario) si funcionalidades como DISA¹ y accesos remotos a la administración de la consola han sido activados.

- Mantenga seguro los buzones de correo, cambie periódicamente las contraseñas y elimine los buzones de correo no utilizados (fuerce a los usuarios a cambiar las contraseñas en su primer inicio de sesión a su buzón de correo y/o añadir un prefijo, no permita disponer de las contraseñas que estén relacionados con su número de extensión). Bloquee la marcación de salida de llamadas desde su sistema de correo de voz.
- Programe el sistema de comunicación para que rechace intentos de conexiones SIP, que tengan clave o extensión invalida, esto mitiga la posibilidad de un ataque de fuerza bruta.
- Limite el uso no autorizado de las líneas VoIP, permita solo una o dos llamadas simultáneas por entidades SIP cuando sea posible.
- Aliente a los empleados a informar sobre llamadas y mensajes de voz en otros idiomas, sobre todo fuera de horario.
- Si no lo requiere, no olvide restringir marcaciones a números (159, 179 y 199) de operadora asistida internacional. Adopte la filosofía del principio de restricción de llamadas hacia destinos de alto riesgo y solo la apertura a los lugares que sean solicitados o autorizados, mantenga registros de las llamadas por un período prudencial.
- Solicite continuamente al proveedor de la planta telefónica las características de nuevas versiones, actualizaciones de software en lo que se refiere a parches para corregir vulnerabilidades que permitan fortalecer su sistema telefónico.
- Utilice IDS² y herramientas de protección contra el fraude por abuso telefónico.
- Si se requiere un usuario viajero o móvil, se recomienda instalar el softphone Zoiper, que utiliza protocolo IAX, se puede usar un puerto diferente al estándar, es mucho más seguro, la clave o password de usuario viaja en MD5, los ataques están orientados hacia SIP y no a IAX, y por muchas razones más IAX es la alternativa ideal.

1. Direct Inward System Access por sus siglas en inglés, Perfeccionamiento del Sistema de Acceso Directo.

2. Intrusion Detection System, por sus siglas en inglés, Sistema Detección de Intrusos.

Desarrolle un plan de acción oficial en la política de la compañía para situaciones de emergencia a corto plazo: que acciones deben ser adoptadas y los procedimientos para abordar posibles problemas de seguridad en su sistema telefónico.

Audite periódicamente su sistema PBX para comprobar la seguridad, puntos débiles y la forma en que la programación se ajuste a las necesidades de la empresa. Mantenga un registro detallado de estas visitas.

- Realice un monitoreo permanente de los destinos tanto entrantes como salientes, hacia y desde su planta telefónica, para detectar tráfico irregular. Si detecta algún tráfico irregular o sospecha del mismo comuníquese inmediatamente con su asesor comercial o con ETB.