



## ANEXO DE CONDUCTAS NO AUTORIZADAS PARA EL CLIENTE.

Entre las partes **OPERADOR** y **CLIENTE**, se ha convenido lo relacionado en las siguientes cláusulas, las cuales hacen parte integral del contrato.

### CLAUSULA PRIMERA: DEFINICIONES

Para efectos de lo señalado en el presente anexo se tendrán en cuenta las siguientes definiciones:

#### DEFINICIONES:

METODOS DE COMUNICACIÓN NO AUTORIZADOS: Es cualquier actividad o modalidad utilizada por el **CLIENTE** tendiente a violar en forma directa o indirecta el régimen de telecomunicaciones, y en especial el marco legal, reglamentario o regulatorio de la prestación del servicio de Telefonía Pública Básica Conmutada – RTPBC (Red Telefónica Pública Básica Conmutada) y del servicio de Telefonía Móvil Celular o de cualquier servicio de telecomunicaciones o actividad inherente a éstos.

Se entiende que tienen la naturaleza de métodos de comunicación no autorizados, entre otros: 1). Call back: proceso por el cual una persona que origina una llamada telefónica, es inmediatamente colgado y vuelto a llamar (tras unos segundos) sin que incurra en ningún tipo de coste en la realización de dicha llamada; 2) Bypass: Procedimiento que consiste en recibir tráfico de larga distancia internacional, sin hacer uso de los operadores de telecomunicaciones habilitados legalmente para prestar el servicio; 3) Reoriginamiento de llamadas: Procedimiento que permite reenrutar tráfico internacional, nacional o celular ocultando su verdadero origen y simulándolo como tráfico de Local; 4) Tercer país: Procedimiento que consiste en ingresar ilegalmente tráfico de larga distancia al país cuyo destino es otro país; 5). La reventa y/o comercialización de servicios sin autorización del **OPERADOR**; 6). Uso y/o manipulación no autorizada de redes por parte del **CLIENTE** o a través de terceros; 7). La alteración de las señales de los equipos terminales o abonados; 8). La alteración de cualquier equipo, sistema o dispositivo de acceso de tal forma que se modifique la medición del consumo de los servicios o se sustraiga su pago; 9). El acceso no autorizado a códigos de acceso o números de identificación personal; 10). El acceso a servicios suplementarios o a categorías de programación sin previa autorización del **OPERADOR**; 11). La interceptación de comunicaciones sin orden de autoridad Competente; o cualquier modalidad similar o de uso ilegal de las redes y de fraude en su utilización; o cualquier otra forma de incumplimiento o violación de las disposiciones legales, reglamentarias o contractuales en materia de telecomunicaciones. 12) La instalación de Malware: software malicioso; 13) Smishing: fraude por mensajes de texto. 14) Fraude con



tarjeta de crédito. 15) Phishing: Suplantación de página web para intentar adquirir información confidencial de forma fraudulenta. 16) El acceso no autorizado por medio de internet a servidores o servicios telefónicos (hardware o software) con el fin de vulnerar la seguridad de otros clientes. 17) Pharming: es la explotación de una vulnerabilidad en los servidores DNS (Domain Name System) que permite a un atacante redirigir un nombre de dominio a otra máquina distinta. 18) Vishing: por medio de una llamada de VoIP y la ingeniería social engañan a personas para obtener información financiera o útil para la suplantación de identidad.



## CLAUSULA SEGUNDA: OBLIGACIONES ADICIONALES DEL CLIENTE

Además de las consagradas en el contrato, el **CLIENTE**, tiene las siguientes obligaciones adicionales:

1. Abstenerse de usar, autorizar, propiciar, facilitar o patrocinar la comercialización de los servicios de telecomunicaciones ofrecidos por el **OPERADOR**, para obtener beneficio o lucro económico para sí o para terceras personas naturales o jurídicas sin autorización expresa y escrita del **OPERADOR**.
2. Abstenerse de emplear los servicios ofrecidos por el **OPERADOR** para la prestación de servicios o comunicaciones no autorizados en virtud del contrato, la regulación y la ley
3. El **CLIENTE** se obliga a responder por el mal uso que terceros o el mismo **CLIENTE** hagan de los equipos, servicios e información que se entreguen y se presten por parte del **OPERADOR** durante el desarrollo del contrato. En consecuencia, el **CLIENTE** deberá velar por el cuidado de los equipos, servicios e información y se compromete a utilizar los servicios para fines lícitos.
4. Está prohibido que el **CLIENTE** aloje contenidos de pornografía infantil, use o permita usar el servicio con fines de explotación, pornografía, turismo sexual y demás formas de abuso sexual contra menores de edad.
5. Queda expresamente prohibido al **CLIENTE** utilizar las facilidades inherentes al presente contrato para establecer métodos de comunicación no autorizados descritos en el capítulo de Definiciones y los demás que las leyes y la regulación consideren como irregulares o ilegales.
6. Abstenerse de presentar documentación falsa respecto a su identidad como persona natural (cédula de ciudadanía) o jurídica (certificado de cámara de comercio) e información que no corresponda a la realidad (referencias, direcciones inexistentes, documentos presentados como prueba para algún trámite, entre otra).



7. **EL CLIENTE** no podrá hacer uso de ninguno de los servicios ofrecidos por **EL OPERADOR** para hacer llamadas de tercer país, o reventa de servicios no expresamente autorizados por el **OPERADOR**. Tampoco se podrá utilizar los servicios del **OPERADOR** como medio de conexión alterna hacia otros destinos que no hayan sido expresamente autorizados por las partes en el contrato respectivo.
  
8. **EI CLIENTE** debe abstenerse de instalar software proveniente de sitios que no son los certificados por los fabricantes, ni software sin licencia ya que podría contener aplicaciones malintencionadas y generar consumos extras en la facturación o pérdida de información.
  
9. Si **EL CLIENTE** recibe mensajes de texto SMS de un número celular informando que ganó un premio debe verificar siempre el concurso en [www.movistar.co](http://www.movistar.co) y comunicarse con **EL OPERADOR** por los canales definidos.
  
10. **EL CLIENTE** es responsable del correcto uso de los servicios que el **OPERADOR** ofrece mediante la página web, incluyendo pagos electrónicos y contratación de servicios, el **CLIENTE** debe tener en cuenta que el **OPERADOR** nunca le solicitará datos personales a través de correos electrónicos.
  
11. **EL CLIENTE** debe tener en cuenta que, como requisito previo para ser operador de un servicio de telecomunicaciones, la Ley de TICS, 1341 de 2009 en sus artículos 10 y 15, le exige la habilitación para la prestación de los servicios de telecomunicaciones, mediante la figura de Autorización General, la cual sustituye los conceptos de licencia y título habilitante convergente anteriormente aplicables.
  
12. **EI CLIENTE** tiene como obligación realizar un uso adecuado del servicio contratado de acuerdo con lo estipulado en el contrato firmado y a lo expresado por las autoridades que tengan incidencia en el uso del servicio.
  
13. Si **EL CLIENTE** ha solicitado servicios de planta telefónica en calidad de arriendo o compra a través de alguno de los proveedores autorizados por el **OPERADOR**, tiene como obligación diligenciar el Check List Técnico adjunto, que permite asegurar la configuración básica minimizando el riesgo de conductas irregulares en las centrales telefónicas.



14. **EI CLIENTE** debe conocer y mantener estrictos cuidados con la seguridad de estos equipos, asegurando que la configuración de los mismos no sea manipulada por terceros diferentes a los autorizados por EL OPERADOR, en caso de arrendamiento. Después de cada mantenimiento, EI CLIENTE debe siempre asegurar que los equipos mantengan la configuración definida en el Check List Técnico.

15. **EI CLIENTE** se obliga a rechazar cualquier servicio de instalación o mantenimiento de su planta telefónica, si no ha verificado satisfactoriamente el cumplimiento de cada uno de los puntos definidos en el Check List Técnico.

16. **EI OPERADOR** no será responsable de la seguridad de la red donde sean instalados los equipos suministrados para el servicio contratado independientemente de la modalidad bajo la cual se entreguen los productos por parte de **OPERADOR al CLIENTE**.

17. **EI CLIENTE** debe proteger la ubicación física de la central telefónica o PBX, el cuarto de equipos y/o gabinetes, el lugar en donde se encuentran instalados estos equipos deben tener su respectivo mecanismo de seguridad a este sitio únicamente debe acceder personal autorizado y el **CLIENTE** llevar un control de registro de entrada y salida.

18. El suministro, licenciamiento, actualización y soporte de las aplicaciones de seguridad de la información como los antivirus, antispyware, antispam, antimalware, cifrado de datos, prevención de fuga de la información, firewall local, detección y prevención de intrusiones local, filtro de contenido, navegación segura, entre otros, serán de responsabilidad y estarán a cargo única y exclusivamente del **CLIENTE**.

19. En general, si en su organización están instalados E1's, RDSI, Troncal SIP o líneas telefónicas normales interconectadas a su planta telefónica conformando un PBX administrado por usted o a través de un tercero que le preste este servicio, le recomendamos conocer y mantener estrictos cuidados con la seguridad, mantenimiento y manejo de estos equipos, los cuales son de entera responsabilidad del **CLIENTE**, por lo cual tenga en cuenta las siguientes recomendaciones:

Si la administración de la planta telefónica es a través de los servicios de un tercero, acostumbre a firmar cláusulas de penalización y responsabilidad



jurídica y económica por fraudes realizados y atribuidos a vulnerabilidad del PBX.

Adopte la filosofía del principio de restricción de llamadas y solo la apertura a los lugares que sean solicitados o autorizados.

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.

Establezca políticas claras sobre la seguridad del sistema telefónico PBX, establezca un plan de marcación y defina responsables del tráfico, limite las llamadas de las extensiones que no requieren comunicación LDI ó LDN ó Móviles, no permita configuración de extensiones sin uso o responsable.

Audite periódicamente su sistema PBX para comprobar la seguridad, puntos débiles y la forma en que la configuración se ajuste a las necesidades de la empresa.


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 **EL OPERADOR**, asigne dentro de su empresa personal responsable de este monitoreo.

Revisar periódicamente la facturación de llamadas de su Central o PBX en especial los servicios de larga distancia y celular, con el fin de identificar consumos fuera de lo normal.

20. Se exonera de toda responsabilidad al **OPERADOR** por el uso indebido que el **CLIENTE** de a los productos y servicios suministrados, cámaras, puestos de trabajo informático, teléfonos inalámbricos, sesiones de llamadas VoIP, servicios de voz tradicional, servicios de internet, televisión, datos, mensajes de texto, servidores de correo, servidores de datos, plantas telefónicas, transferencia de archivos, entre otros.



21. **EI CLIENTE** deberá diligenciar el Checklist Técnico que se indica a continuación, el cual permite la configuración básica para minimizar la materialización de un evento de fraude en las centrales:

			
<b>Check list técnico control fraude recomendaciones de configuración básica para prevenir fraude en centrales telefónicas</b>			
<b>Ítem</b>	<b>Descripción</b>	<b>¿Se configuro correctamente? SI/NO</b>	<b>¿Por qué no se configuro?</b>
Llamadas fuera de horario laboral	Configuración mediante la cual se bloquean las llamadas que se intenten realizar fuera del horario laboral		
Bloqueo de puertos	Facilidad de la central telefónica para deshabilitar los puertos que no se requieran para el servicio de voz.		
Bloqueo de Operadora asistida	Funcionalidad que permite mediante la marcación del número de activación de tono, seguridad del 199,179 ,159 y 191, 171 y 151 para comunicarse con las Operadoras (humanas) de MOVISTAR, ETB, UNE para solicitar llamadas internacionales y nacionales respectivamente.		
Salida de llamadas a Celular	Funcionalidad que permite restringir total o parcialmente la salida de llamadas a cualquier Operador de la red celular		
Salida de llamadas a destinos Nacionales (LDN)	Funcionalidad que permite restringir total o parcialmente la salida de llamadas a cualquier destino Nacional.		
Salida de llamadas a destinos Internacionales (LDI)	Funcionalidad que permite restringir total o parcialmente la salida de llamadas a cualquier destino Internacional.		
Salida de llamadas a líneas especiales 01800/01800,113,etc.	Funcionalidad que permite restringir total o parcialmente la salida de llamadas a destinos especiales.		
DISA	Funcionalidad que permite acceder a una extensión determinada conectada a la plata desde el exterior sin necesidad de pasar por la planta telefónica.		



Buzón de Voz por grupos	Funcionalidad que permite activar el sistema de buzones para un grupo de extensiones de la planta telefónica,		
	fuere a los usuarios a cambiar las contraseñas periódicamente.		
Usuarios de consulta	Habilitación o creación de usuarios de consulta para monitoreo de la planta telefónica.		
Códigos de llamadas	Códigos o claves configurados en la planta para realizar llamadas a celular LDN, LDI, 01800 etc. Estos se pueden asignar por ext., por grupo por perfil de usuario.		
Credenciales de accesos	La contraseña asignada tanto para fines de administración de la planta, como para la salida de llamadas a destinos especiales (Móviles, LDN, LDI etc.). Deberán contener al menos una característica alfanumérica y ser mínimo de 6 caracteres. Por otro lado, se sugiere que estas se cambien cada 2 meses o cuando se realice cambios de personal.		
Acceso Remoto usando modem	Funcionalidad para acceso remotos a la planta telefónica con fines de mantenimiento.		
Usuario de prueba	Usuario ficticio creados por el proveedor de la planta o solicitados por el cliente para realizar pruebas de entrega de la central. Esto deberán ser eliminados una vez finalizadas las mismas.		
Protocolo de acceso	Para el acceso a la planta telefónica se pueden habilitar el protocolo FTP, Telnet, SSH, o Ipsec. Estos no deben estar permanentemente activos. Solo en momentos de soportes y mantenimiento.		
Política de Firewall seguridad lógica (aplica para plantas IP)	Protección de la red LAN del cliente mediante un dispositivo especial de Firewall y IDS. En caso de que la central sea IP, esta deberá estar protegida por parte del cliente contra posibles ataques tanto internos como externos.		





NAT (Aplica solo para plantas de IP)	Configuración que se realice en un dispositivo del cliente (Firewall, Router, etc.) mediante la cual no se asigna dirección IP pública sino IP privada. Se recomienda que en todos los casos el cliente habilite NAT.		
--------------------------------------	---	--	--

### CLAUSULA TERCERA: SANCIONES

1. La realización de las conductas descritas en las cláusulas anteriores utilizando cualquiera de las facilidades asignadas, acarreará para el **CLIENTE** la terminación unilateral del presente Acuerdo por parte del **OPERADOR**, en consecuencia se suspenderá inmediatamente el servicio y se retirará el enlace y los demás equipos que se hayan instalado, sin perjuicio de iniciar las acciones legales correspondientes y de resarcimiento del perjuicio ocasionado, para lo cual se tasarán a la máxima tasa permitida.
2. Cuando se detecte la indebida utilización de alguna de las líneas telefónicas de conformidad con lo establecido en este anexo, el **OPERADOR** podrá terminar el contrato y retirar del servicio todas las líneas y/o servicios que tuviere asignadas. Una vez detectado el hecho el **OPERADOR** tendrá derecho a suspender de inmediato el servicio, de lo cual se dará aviso posterior al **CLIENTE**, sin perjuicio de que se adelante el procedimiento de terminación o corte de los servicios prestados.
3. Sin perjuicio de las demás sanciones aplicables, en caso de que el **CLIENTE** sea detectado reoriginando tráfico internacional, nacional o móvil entrante simulándolo como local deberá pagar al **OPERADOR** la cantidad de minutos cursados desde la fecha de instalación hasta el momento de la terminación por el valor del cargo de acceso que el **OPERADOR** tenga establecido en promedio con los operadores de TPBCLD Y en el evento de tratarse de reoriginamiento de tráfico móvil, el valor regulado por minuto para las llamadas fijo-móvil.
4. En caso de que el **OPERADOR** tenga conocimiento de la existencia del tipo de contenidos relacionados en el numeral 4 de la cláusula segunda del presente anexo, en su propia infraestructura, se denunciará al **CLIENTE** ante la autoridad competente y procederá a retirarlos y a terminar los contratos unilateralmente, sin perjuicio de las sanciones administrativas y penales a que haya lugar.



5. En caso de que el **OPERADOR** detecte falsedad en los documentos y/o en la información presentada por el **CLIENTE** para adquirir cualquiera de los servicios ofrecidos por el **OPERADOR** o como prueba en cualquiera de los trámites ante el **OPERADOR**, procederá a dar por terminado unilateralmente el contrato, sin perjuicio de las demás sanciones a que haya lugar.

#### **CLAUSULA CUARTA: DERECHO DE INSPECCIÓN**

En caso de que el **OPERADOR** requiera practicar sin previo aviso visita de terreno para hacer la verificación de un presunto fraude detectado, el **CLIENTE** deberá facilitar la inspección en sus instalaciones o en cualquier parte de la red y permitir la entrada a éstas a una persona plenamente identificada y autorizada por el **OPERADOR** para hacer las corroboraciones a que haya lugar. De la visita de terreno se debe levantar un acta en la que se deje constancia de lo ocurrido en la visita.