

Política antifraude EXTERNA

(Es externa y está publicada en el sitio web desde la siguiente página, no reemplaza a la política antifraude interna)

Código del documento: POLT-FACC-002

Versión: 1.0

Área Responsable: Jefatura riesgos y auditoría

Áreas involucradas: Toda la compañía

LLEGAMOS A CAMBIAR LA TELEFONÍA MÓVIL



1. Marco de Actuación

Partners Telecom Colombia S.A.S. (en adelante PTC), y su marca WOM, en el ejercicio de su responsabilidad social, en congruencia con sus valores corporativos y objetivos estratégicos, establece la presente Política de Gestión del Riesgo de Fraude. Esta política establece los principios, valores y el comportamiento esperado de La Empresa respecto a los incidentes de materialización de este riesgo y las afectaciones que produce a sus contrapartes.

2. Alcance

Esta Política aplica para el manejo de todos los eventos, alertas, acciones, incidentes, casos, reportes y alarmas que se deriven del riesgo de fraude, las acciones que se adelantarán por parte de PTC y los procedimientos de debido proceso para dar cumplimiento a lo establecido en las normas vigentes; así como para ejercer el derecho que le asiste como empresa legalmente constituida, a resguardar sus intereses económicos de quienes obrando de mala fe, intentan obtener un beneficio propio o para un tercero en detrimento de los ingresos, imagen y sostenibilidad de la Compañía.

3. Glosario

Para las disposiciones de esta Política se tratará el fraude en telecomunicaciones de acuerdo con lo establecido en publicaciones de organismos de la industria, tales como el ITU (Unión Internacional de Telecomunicaciones por sus siglas en inglés), la GSMA¹ y TM Forum², así como las futuras actualizaciones que se realicen sobre las mismas. Para el entendimiento de lo que se considera fraude, Partners Telecom Colombia define a continuación las generalidades sobre las que basa la gestión de este:

- Fraude Externo es cualquier acción intencional ejercida por un individuo diferente a un empleado de la Compañía, por un grupo o empresa con el fin de recibir un beneficio para sí o para un tercero a través de: mentiras, engaños, delitos como el hurto y/o el uso indebido del servicio, de la marca, o de las herramientas que proporciona Partners Telecom Colombia a sus contrapartes. Dicha acción genera como consecuencia la pérdida de información, patrimonial, económica o reputacional, así como la afectación al cumplimiento de los objetivos estratégicos de Partners Telecom Colombia, en situaciones en las que se incumple el principio de presunción de buena fe.
- Fraude Interno es aquella eventual conducta cometida por uno o más empleados de Partners Telecom Colombia en el uso de sus funciones, cuyos principales medios son la autoridad, las atribuciones y los permisos conferidos a él o ellos por la compañía, y que tiene como finalidad el beneficio propio o de terceros que genere una afectación a los intereses de la Compañía.

Partners Telecom Colombia reconoce que el riesgo de fraude es intrínseco al sector de las telecomunicaciones móviles alrededor del mundo, y ha establecido mecanismos de mitigación del mismo, procurando reducir el nivel de riesgo asociado a las posibles materializaciones de éste, así mismo trabajará en conjunto con las instituciones del Estado y con las demás empresas del ecosistema móvil para desincentivar este tipo de prácticas.

¹ La GSMA representa los intereses de los operadores móviles en todo el mundo. [Fecha de consulta: Marzo 2021]. Disponible en: <http://www.gsma.com/>

² El TM Forum ayuda a los proveedores de servicios de comunicaciones (CSP) y sus proveedores a transformarse digitalmente y prosperar en la era digital. Hacemos esto proporcionando un entorno colaborativo abierto y soporte práctico que permite a los CSP y proveedores transformar rápidamente sus operaciones comerciales, sistemas de TI y ecosistemas para capitalizar las oportunidades que se presentan en un mundo digital en rápida evolución. [Fecha de consulta: Marzo 2021]. Disponible en: <https://www.tmforum.org/>



4. Principios Rectores

- **Honestidad:** Partners Telecom Colombia procurará actuar siempre de manera transparente y honesta ante sus usuarios, accionistas, proveedores, socios comerciales, empleados y en general todas sus contrapartes; adoptando una postura de cero tolerancia al fraude y ante cualquier actuación que atente contra la veracidad y la confianza que debe prevalecer en las relaciones con sus contrapartes. No aceptará de ninguno de sus representantes o empleados que actúen en forma contraria a este principio, que así mismo se configura como uno de sus valores.
- **Confidencialidad:** El fundamento de esta política se basa en conservar una estricta reserva por parte del área de Control Fraude. Esta reserva implica el compromiso de no revelar ninguna información obtenida durante una investigación para fines diferentes a los requeridos para adelantarla. De igual forma la persona denunciante se compromete a guardar reserva de la información que le sea requerida, de la investigación que se adelante y de las personas que participan de la misma.
- **Celeridad:** Dados los impactos que produce el fraude, toda alerta de fraude será gestionada en el menor tiempo posible, primando el compromiso de tomar acciones oportunas de manera temprana y en lo posible automáticas. Este principio le impone exigencias, responsabilidades y deberes permanentes al área de Control Fraude. Así mismo, se espera una participación y denuncia oportuna de cada persona que tenga conocimiento de una situación de fraude en la empresa o que afecte sus intereses.
- **Debido Proceso:** Todo cliente, empleado, proveedor o socio comercial tiene el derecho a que se asegure que el proceso de investigación sea realizado de la manera más transparente posible, permitiendo ser escuchado y exponer las justificaciones debidas ante cualquier situación en la que se presuma la ocurrencia de un fraude, partiendo del principio de buena fe y moral de todas las personas.

5. Directrices

Partners Telecom Colombia cuenta con un área de Riesgos & Auditoría con funciones de Control de Fraude que se encargará de:

- Identificar oportunamente los riesgos de fraude existentes en la prestación de los servicios y de implementar medidas preventivas que reduzcan la probabilidad y/o el impacto de incidentes de fraude, así mismo evaluará de manera periódica la eficiencia de estas medidas para ajustar los controles ante las variaciones que se identifiquen en su frecuencia de materialización y ante los cambios en el contexto externo e interno de la Compañía.
- Investigar todos los casos o alertas de posible fraude que se reciban como denuncia y los que se evidencien con base en controles y monitoreo de las diferentes operaciones relacionadas con clientes, canales de ventas, activación, facturación, recaudos, compras, contrataciones, prestación de servicios, inventarios y activos fijos, entre otras.
- Gestionar con el apoyo de diferentes áreas de la compañía que se ejecuten los recursos administrativos y/o legales para el cobro o recuperación de los bienes o derechos económicos que haya perdido o en los que se vea afectado Partners Telecom Colombia ante un evento de fraude.
- Promover a través de entrenamientos y capacitaciones una cultura de autocontrol, de denuncia y de cero tolerancia al fraude y a comportamientos deshonestos en la operación, ayudando a los

LLEGAMOS A CAMBIAR LA TELEFONÍA MÓVIL



empleados y contrapartes a identificar las situaciones que puedan estar asociadas a eventos irregulares o actos indebidos.

- Poner en conocimiento de las autoridades nacionales los hechos que se configuren como posibles delitos, así mismo instar a sus contrapartes a cumplir con este deber ciudadano.
- Informar oportunamente los casos de fraude a las directivas de la empresa y a las áreas que pudieran resultar afectadas, así como las revisiones y actualizaciones sobre las plataformas, controles y en general todo el sistema de gestión de riesgos de fraude de la compañía.

6. Generalidades

- La presente Política establece un marco de referencia para el tratamiento de situaciones asociadas a fraude, sin embargo se debe contemplar que las ofertas comerciales, promociones, servicios especiales o suplementarios, incentivos y en general cualquier producto o servicio que se comercialice y sus condiciones de activación y de comercialización a través de los diferentes canales, pueden establecer condiciones particulares que harán parte integral del marco de gestión del riesgo de fraude y que se establecerán en los términos y condiciones particulares de cada uno. El área de Riesgo & Auditoría velará por que exista coherencia entre los diferentes lineamientos que se emitan.
- Todas las promociones y beneficios se pierden en caso de identificarse y comprobarse un evento de fraude, o una actuación de mala fe por parte del cliente. Así mismo, los cumplimientos y bonificaciones comerciales excluirán todas las ventas que estén relacionadas con los eventos descritos en este punto, que incluyan o no las promociones y los beneficios, o sobre las cuales se haya incumplido alguna política.

7. Obligaciones de los clientes

Partners Telecom Colombia establece a continuación las obligaciones generales que aplican para todos los servicios y modalidades de contratación, las cuales incluyen servicios en modalidad prepago y pospago, así como los diferentes servicios que son ofrecidos a nuestros clientes, incluyendo los servicios ilimitados.

Obligaciones generales:

Conforme a la regulación expedida por la CRC, como usuario usted tiene -entre otras- las obligaciones de hacer uso adecuado de las redes, de los servicios y de los equipos necesarios para la prestación de los mismos y actuar de buena fe durante toda la relación contractual. Si PTC advierte el uso indebido del servicio de voz móvil, datos o SMS, le informará dicha circunstancia y tomará las medidas necesarias para preservar el buen uso de redes y servicios si fuera necesario. Se entiende por uso indebido del servicio: i) el uso abusivo o fraudulento del servicio mediante su explotación comercial, incluido pero no limitado a la reventa, reoriginación de llamadas y uso en plantas telefónicas; y ii) el uso del servicio con fines ilegales (como medio para la materialización de delitos, incluido pero no limitado a suplantación, estafa, extorsión, delitos informáticos, entre otros). En caso de comprobarse, con fundamento en nuestros procesos de control del fraude, que dicho uso indebido persiste, de conformidad con la regulación vigente, y una vez agotadas las instancias de debido proceso, PTC podrá dar por terminado el contrato o desactivar la línea móvil.

LLEGAMOS A CAMBIAR LA TELEFONÍA MÓVIL



Obligaciones particulares de los clientes y medidas de prevención:

Adicional a las obligaciones previamente establecidas, a continuación se establecen obligaciones aplicables a diferentes situaciones susceptibles de generar riesgo de fraude (factores de riesgo) y medidas que define PTC para prevenir y mitigar el riesgo de Fraude. En el caso de los servicios que presta PTC, las presentes obligaciones no son aplicables a los que se ofrezcan como ilimitados.

Datos: Es considerado un uso fraudulento del servicio aquel que se realiza mediante la instalación de aplicaciones en el dispositivo de navegación, y que tiene por objeto engañar o sustituir la manera como la red registra y controla el tráfico. De igual manera, el uso del servicio es de carácter personal, no se encuentra autorizado el uso para reventa del servicio; las aplicaciones, uso o explotación de tipo comercial (tales como Café Internet, comercialización por suscripción, entre otras) está estrictamente prohibido. El usuario debe abstenerse de este tipo de prácticas, y en caso de hacerlo, podrá estar sujeto a controles de velocidad, suspensión del servicio y/o terminación del contrato.

SMS: El usuario debe abstenerse de realizar prácticas consideradas como fraudulentas, tales como el envío de SMS publicitarios, mensajes no deseados por el cliente que los recibe (SPAM), ofertas falsas (incluyendo smishing e intentos de estafa), el envío de un alto número de mensajes en muy corto espacio de tiempo (flooding). La comisión de dichas prácticas puede llevar a la suspensión del servicio y/o terminación del contrato de manera unilateral por parte de la empresa.

Voz: Es considerado un uso fraudulento del servicio la reoriginación de llamadas provenientes del exterior del país con terminación en una red PLMN o PSTN por un usuario móvil de PTC (Bypass). Así mismo, se considera un uso fraudulento del servicio de voz la realización de llamadas a números de emergencia, o líneas gratuitas de servicio al cliente, en gran cantidad, o de larga duración o con propósito diferente a la naturaleza de estos servicios. El usuario debe abstenerse de realizar este tipo de prácticas y, en caso de hacerlo, podrá estar sujeto a suspensión del servicio y/o terminación del contrato.

Equipos: Como medida de prevención de una posible afectación a nuestros clientes, a la disponibilidad de los equipos terminales móviles (ETM) para nuestros clientes, y a los ingresos de la Compañía, se establecen las siguientes condiciones respecto a la compra de equipos con cualquier tipo de descuento o beneficio:

- El cliente podrá comprar cada seis (6) meses un máximo de un (1) equipo por cada línea que tenga a su nombre en prepago o postpago.
- El cliente podrá pagar de contado (efectivo o tarjeta debito) la cantidad de equipos que corresponda al número de líneas activas a su nombre, y que estén dentro del lapso permitido para renovación, el cual se aplicará por un periodo de seis (6) meses a partir de la fecha de compra de manera individual. Esto quiere decir que, si el cliente adquirió los equipos en diferente fecha, el plazo se contará de manera independiente a partir de la fecha de adquisición de cada equipo
- Si el pago es a través de tarjeta de crédito, el cliente podrá pagar usando este medio de pago hasta un máximo de tres (3) equipos. Los equipos restantes que le permita la cantidad de líneas que tenga a su nombre para aplicar descuentos, o los demás equipos adquiridos en modalidad libre, deberán ser pagados de contado.

De manera específica, para cada promoción se podrá definir una cantidad menor de equipos que pueden ser comprados por una misma persona, dichas restricciones serán establecidas en los Términos y Condiciones de cada oferta (TyC). Los equipos que se ofrecen sin promoción, en modalidad libre o sin línea móvil asociada y con pago de contado no tienen un límite establecido por defecto, sin

LLEGAMOS A CAMBIAR LA TELEFONÍA MÓVIL



embargo, podrán ser sujetos a otro tipo de análisis de riesgos, incluido pero no limitado al riesgo de Lavado de Activos y Financiación del Terrorismo.

8. Modalidades de fraude y medidas adoptadas

Fraude suscriptor

PTC tiene implementadas herramientas tecnológicas para prevenir los casos de suplantación de identidad, sin embargo, si usted es víctima de una suplantación de identidad, en la que fueron adquiridas líneas a su nombre que no reconoce, puede reportarlo por cualquiera de nuestros canales de atención. Dicha información será dirigida al área correspondiente para su investigación, los formatos y documentos que se solicita diligenciar tienen como finalidad recibir la información exacta de la situación presentada y evitar generar afectaciones mayores a los usuarios que puedan estar en esta situación, ya que en algunos casos pueden existir líneas móviles que sí fueron adquiridas y son utilizadas por la persona que pudo ser suplantada.

Fraude de Larga Distancia Internacional

Para las líneas cuenta control o híbridas y para los suscriptores en modalidad prepago, el acceso al servicio de LDI se realiza a través de recarga o de compra de paquetes, con el objetivo de que el cliente en PTC tenga total control de los consumos que realiza, acorde al plan que ha seleccionado. Para el caso de clientes en modalidad pospago, se establecerá un cupo de crédito con base en el perfil de riesgo del cliente. No obstante, y dado que es posible que el cliente utilice el servicio de LDI mediante la modalidad de multiacceso, y con el propósito de evitar eventos de fraude que el cliente no pueda controlar, PTC tiene implementadas herramientas tecnológicas para identificar llamadas con perfil de fraude que podrán llevar al bloqueo del servicio de LDI, o la suspensión de la línea dependiendo el nivel de riesgo asociado a la alerta generada.

Portabilidad numérica

Para las solicitudes de portabilidad que se reciban a nombre de personas jurídicas como usuarias de líneas en prepago, se realizarán las validaciones pertinentes, utilizando las herramientas tecnológicas que nos permitan generar reglas para identificar situaciones de fraude. Así mismo, se realizarán procesos similares para las solicitudes masivas o individuales de portabilidad que puedan corresponder a alertas tempranas de fraude, sobre las que se han identificado riesgos asociados a prácticas en el sector que terminan afectando clientes y, en algunos casos, generando actuaciones que se salen de la presunción de buena fe del cliente para realizar el proceso.

Atendiendo lo establecido en la Ley 1801 del 2016 (Código Nacional de Policía y Convivencia) y específicamente en el Capítulo IV, Artículo 95, numeral 12 y 13, no se podrá activar una línea y su respectiva SIM Card sin que el usuario haya proporcionado sus datos biográficos, los cuales se presumen entregados de buena fe, reales, y que corresponden al usuario que realiza el proceso de activación. En los casos en los que el cliente considere que el rechazo por fraude a su solicitud de portabilidad ha sido injustificado, este podrá realizar los procesos de activación de la línea requeridos, o de normalización de su situación de posible fraude. Si este procedimiento no es efectivo, también podrá hacer uso de los canales de atención, para solicitar que se revalúe el motivo de este rechazo. De igual manera, se establece que una línea en modalidad prepago solo estará activa hasta tanto el cliente realice una recarga de saldo, salvo los casos en los que se trate de una SIM Card promocional en cuyo caso, ésta ya cuenta con una recarga de obsequio.

Fraude en medio de pago

LLEGAMOS A CAMBIAR LA TELEFONÍA MÓVIL



Tanto para el pago de equipos, como para el pago de servicios, cuando éste sea realizado con tarjeta de crédito o cheque y sea rechazado por el banco, se realizará la desaplicación del pago en el sistema, lo cual podrá generar que la factura sujeta a esta desaplicación del pago genere un estado de mora, y que, en consecuencia, se disparen los procesos de recuperación de cartera a que haya lugar. Se considera así mismo un intento de fraude el realizar por cualquier medio la alteración de los equipos o sistemas de la red, o en el mismo dispositivo de acceso, de tal manera que se logre modificar la medición del consumo para la facturación de alguno o todos los servicios prestados por PTC, o que de forma alguna logre que se sustraiga su pago.

Estafas e Ingeniería social

PTC es consciente que el servicio de voz, SMS y de datos puede ser utilizado para engañar a los clientes actuales y potenciales con promociones, sorteos y premios que no corresponden a la realidad, o a los ofrecidos por la Compañía. Esta modalidad de fraude se aprovecha de las reacciones intensamente emotivas que pueden generar en la mayoría de personas ciertas situaciones poco probables: premios de alto valor (vehículos, altas sumas de dinero en efectivo), eventos o circunstancias de peligro (requerimientos penales, cierre de cuentas o imposibilidad de acceder a información importante), circunstancias que apelan a la solidaridad o ayuda masiva (campañas de donación, protección de derechos). En caso de que reciba una comunicación por cualquier medio (mensaje de texto, llamada de voz, correo electrónico o notificación del navegador en un teléfono inteligente o computador, entre otros) en la que se mencione un beneficio, concurso o un premio a nombre de PTC, lo invitamos a corroborar la información a través de nuestra página web y canales de atención (números de atención y redes sociales). En ningún caso PTC le solicitará que realice recargas, pagos o que suministre contraseñas o claves para participar en los concursos. De igual manera, PTC lo invita a ser cuidadoso con los hipervínculos y documentos adjuntos que puedan contener correos electrónicos enviados a nombre de la Empresa, ya que en algunos casos pueden ser aprovechados para cometer estafas o robar información personal. Por último, es recomendable el uso de herramientas de múltiple factor de autenticación siempre que estén disponibles, así como tener cuidado con el acceso a internet desde redes públicas abiertas desde los equipos que utiliza para sus transacciones privadas, ya que la información que viaja a través de estas redes puede estar siendo capturada por personas inescrupulosas con fines delictivos.

Hurto administrativo de equipos

Cuando se identifiquen equipos hurtados, sustraídos indebidamente o robados de nuestras bodegas; o que hayan sido obtenidos mediante maniobras fraudulentas, engaños o suplantación en una operación de venta, además, en los casos en los que este equipo no haya sido pagado en su totalidad, PTC procederá a realizar el reporte del ETM (equipo terminal móvil) en bases negativas con motivo fraude o hurto administrativo, bajo las disposiciones legales existentes en esta materia. Para proceder con el retiro del reporte, el poseedor del equipo deberá demostrar su procedencia legal y/o eventualmente trasladar su queja a quien vendió dicho equipo para que aclare la situación que se registra en PTC y la cual dio origen a dicho reporte.

Spoofing de sitio web

Cuando ingrese a la página web de WOM, no lo haga a través de hipervínculos que le hayan llegado por correo electrónico, mensajes de redes sociales o mensajes de texto, procure siempre digitar la dirección en su navegador y hágalo desde un dispositivo que tenga las medidas de seguridad recomendadas (antivirus instalado y actualizado, sistema operativo que incluya las más recientes actualizaciones de seguridad y equipos que no sean de uso público o compartido con desconocidos). La URL de la página web de WOM es: <https://www.wom.co> debe tener cuidado si la dirección es diferente, ya que hay una muy alta probabilidad de que se trate de un sitio que intenta suplantar la

LLEGAMOS A CAMBIAR LA TELEFONÍA MÓVIL



página web oficial, en general, los estafadores utilizan información de la página real y varían ligeramente la dirección URL con el objetivo de confundir a quien se dirige a esta página falsa. De igual manera, cualquier intento de crear identidades falsas de la Empresa, sus funcionarios o sus canales de venta y distribución; o que induzcan a confusión en los clientes actuales o potenciales sobre la identidad de la marca o las funciones atribuidas a las personas, serán consideradas eventos de fraude y podrán generar consecuencias administrativas, disciplinarias y legales. En caso de que para este fin se estén utilizando servicios de la compañía, éstos podrán ser sometidos a suspensión o terminación de contrato.

Integridad y privacidad de las comunicaciones

PTC cuenta con medidas estándar de cifrado para el registro de las líneas móviles en su red mediante mecanismos de autenticación mutua, así como mecanismos de cifrado de las llamadas para impedir que las líneas telefónicas puedan ser clonadas o intervenidas. No obstante, en cumplimiento de las disposiciones nacionales en materia de interceptación legal de llamadas, PTC provee los mecanismos para que las autoridades competentes de acuerdo con la legislación nacional realicen dichos procedimientos mediante el uso de este mecanismo. Así mismo, ha implementado procesos y herramientas para evitar que la información de los clientes pueda ser accedida de manera involuntaria por personal no autorizado. Cualquier intento de violar el derecho a la privacidad de cualquiera de los servicios prestados por PTC, o la intimidad de las personas, bien sea por medio de intentos de interceptación ilegal, grabación de las comunicaciones, intentos de acceso a la red mediante herramientas intrusivas (hacking) o de escucha (sniffer), uso de sistemas de descubrimiento de vulnerabilidades o intentos de obtención o quiebre de contraseñas, la simulación de mensajes de señalización o señales de radioacceso, la instalación de dispositivos o software de acceso a los equipos de la red o de los clientes sin su consentimiento, el utilizar conexiones físicas o lógicas a la red o a los servicios violando o alterando los mecanismos de protección establecidos, será considerado como intento de fraude y podrá ser sometido a procedimientos de suspensión o terminación del servicio.

Disponibilidad de la red y plataformas tecnológicas

PTC ha implementado herramientas y plataformas que procuran que se preserve la disponibilidad de los sistemas de información en los que se soporta la operación de la red de telecomunicaciones y los servicios de TI requeridos para su soporte, cualquier intento de generar indisponibilidad de la red o de los servicios mencionados mediante ataques de denegación distribuida del servicio (DDOS), la utilización de equipos que incumplan las normas técnicas, o que no se encuentren homologados en el territorio nacional, la alteración de las señales de radio producidas por los dispositivos de acceso a la red, el uso de categorías o mecanismos de programación remota mediante códigos de las centrales, la simulación de mensajes de la red o de alguno de sus servicios para falsear protocolos de comunicación, la violación o intento de violación a la seguridad de la red, sus sistemas de protección o los de terceros que participen en la generación, transmisión o recepción de las comunicaciones de los clientes, o cualquier intento de acceso no autorizado, uso desproporcionado de recursos de red, conexiones que impidan a otros clientes acceder a los servicios, será catalogado como posible fraude y se tomarán las medidas correspondientes que podrán incluir la suspensión del servicio y/o la terminación del contrato.

LLEGAMOS A CAMBIAR LA TELEFONÍA MÓVIL

