Nº 00129-DAPU/2021

A	**:**	SERGIO ENRIQUE CIFUENTES CASTAÑEDA **GERENTE GENERAL**
ASUNTO	**:**	PROYECTO DE MODIFICACIÓN NORMATIVA DEL TEXTO ÚNICO ORDENADO DE LAS CONDICIONES DE USO DE LOS SERVICIOS PÚBLICOS DE TELECOMUNICACIONES.
FECHA	**:**	**3 de diciembre de 2021**

		CARGO	**NOMBRE**
ELABORADO POR	:	ESPECIALISTA ECONÓMICO PRINCIPAL	YOEL RIOS ARROYO
		COORDINADORA LEGAL	MATILDE JUDITH GONZALEZ VILLANUEVA
REVISADO POR	:	SUBDIRECTORA DE PROTECCIÓN DEL USUARIO	HAYINE GUSUKUMA LOZANO
APROBADO POR	:	DIRECTORA DE ATENCIÓN Y PROTECCIÓN DEL USUARIO	TATIANA PICCINI ANTON

ÍNDICE

1. OBJETIVO

El presente documento tiene por objeto sustentar el proyecto de modificación normativa del "Texto Único Ordenado de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones" (en adelante, Condiciones de Uso), el cual atienda la problemática de contratación y activación del servicio público móvil (tales como contrataciones no solicitadas, cuestionamiento de titularidad de líneas prepago y reposición fraudulenta de chips en el servicio público móvil) a través de los diferentes canales de atención a usuarios sean presenciales o digitales.

2. DECLARACIÓN DE CALIDAD REGULATORIA

En aplicación de lo dispuesto por la Resolución N° 069-2018-CD/OSIPTEL[1], se declara que el proyecto normativo que se sustenta en el presente informe cumple con los Lineamientos de Calidad Regulatoria.

3. ANTECEDENTES

En virtud de la función normativa del OSIPTEL, establecida en el artículo 3 de la Ley Marco de los Organismos Reguladores de la Inversión Privada en Servicios Públicos (Ley N° 27332)[2], este organismo aprobó, mediante la Resolución N° 138-2012-CD/OSIPTEL[3], la norma de las Condiciones de Uso, en la que se establecen los derechos y obligaciones que corresponden a abonados, usuarios y empresas operadoras de los servicios públicos de telecomunicaciones, tanto al momento de la contratación del servicio, durante la provisión del mismo, así como al término de la relación contractual.

Asimismo, considerando la dinámica propia del mercado de los servicios públicos de telecomunicaciones, el OSIPTEL ha dispuesto una continua evaluación de las normas establecidas en las Condiciones de Uso, a fin de que estas cumplan con eficiencia con el objetivo de evitar la vulneración de los derechos de los usuarios o la aplicación de prácticas comerciales que podrían resultar lesivas o riesgosas para los usuarios. Es por ello, que Condiciones de Uso ha sido actualizada y modificada parcialmente mediante las resoluciones N° 095-2013-CD/OSIPTEL, 138-2014-CD/OSIPTEL, 056-2015-CD/OSIPTEL, 096-2018-CD/OSIPTEL, 224-2018-CD/OSIPTEL, 006-2020-CD/OSIPTEL, 163-2019-CD/OSIPTEL, 138-2020-CD/OSIPTEL, 153-2020-CD/OSIPTEL y 019-2021-CD/OSIPTEL.

Al respecto, se debe señalar que mediante la Resolución N° 056-2015-CD/OSIPTEL[4] el OSIPTEL dispuso que la contratación del servicio público móvil prepago se realice a través de una verificación biométrica, con la finalidad de contar con un registro de abonados confiable, a fin de que no se registren bajo la titularidad del usuario servicios que no contrató, que las empresas operadoras tengan un registro de los distribuidores autorizados que participan en la contratación del servicios, que los usuarios con más de 10 líneas tengan que realizar sus contrataciones adicionales de manera presencial, que la reposición del SIM card se realice de manera presencial y previa verificación biométrica, entre otras disposiciones.

[1] Publicada en el Diario Oficial El Peruano el 22 de marzo de 2018.
[2] Modificada en parte por la Ley N° 27631.
[3] Publicada en el Diario Oficial El Peruano el 27 de setiembre de 2012.
[4] Publicada en el Diario Oficial El Peruano el 5 de junio de 2015.

Por otra parte, mediante la Resolución N° 096-2018-CD/OSIPTEL[5], se amplía el uso de la verificación biométrica al servicio público móvil en las modalidades postpago y control, se establecen mayores reglas para la verificación no biométrica, y para evitar que terceros realicen cambios de SIM Cards sin consentimiento del abonado, perjudicando la correcta prestación del servicio, así como facilitando fraudes financieros, se dispuso que para hacer efectiva la reposición del *SIM card* siempre se realice la verificación biométrica o que la activación del servicio se realice mediante la contraseña única, entre otros cambios normativos.

En el caso de la Resolución N° 006-2020-CD/OSIPTEL[6], el OSIPTEL propuso cambios normativos para atender el problema de las contrataciones no solicitadas en el servicio público móvil y las suplantaciones en la verificación biométrica, tal como mejorar el proceso de validación de la identidad del abonado contratante, mantener informado al abonado sobre el inicio del proceso de portabilidad, contratación de líneas nuevas o cambios de titularidad y desincentivar la adquisición fraudulenta de equipos terminales.

Como se puede apreciar, estas tres modificaciones normativas han estado motivadas por la falta de medidas de seguridad en la contratación, activación o reposición de una línea o SIM Card del servicio público móvil, que no permiten contar con un registro de abonados confiable y evitar que terceros accedan a trámites que corresponden al titular del servicio. Sin embargo, a pesar de los esfuerzos del OSIPTEL por garantizar a los usuarios adecuados niveles de seguridad en el uso de los servicios públicos de telecomunicaciones, los casos de fraudes se han mantenido y se han diversificado las modalidades delictivas.

A nivel mundial, se aprecia una creciente tendencia por parte de las organizaciones criminales a vulnerar a los usuarios a través de los procesos de autenticación en los servicios públicos de telecomunicaciones, debido a que los *smartphones* contienen los datos personales de los usuarios y a que, en general, las empresas operadoras no suelen hacer un gran esfuerzo por garantizar que dichos procesos sean adecuadamente seguros.

En este contexto, es muy probable que este problema pueda incrementarse a niveles críticos, debido a que el uso del servicio público móvil y de los smartphones es cada vez más masivo e intensivo. Los usuarios cada vez más hacen uso de aplicativos (app) y servicios *web* que permiten a los usuarios realizar diversas transacciones y servicios *web* (pago de servicios, transferencias financieras, etc.).

Particularmente, en el caso de los *smartphones*, su diseño está orientado a integrar la información personal de los usuarios en el uso de los diversos aplicativos y, por tanto, almacenan una importante cantidad de información sensible de los usuarios (ubicación, lugares de visita frecuente, contactos del usuario, datos financieros, etc.). Estas características se han convertido en un objetivo para la delincuencia, ya sea para acceder a esa información o para cometer actos delictivos.

El OSIPTEL, en atención a estos riesgos y buscando evitar que se suplante la identidad del abonado al momento de la contratación del servicio u otros trámites relevantes que inciden en la continuidad de la prestación del servicio, ha encontrado que la contratación y activación del servicio público móvil requiere ser realizada bajo ciertas condiciones mínimas de seguridad, y que, por ello, su comercialización no puede ser concebida

[5] Publicada en el Diario Oficial El Peruano el 1 de mayo de 2018.
[6] Publicada en el Diario Oficial El Peruano el 9 de enero de 2020.

como si se tratase de un bien cualquiera, que puede ser entregado o transferido en cualquier lugar de la ciudad, sin ningún tipo de control o supervisión.

Considerando que la problemática antes mencionada se mantiene e incluso se ha diversificado con la aparición de fraudes a través de la suplantación de usuarios en el proceso de reactivación de líneas suspendidas, se ha visto conveniente formular una nueva propuesta normativa, que atienda los nuevos riesgos que amenazan a los usuarios.

4. REGULACIÓN BASADA EN RIESGOS

Actualmente, los *Smartphone* o teléfonos inteligentes ofrecen diversos aplicativos y funcionalidades que requieren de la información personal e incluso financiera de los usuarios. No obstante, se debe señalar que, además de los evidentes beneficios de estos teléfonos; han surgido también paulatinamente nuevos riesgos. En efecto, la delincuencia ha puesto la mira en los *Smartphone*, los *chips* y los aplicativos móviles, y ha encontrado diversas oportunidades de utilizar la información de los usuarios, registrada en estos equipos, para cometer fraudes y estafas.

En este contexto, dado que el objetivo de este informe es evaluar la problemática relacionada con este tipo de riesgos, se ha considerado pertinente que en esta sección se realice una exposición general sobre el enfoque de regulación basado en riesgos. Así, mediante esta revisión previa, se busca proveer de un marco conceptual y teórico que facilite el análisis de esta problemática y la propuesta de alternativas de solución.

4.1. Aspectos económicos del riesgo

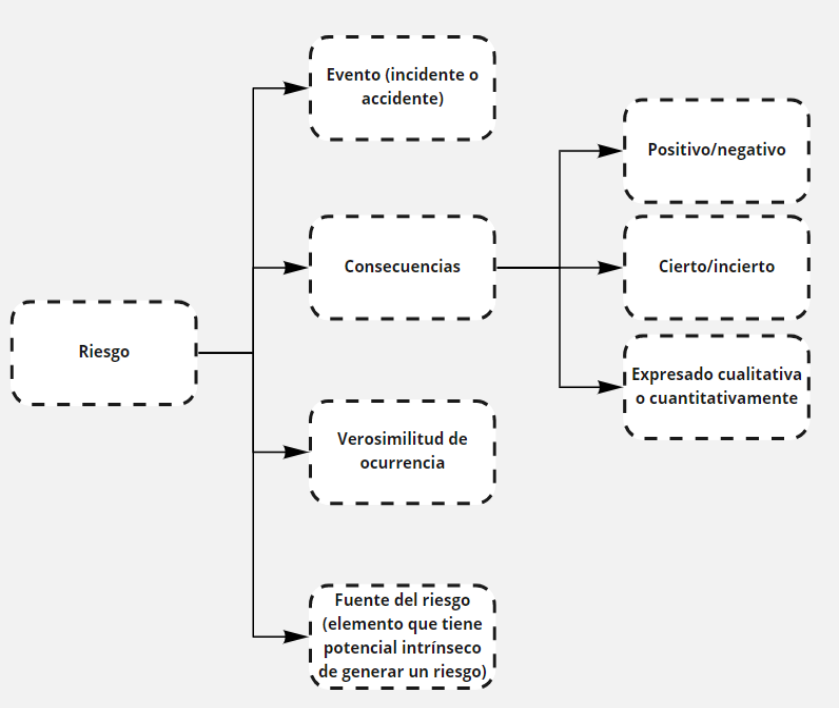
El ISO 31000: 2009 define el riesgo como el efecto de la incertidumbre en los objetivos o como una desviación en los resultados esperados[7]. Los componentes principales del riesgo[8] son la probabilidad o verosimilitud y el impacto o consecuencia; no obstante, también se pueden tomar en cuenta otros componentes: el evento que podría desencadenar el riesgo, la fuente del riesgo y los tipos de consecuencias (ver figura N° 1).

Siguiendo la conceptualización del ISO 31000: 2009, el evento es definido como una o varias ocurrencias o cambios de un conjunto particular de circunstancias, aunque también la no ocurrencia de algo podría conceptualizarse como un evento. Los eventos se clasifican en accidentes e incidentes. Asimismo, la fuente del riesgo se define como un elemento que solo o en combinación con otras fuentes tiene intrínsecamente potencial de generar un riesgo.

Por otro lado, la verosimilitud, según el ISO 31000: 2009, es el parámetro menos conocido que influye en el riesgo, en tanto que es la probabilidad de que algo suceda. Cabe señalar que la probabilidad del riesgo es desarrollado por las personas a partir de sus creencias respecto a la verosimilitud del riesgo, mediante una función de distribución “subjetiva”[9]. Así, según Hirshleifer J. y Riley J. G. (1992), un alto grado de confianza subjetiva sobre cómo se desarrollarían los eventos reflejaría una distribución de probabilidad poco dispersa o concentrada; mientras que un alto grado de duda, supondrían una gran dispersión en la probabilidad.

[7] Esta referencia se tomó de UN (2013).
[8] En la literatura económica riesgo e incertidumbre tienen el mismo significado, salvo en el caso de Knigth (1991), quien propuso diferenciarlos en función de si la probabilidad es objetiva o subjetiva.
[9] Fisher, I. (1912) y Savage, L. J. (1954).

Figura N° 1:
COMPONENTES DEL RIESGO



Fuente: *United Nations* (2013).

Desde un enfoque de la teoría neoclásica, los agentes económicos actúan de manera racional y, por tanto, son capaces de evaluar el riesgo ponderando el impacto y la probabilidad de ocurrencia, y maximizando su utilidad esperada. Cabe señalar que la utilidad esperada se define como la esperanza matemática de la utilidad que se obtendría con y sin el evento adverso que produce el riesgo. Siguiendo la definición formal de Neumann-Morgenstern (1944), esta sería una suma ponderada de las probabilidades de ocurrencia y las utilidades de cada estado de naturaleza:

$$U(x) = \pi_1 v(c_{x1}) + \pi_2 v(c_{x2}) \quad (1)$$

Donde, π_1 y π_2 son la probabilidad de ocurra o no ocurra el evento adverso, c_{x1} y c_{x2} son las consecuencias en cada escenario, v es la utilidad de cada escenario y U es la utilidad esperada del acto x. Esto implica que, en un contexto de incertidumbre, las decisiones racionales de los individuos se ven influenciado no solo por la utilidad de tener o adquirir un bien, sino también por los eventuales riesgos que implican.

En cambio, desde el enfoque de la economía institucional[10], los riesgos forman parte de aquellos imprevistos no contemplados en los contratos, o como lo indica Oehler A. et al. (2015), se trata de situaciones donde los individuos son incapaces de determinar las consecuencias potenciales de decisiones específicas o la probabilidad de ocurrencia de sus consecuencias. En abstracto, un contrato es todo acuerdo que genera una transacción, los cuales por definición serían incompletos debido a las asimetrías de información y demás factores que se encuentran fuera del control de las partes.

[10] La economía institucional fue desarrollada por Willianson Oliver E. (1985) y Coase. Ronald H. (1937)

Por otra parte, desde el enfoque de la economía del comportamiento[11], los individuos no serían racionales como lo plantea la teoría neoclásica, sino que tendrían más bien una racionalidad limitada que les induciría en algunos casos a actuar de manera irracional o sesgada debido a la sobre carga de información, sobre carga de alternativas de elección, tasas de descuento hiperbólicas, etc. En este caso, los individuos no son capaces de identificar y cuantificar los riesgos y su percepción del riesgo puede ir cambiando, incluso estando en situaciones similares. Este enfoque permite un acercamiento a la dimensión psicológica del riesgo, y cómo ello puede inducir a los agentes económicos a adoptar decisiones inadecuadas.

4.2. El riesgo como problema regulatorio

La intervención del Estado, a través de la regulación económica, solo se justifica cuando las fuerzas de mercado no tienen la capacidad ni la dinámica suficiente para resolver las ineficiencias asignativas. En el caso de los riesgos, no se tendría que regular si en el mercado existen mecanismos eficientes para asignar y distribuir los riesgos, y cada agente económico pudiese elegir su grado de exposición. Cabe señalar que las soluciones privadas frente a los riesgos suelen ser los seguros, los cuales son mecanismos que permiten a los individuos mejorar su utilidad esperada.

No obstante, en muchos casos los riesgos podrían tener cierta magnitud y alcance que no puede ser manejado de manera eficiente solo por el mercado, y requiere de la Estado para poder afrontarlo. En este caso, el Estado podría asumir la responsabilidad de mitigar un riesgo, ya sea reduciendo la probabilidad de ocurrencia o la magnitud de su impacto, generando en las personas un incremento de su utilidad esperada y, por tanto, una mejora en el bienestar social. Cabe señalar que el bienestar social se suele concebir como una función de todas las utilidades individuales.

Cabe señalar que el Estado no debería asumir la responsabilidad de mitigar todo tipo de riesgo que amenace a las personas, dado que podría distorsionar la elección de los individuos respecto a su exposición al riesgo, e incentivar las conductas imprudentes. Es decir, la estrategia más recomendable es definir mecanismos de compartición de riesgos y definir una regulación gradual de los riesgos.

Al respecto, frente a un evento riesgoso, el regulador podría adoptar diversas acciones, como por ejemplo prohibir la ejecución de los actos que podrían desencadenar ese riesgo, establecer requisitos para autorizar la ejecución de esos actos y minimizar el riesgo, definir protocolos, etc. En cualquier caso, la decisión adoptada por el regulador podría terminar impidiendo que se realicen actos que no tenían una alta probabilidad de riesgo, o permitiendo actos que sí eran riesgosos. Por ello, según OECD (2010), el Estado podría cometer dos tipos errores:

- Error Tipo I: Subregular o permitir la ocurrencia de riesgos.
- Error Tipo II: Sobreregular o prohibir actos levemente riesgosos.

Estos dos tipos de errores ocurren cuando el regulador no ha realizado una adecuada medición de la probabilidad del riesgo, su magnitud e impacto. Sin embargo, se debe señalar que los riesgos usualmente tienen una naturaleza dinámica y con información limitada, por lo que el regulador requiere tener un enfoque adaptivo al momento de abordarlo. Esto quiere decir que, el regulador necesita reevaluar constantemente sus

[11] Este enfoque fue planteado por Herbert A. Simon (1955).

decisiones, y reajustar las medidas adoptadas ya sea para reducir el error tipo I o el error tipo II.

En ese sentido, resulta importante que el regulador incorpore el análisis de los riesgos con la finalidad de graduar su intervención, esta manera de proceder es lo que se ha denominado como regulación basada en riesgos. Según OECD (2010), las principales características de este tipo de regulación son:

- A cada actividad le corresponde un nivel de riesgo y por ende una medida que corresponda a dicho nivel.
- Estima la interacción entre las actividades reguladas (la disminución del riesgo de una actividad puede incrementar el riesgo en otra).
- Está sujeta a una evaluación continua de los riesgos y por ello es dinámica.
- Se identifica el nivel de riesgo y con base a ello se diseña la regla adecuada.

Por otra parte, la gradualidad de la regulación basada en riesgos supone cuatro niveles de intervención que se podrían plantear en función de la gravedad:

- Evitar el riesgo: prohibir actividades.
- Transferir el riesgo: buscar que otro agente incurra en el riesgo a través de contratos y seguros.
- Retener los riesgos: aceptar las pérdidas asociadas al riesgo mediante la definición de planes de manejo.
- Reducir los riesgos: disminuir la probabilidad de la ocurrencia del riesgo.

Cabe señalar que la regulación basada en riesgos se contrapone al principio precautorio que muchos reguladores suelen implementar. La aplicación de este principio implica regular a todos bajo el mismo estándar sin considerar los diferentes niveles de riesgo, no se consideran los efectos adversos de una regulación muy estricta, no se actualiza y, primero se implementa la regla y luego se evalúan si controla el riesgo.

5. RIESGOS EN LA PROVISIÓN DEL SERVICIO PÚBLICO MÓVIL

5.1. Contexto internacional

a) Amenazas y riesgos en el sector telecomunicaciones

Los avances tecnológicos han traído grandes beneficios a los hogares y permitido que las empresas incrementen su productividad y eficiencia. No obstante, también se han generado nuevos tipos de riesgos y amenazas, debido a que las tecnologías de información brindan a los delincuentes diversas oportunidades para acceder a los datos personales y financieros de muchos usuarios, y realizar fraudes y robos.

Al respecto, Squire Technologies (2020), una conocida empresa que trabaja en el desarrollo de soluciones informáticas contra las amenazas y fraudes, señala que los fraudes en el sector telecomunicaciones es una de las principales fuentes de pérdidas de ingresos.

Asimismo, el daño de los fraudes en el sector telecomunicaciones no se restringe a las pérdidas económicas que se generan a las empresas operadoras, dado que también restan valor a la marca, afectan la reputación de las empresas, etc.

Este nuevo escenario ha supuesto que las empresas operadoras cambien su enfoque respecto a los riesgos de fraude. Squire Technologies (2020) señala que tradicionalmente las empresas operadoras han tenido una estrategia reactiva orientada a tener solo plataformas de monitoreo de gran escala para la detección de fraudes; pero que no garantiza detener a los estafadores. En este contexto, lo que se requiere es que las empresas puedan detectar los fraudes en tiempo real, a fin de poder implementar medidas de defensa de manera ágil y eficiente.

Al respecto, Tamas K. (2021a) señala que las redes telefónicas son una de las más grandes y antiguas en el mundo, y representan el 48% de los ingresos mundiales del consumo electrónico, por lo que los estafadores han desarrollado instrumentos y prácticas para explotar y extraer parte de ese valor. Entre los principales tipos de fraudes se encuentran:

- Compartición de ingresos de números internacionales *premium*: En este caso, los estafadores realizan llamadas falsas a través de un número internacional Premium y cortan la llamada, de manera que inducen a los usuarios a devolver la llamada. Cabe señalar que este tipo de números internacionales permiten compartir los ingresos entre la empresa operadora y el titular del número, por lo que, al ejecutarse el fraude, parte de los ingresos será recibido por los estafadores.
- Bypass y arbitraje: El estafador enruta su llamada a través de internet para buscar la menor tarifa de terminación, y obtener llamadas baratas. En el arbitraje, el estafador aprovecha las diferencias de precios.
- Hackeo de las centrales telefónicas: Las centrales suelen estar basados en IP, por lo que son susceptibles de ser hackeadas.
- Compra en masa de tarjetas SIM y terminales móviles mediante tarjetas de crédito robadas con el objetivo de emular redes móviles residenciales.
- Contratación fraudulenta del servicio telefónico con documentos de identidad robados y tarjetas de crédito robados.
- Robo de la cuenta on line de los usuarios
- *SMS Phishing*, el cual consiste en enviar un SMS con información falsa y con la finalidad del que el usuario ingrese a un link que el robará información.
- *SIM Jacking* o *SIM Swapping*, consiste en reportar el robo o la pérdida de un celular ajeno, para poder solicitar la reposición del SIM card.

Como se puede apreciar, en la actualidad, existen muchos riesgos para los usuarios de los servicios públicos de telecomunicaciones, debido a que la delincuencia ha encontrado oportunidades para realizar diversos actos ilícitos. Esta situación no debe concebirse como ajeno a la industria o sector telecomunicaciones, sino como una amenaza a la imagen de las empresas operadoras y del regulador y, por supuesto, una posible vulneración al patrimonio e integridad de los usuarios de los servicios públicos de telecomunicaciones.

b) Reposición fraudulenta de *SIM card*

Entre las diversas amenazas o fraudes anteriormente mencionados, se debe destacar la reposición fraudulenta del *SIM card*, conocido también como *SIM Swap*. Este tipo de fraude consiste en que el estafador reporta el celular como robado y perdido, y hace bloquear la línea, para luego solicitar la reposición del *SIM card*. Una vez que ha

obtenido el nuevo *SIM card*, activa la línea y empieza a buscar tener acceso a las cuentas personales del usuario (correo electrónico, cuentas bancarias) para poder realizar algún tipo de transacción. Cabe señalar que esta práctica ha ganado notoriedad debido a la estafa sufrida por Jack Dorsey, CEO de *Twitter*.

En la figura N° 1, se puede apreciar que el modus operandi del estafador comienza con la obtención de la información personal existente en las redes sociales, la cual le sirve para elegir a la víctima y para definir la mejor estrategia para lograr engañar a los protocolos de autenticación de las empresas operadoras.

En un segundo momento, el estafador hace contacto con los asesores de las empresas operadores, buscando engañarlos para poder desactivar o bloquear el *SIM card* de la víctima. Se ha observado que actualmente los estafadores pueden realizar verificaciones biométricas fraudulentas, hacerse pasar por apoderados, etc.

Una vez logrado, la desactivación de la línea de la víctima, el estafador solicitará la reposición del Chip o *SIM card*, con el objetivo de activarlo en un equipo de su propiedad, y así obtener acceso a las cuentas financieras de la víctima, y poder ejecutar el robo. Usualmente, los usuarios no suelen ser conscientes que su *SIM card* ha sido bloqueado, por lo que brindan al delincuente el tiempo necesario para poder ejecutar su plan.

Figura N° 2
REPOSICIÓN FRAUDULENTA DEL *SIM CARD* (*SIM SWAP*)

Fuente: Squire Technologies (2020), What is SIM Swap Fraud.

Cabe señalar que, el *SIM Swapping* continúa atacando a las empresas de telecomunicaciones. Tamas K. (2021b) enfatiza que, a pesar de las alertas existentes respecto a este tipo de fraude, las empresas de telecomunicaciones no han

desarrollado algo nuevo, y el *SIM Swap* sigue creciendo de manera rampante y sin control, al igual que los ataque a las cuentas on line de los usuarios.

Por otra parte, Kaspersky Lab[12], una empresa dedicada al desarrollo de soluciones informáticas contra el hackeo y otras amenazas, ha señalado que el SIM Swapping es una modalidad de fraude ampliamente utilizado por cibercriminales en América Latina y África. Por ejemplo, en Brasil se han registrado pérdidas de hasta USD 2500 y en Mozambique ha habido un ataque que causó una pérdida de USD 50 000. La investigación encontró que en algunos casos los empleados de las empresas de telecomunicaciones no son capaces de distinguir un documento fraudulento, y en otros casos ha habido empleados corruptos, reclutados por los cibercriminales por un pago de USD 10 a USD 40 por SIM activada.

Según Fabio Assolini, analista sénior de Kaspersky Lab, los estafadores solo necesitan un número telefónico para poder iniciar un intento de fraude, por lo cual suelen buscar bases de datos filtradas, comprar bases de datos de vendedores o usar aplicaciones que ofrecen servicios de identificación de llamadas. Este analista señala que el paso más seguro para enfrentar estos fraudes es la eliminación de la autenticación con doble factor basada en SMS de confirmación, y en su lugar se debería preferir por un token físico o por la generación de una OTP en una aplicación móvil, como Google authenticator. No obstante, la aplicación de estas soluciones dependería de las empresas bancarias o de los mismos usuarios.

En cambio, Assollini recomienda que las empresas operadoras deberían implementar un mensaje automático que se envíe al número para comunicarle al propietario de que ha habido una solicitud de cambio de SIM card, si no es autorizado, el usuario debe ponerse en contacto con la empresa operadora.

Por otro lado, se debe señalar que el problema de las reposiciones fraudulentas del SIM card también ha sido objeto de análisis en el 7° SOUPS (*Symposium on Usable Privacy and Security*) - 2020, evento auspiciado por la ACM (*Association for Computing Machinery*) y la USENIX (*The Advanced Computing System Association*). Específicamente, Lee, K et al. (2020) presentaron un estudio empírico sobre las falencias en los procesos de autenticación, implementados por las empresas operadoras de telecomunicaciones de EEUU. Este estudio consistió en crear 10 identidades ficticias, y probar la seguridad de los sistemas de autenticación de las empresas. A partir de los resultados, estos investigadores recomiendan adoptar las siguientes acciones:

- Las empresas operadoras debería suspender los métodos inseguros de validación. Se refieren específicamente a las preguntas reto, dado que los estafadores podrían realizar ingeniería social. Además, el uso de este tipo de preguntas encierra el riesgo de que los asesores accedan a la información personal de los abonados.
- Se recomienda métodos de autenticación telefónica apoyado con la *website* o la *app login*, o usar contraseñas de un solo uso (*one-time password*) vía la llamada.
- Brindar opciones de seguridad adicional para los usuarios.
- Las empresas operadoras deben reportar y comunicar los intentos de autenticación a los usuarios. Además, se tendría que limitar la cantidad de intentos repetidos de reposición.

[12] La clonación de tarjetas SIM aumenta en la región robando hasta US$2.500 por víctima | Kaspersky

- Se podría retrasar la activación de la *SIM card* por 24 horas, en ese tiempo se tendría que enviar notificaciones a otros números de contacto.
- Restringir el acceso a la información personal de los abonados a los asesores de las empresas, dado que pueden existir filtraciones.
- Entrenar mejor a los asesores para poder detectar fraudes

c) Regulación del registro de *SIM card*

Como se ha indicado previamente, en la actualidad existen diversos riesgos y amenazas vinculados con la contratación del servicio público móvil, activación y reposición de la *SIM card*. Por ello, la mayoría de los países han implementado la regulación del registro de la *SIM card*, con la finalidad de disuadir el robo de celulares, la clonación de las *SIM card* y la ejecución de fraudes mediante contrataciones no solicitadas.

En efecto, la regulación del registro de la *SIM card* tiene por finalidad obligar que las empresas operadoras comercialicen las líneas mediante la previa identificación de los compradores. Cabe señalar que el objetivo de identificar a las personas que han adquirido una línea móvil o están solicitando la reposición es evitar que personas inescrupulosas adquieran una *SIM card* y lo usen para cometer actos ilícitos.

Al respecto, la GSMA (2019b) ha reportado que el registro de la *SIM card* es obligatorio en 150 países a diciembre del 2018. A nivel del continente americano, no sería obligatorio en EEUU, Canadá, México, Colombia, Nicaragua, Costa Rica, Chile y Paraguay; sin embargo, estos dos últimos países estarían evaluando su implementación. Entre los países latinoamericanos que han establecido la obligatoriedad, solo Perú ha incluido la verificación biométrica. Otros países con verificación biométrica son Nigeria, Uganda, Siria, Arabia Saudita, Bosnia, Pakistán, Bangladesh, Birmania y Nueva Guinea.

Asimismo, la GSMA (2019b) también ha identificado que existen tres modelos de implementación: (i) captura de la información personal y conservación por parte de la empresa operadora, (ii) captura de la información personal y se comparte con el regulador, y (iii) captura de la información personal y validación con alguna base de datos del gobierno. El primero modelo ha sido implementado por el 85% de los países, el segundo y tercer modelo lo tienen el 4% y 11% de países, respectivamente. A nivel del continente americano, Ecuador y Perú han implementado el tercer modelo, mientras que el resto se encuentra en el primer modelo.

Por otra parte, se debe señalar que reglas establecidas para el registro de una *SIM card* varía en cada país, pero las más comunes son: registro de los comercializadores autorizados, definición de los lugares apropiados para el registro, tipos de documentos que se requieren para la identificación, número de máximo de líneas que se pueden adquirir, etc.

En el caso de los lugares autorizados para el registro de la *SIM card*, algunos países lo han restringido a las oficinas comerciales de las empresas operadoras, otros permiten que se realice en puntos de venta, con agentes acreditados, revendedores o kioskos. En el cuadro N° 1, se puede apreciar la cantidad de países por tipo de lugar de venta autorizado para la comercialización de la *SIM card*.

Cuadro N° 1
EXPERIENCIA INTERNACIONAL EN EL REGISTRO DE SIM CARD

Región	**Requiere el registro del *SIM card* para la contratación**	**Dónde se registra la *SIM card* para la contratación**
África	Sí en 44 de 45 países No en Lesoto	45 países en punto de venta o en tiendas de la marca 1 país en tienda o revendedores de telecomunicaciones (Costa de Marfil)
América	31 de 37 países No en Canadá, Trinidad y Tobago, México, Nicaragua, Panamá y Estados Unidos	29 países en punto de venta o tienda de la marca 1 país en distribuidor autorizado 1 país en línea (Chile)
Asia Pacífico	36 de 41 países No en Georgia, Tonga, Kiribati, Laos y Nueva Zelanda	35 países en tienda o punto de venta 1 país en oficina de los proveedores (Irán)
Europa	23 de 45 países No en 22 países	20 países en tienda o punto de venta 1 país en línea (Eslovaquia) 1 país por oficinas de correo (Ucrania)
Oriente Medio	7 de 8 países No en Israel	7 países en tienda o punto de venta

Elaboración: OSIPTEL.

En relación con la venta de la *SIM card* en la vía pública, se debe señalar que es un fenómeno de países africanos con altos niveles de informalidad, tal como Nigeria y Uganda. En el caso de Nigeria, la venta de la *SIM card* se encuentra prohibida por la NCC (*Nigerian Communications Commission*)[13]; no obstante, la población suele estar habituada a comprar los chips en autos y carretillas, a personas, a pesar de que están mal registradas o registradas a nombre de un tercero. En el caso de Uganda, la UCC (*Uganda Communications Commission*) también ha ordenado a todos los proveedores de servicios de telecomunicaciones y sus agentes que dejen de vender o vender tarjetas SIM en las calles[14]. La UCC está solicitando el apoyo de la policía para el arresto de los vendedores ambulantes de la *SIM card*.

Por lo tanto, se puede apreciar que a nivel internacional existe una preocupación respecto a los diversos riesgos y amenazas a los que están expuestos los usuarios en

[13] https://dailytrust.com/danger-as-recycled-sim-cards-flood-streets-markets
[14] https://ugandaradionetwork.net/story/regulations-on-sim-card-vending-in-the-offing

el momento de la contratación de una línea móvil, activación o reposición de una *SIM card*. Esta situación ha impulsado que en muchos países se implementen regulaciones para el registro de las *SIM card*, donde se definen protocolos de seguridad que garanticen la identificación de las personas que adquieren una línea móvil. Todas estas regulaciones están orientadas a brindar una mayor seguridad a los usuarios de los servicios públicos y así evitar que sean víctimas de los delincuentes, particularmente los estafadores.

Por otra parte, a nivel de iniciativas regulatorias, se debe destacar que la ACMA[15], regulador de telecomunicaciones en Australia, recientemente ha actualizado las normas para la verificación de identidad en la portabilidad[16] en atención al problema de los fraudes por reposición de la *SIM card* y ha adoptado las siguientes decisiones:

- Antes de realizar la portación, se debe verificar que el solicitante está haciendo uso efectivo del terminal móvil. Se puede realizar una llamada o enviar un código de identificación. En el caso del apoderado de una persona jurídica se debe verificar si tiene acceso directo al número primario asociado.
- Usar un código único de identificación.
- Usar uno o más de formas de información biométrica.
- En caso no sea posible la verificación se podrá presentar 2 documentos de categoría o 1 documento de categoría A y 2 documentos de categoría B. Los documentos de categoría A son: Licencia de conducir, pasaporte, certificado de nacimiento, carné militar, certificado de ciudadanía, DNI, licencia para portar armas, etc. Los documentos de categoría B son: recibo de servicio móvil, carné de estudiante, registro vehicular, etc.
- Los documentos emitidos por el gobierno deben ser autenticados a través de los servicios de verificación del gobierno.

Asimismo, en Italia, la AGCOM[17], regulador del sector de telecomunicaciones en este país, ha aprobado la Delibera N° 96/21/CIR, mediante la cual define algunas salvaguardas para hacer frente a este tipo de fraude:

- El cambio de la *SIM card* solo lo puede solicitar el titular. En caso de robo solo puede ser pedido al operador, y la portabilidad solo se ejecuta luego de tener la *SIM card* activa.
- Para la identificación del solicitante se debe presentar una copia del DNI, de la *SIM card* vieja, y en caso de robo, la denuncia policial.
- Se debe verificar inmediatamente que la línea esté activa mediante un SMS. En caso de robo o pérdida, el procedimiento puede proseguir.

Finalmente, también se debe mencionar que en EEUU se vienen realizando estudios para establecer reglas que aborden el problema de la reposición fraudulenta de la *SIM*

[15] *Australian Communications and Media Authoriy*.
[16] Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standar 2020.
[17] Autorità per le Garanzie nelle Comunicazioni.

card. Específicamente, la FCC[18] de EEUU ha publicado su proyecto normativo, en el cual proponen las siguientes medidas[19]:

- Prohibir efectuar el *SIM Swap* si las empresas no tienen métodos de autenticación seguros. Ejemplos de autenticación segura son las contraseñas de un solo uso enviados en un SMS; e mail o a través de una llamada.
- Establecer procedimientos en caso de intentos fallidos y notificar a los usuarios.
- Introducir requerimiento de entrenamiento y transparencia para el personal de atención al cliente.
- El SIM Swap debería retrasar por 24 horas en caso haya múltiples intentos fallidos de autenticación. En ese período se debe notificar al usuario con SMS y email.
- En caso de fraude, las empresas operadoras están obligadas a colaborar con las víctimas en la obtención de la información y en la recuperación de la línea.
- Cuando se solicita el *SIM Swap* se debe notificar a los usuarios de manera inmediata.
- Requerir la información sobre todos los fraudes en *SIM Swap* y de los reclamos presentados.

En el caso de Canadá, la CRTC[20], el regulador del sector de telecomunicaciones, ha rechazado publicar un proyecto normativo que aborde este problema[21], pero ha señalado que viene trabajando con las empresas operadoras para reducir la incidencia de estos fraudes, aunque no ha querido indicar qué acciones en concreto están realizando, debido a que desean evitar que los estafadores se enteren.

A causa de esta decisión, en este país se ha desatado una controversia, dado que existe una presión ciudadana para que el regulador adopte medidas para frenar la incidencia de estos tipos de fraudes. Señalan que los riesgos son altos para los ciudadanos, y peligro constante; por ejemplo, en Ontario una enfermera fue víctima de este fraude y perdió cerca de $ 10 000 dólares canadienses[22].

En este contexto, la *Public Interest Advocacy Centre* (PIAC), una organización sin fines de lucro que defiende los derechos de los consumidores, ha exigido que las empresas operadoras y la CRTC hagan públicas las acciones que vienen realizando, y dejen de tratar este problema de manera secreta o reservada.

Incluso, algunos usuarios canadienses, considerando que la CRTC ha fallado en regular las empresas del servicio público móvil y proveer consecuencias cuando ellas fallan proteger al usuario de estos fraudes en la reposición de la *SIM card*, ha presentado un petitorio al primer ministro de Canadá para que encargue a la CRTC iniciar una regulación[23].

Al respecto, resulta interesante indicar que, según este petitorio, la actual regulación no presiona a las empresas operadoras para atender este problema, no hay transparencia

[18] *Federal Communications Commission*
[19] *Notice of Proposed Rulemaking: Rules to Prevent SIM Swapping and Port-Out Fraud*
[20] *Canadian Radio-television and Telecommunications Commission.*
[21] Lamont, J. (2020). CRTC, carriers refuse to share data about SIM hijacking and preventions efforts.
[22] https://toronto.ctvnews.ca/nurse-scammed-out-of-nearly-10-000-after-falling-victim-to-new-sim-swap-scheme-1.4690702
[23] https://action.openmedia.org/page/72976/action/1?locale=en-US

respecto a las acciones que se vienen adoptando, no hay manera de medir si estas acciones son efectivas, y no hay consecuencias o responsabilidades para las empresas operadoras por haber fallado en implementar soluciones adecuadas.

Asimismo, los ciudadanos canadienses exigen que las empresas operadoras garanticen que no se activen o porten líneas móviles sin su consentimiento, y que para ello se debería requerir la confirmación mediante un SMS al teléfono original, entre otras medidas que aseguren la seguridad de los usuarios. Si no se realizan cambios normativos, las empresas operadoras seguirán asumiendo la menor responsabilidad, y trasladando el problema a los usuarios.

En el caso del Reino Unido, el regulador OFCOM[24] ha manifestado que no tiene programado realizar una consulta sobre medidas regulatorias aplicables a los fraudes en la reposición de la *SIM card*. No obstante, la problemática en este país es bastante preocupante, dado que entre el 2019 y 2015, este tipo de fraude se han incrementado en 508%[25], como se puede apreciar en el cuadro N° 1. Cabe señalar que, en el 2019, la pérdida generada por este tipo de fraude en este país ascendió a cerca de S/ 14.7 millones, con una pérdida promedio por víctima de S/ 16 646.

Cuadro N° 2
REINO UNIDO: REPOSICIÓN FRAUDULENTA DE SIM CARD EN NÚMEROS

Año	Casos	Pérdida Total (S/)	Pérdida promedio (S/)
2015	144	2 382 627	16 546
2016	161	4 441 807	27 589
2017	359	15 596 765	43 445
2018	3111	15 930 185	5 121
2019	875	14 565 185	16 646
2020	483(b)	4 584 651	9 492

Nota:
(a) La pérdida total se encuentra reportada originalmente en libras esterlinas, se ha aplicado un tipo de cambio de S/ 5.46.
(b) A junio 2020
Fuente: *Action Fraud*.

Cabe señalar que, en el Reino Unido, las empresas operadoras suelen exigir el pasaporte y la licencia de conducir para efectuar la reposición de la *SIM card* de manera presencial. Una investigación realizada sobre esta modalidad de verificación de identidad ha demostrado que varios asesores de las empresas operadoras suelen ser negligentes con la exigencia de estos requisitos[26].

Asimismo, en el caso del canal telefónico, se sabe que es el principal canal donde se ejecutan los fraudes, a pesar de que las empresas operadoras del Reino Unido suelen remitir SMS de notificación a la línea del solicitante, y en caso el celular se encuentre malogrado o perdido, el solicitante debe realizar el trámite de manera presencial y

[24] Office of Communications.
[25] Información reportada en https://www.theguardian.com/money/2020/sep/13/sim-swap-is-on-the-rise-how-can-you-stop-it-happening-to-you
[26] https://www.which.co.uk/news/2020/04/sim-swap-fraud-how-criminals-hijack-your-number-to-get-into-your-bank-accounts/

presentando una foto. Esto se debe a que los estafadores suelen realizar miles de intentos hasta encontrar a un asesor negligente que no cumpla con los protocolos de seguridad. Esto demuestra que la perseverancia resulta rentable para los estafadores.

Por lo tanto, se puede apreciar que el fraude en la reposición de las *SIM card* es fenómeno global y es resultado de la misma dinámica del ecosistema móvil, por lo que las empresas operadoras tienen la responsabilidad de mejorar sus sistemas de autenticación y verificación de identidad. No se trata de un problema de los bancos, sino de un problema que afecta la confiabilidad y seguridad de las redes de telecomunicaciones, por lo que existen razones para que los reguladores tomen acciones orientadas a incentivar a las empresas operadoras a mejorar sus protocolos de seguridad.

Asimismo, se debe reflexionar en torno a que el uso del internet móvil para la realización de transacciones financieras forma parte de los principales atributos que valoran los usuarios al contratar un servicio público móvil, y por ello, cualquier fraude que ocurra debido a que las empresas operadoras tienen sistemas de autenticación o identificación vulnerables afecta la confiabilidad en el uso del servicio, pone en riesgo el buen desempeño de este mercado y daña la imagen de las empresas operadoras.

En línea con este enfoque, la misma GSMA, que es la principal asociación de operadores de redes móviles y organizaciones o industrias relacionadas con el ecosistema móvil, también ha analizado el problema de la reposición fraudulenta de la *SIM card* (*SIM Swap*), y ha formulado las siguientes recomendaciones[27]:

- En los casos en los que el fraude del *SIM card* sea alto, la reposición se debería realizar solo en la oficina de la empresa. En los lugares donde ello no sea posible, este trámite se debería realizar con distribuidores autorizados. En estos casos los servicios financieros tendrían que estar restringidos por 48 horas.
- Se debería requerir la presentación de los documentos de identificación, los cuales tendrían que autenticarse antes de la reposición de la *SIM card*. En los lugares donde ello no sea posible se debería tomar una fotografía.
- Operadores móviles y proveedores de servicios financieros deberían desarrollar mecanismos proactivos de compartición de información. Se podría compartir la identidad y el *SIM card* de los usuarios que han solicitado la reposición de la *SIM card*.
- Desarrollar una lista de perpetradores.

Por otra parte, la GSMA (2019a) también ha formulado recomendaciones a los usuarios para poder evitar ser víctimas de este tipo de fraudes. Específicamente, esta entidad propone lo siguiente:

- Incrementar el nivel de educación de los consumidores respecto a la importancia de tener la práctica rutinaria de proteger sus datos personales (nombre, fecha de nacimiento, dirección, PIN, etc.).
- Informar a los consumidores respecto a cómo actuar en situaciones en la información personal se encuentra comprometida.

[27] GSMA (2019a).

- Desarrollar estrategias proactivas de educación a los usuarios en las últimas técnicas que están siendo utilizadas por los estafadores para robar su información personal.

Por otra parte, la UIT[28] y *Financial Inclusion Global Iniciative* (2019)[29] elaboraron un informe técnico en el que se abordan las vulnerabilidades que afectan a las transacciones financieras digitales. En este informe se señala que la principal razón por la que no se mitigan estas vulnerabilidades es el desalineamiento de intereses y la descolocación de las responsabilidades entre el regulador del sector telecomunicaciones y el regulador del sector financiero. Cabe señalar que la UIT y GSMA ha publicada muchas guías y recomendaciones para los operadores de telecomunicaciones sobre como mitigar estas vulnerabilidades; sin embargo, la tasa de implementación de estas recomendaciones es extremadamente baja.

Este informe señala que menos del 30% de las empresas de telecomunicaciones en la Unión Europea y menos del 0.5% en los países en vías de desarrollo ha implementado estas estrategias de mitigación. Asimismo, enfatiza la falta de conciencia de estas vulnerabilidades y de los costos prohibitivos hacen que las empresas operadoras no implementen medidas de mitigación. En efecto, las empresas de telecomunicaciones no se conciben responsables de estos problemas, y por ello, no tienen incentivos para mitigar las vulnerabilidades de los procesos de contratación. Al respecto, la UIT y la FIGI plantean las siguientes recomendaciones generales:

- Educar a los reguladores del sector telecomunicaciones y financiero de las vulnerabilidades que plagan a todo el ecosistema de los sistemas financieros digitales que operan sobre las redes de telecomunicaciones.
- Los reguladores del sector telecomunicaciones y financiero deberían implementar una regulación que otorgue la responsabilidad a quien corresponda y obligue a las empresas de telecomunicaciones a implementar las medidas de mitigación.
- Los reguladores del sector telecomunicaciones y financiero deberían asegurar un esquema legal que permita reportar incidentes y adoptar requisitos mínimos de seguridad.
- Reguladores de telecomunicaciones deben incentivar el establecimiento de medidas de seguridad base para cada categoría (3G, 4G, 5G) que sea implementado por las empresas de telecomunicaciones con el objetivo de asegurar un entorno de interconexión más seguro.
- Crear diálogo entre los proveedores de servicios digitales financieros y los reguladores de telecomunicaciones con la industria de seguridad en telecomunicaciones, a fin de que se les pueda exponer la existencia de soluciones de mitigación disponibles en el mercado y crear incentivos para que la industria desarrolle nuevas soluciones.
- Incentivar a las empresas de telecomunicaciones, a los proveedores de servicios digitales financieros y a la industria para trabajar juntos e implementar soluciones.

[28] Unión Internacional de Telecomunicaciones, que es el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), encargado de regular las telecomunicaciones a nivel internacional, entre las distintas administraciones y empresas operadoras.
[29] FIGI es la Financial Inclusion Global Iniciative.

Asimismo, el referido reporte técnico de la UIT y la FIGI propone que los reguladores del sector telecomunicaciones adopten las siguientes medidas regulatorias para enfrentar el problema de los fraudes por *SIM swapping*:

- Estandarización de las reglas de reposición de la *SIM card* entre los operadores de redes móviles y los operadores móviles virtuales, incluyendo cuando la reposición forma parte de un proceso de portabilidad.
- Cuando la reposición se solicita mediante un apoderado o representante, se debería requerir una carta poder del abonado y una fotografía del pasaporte del abonado.
- Cuando la reposición es con un apoderado o representante, los asesores de las empresas deben capturar la imagen del apoderado, la cual se debe conservarse durante 12 meses.
- La reposición solo debería darse si la *SIM card* está defectuosa, dañada, fue robada, perdida u obsoleta, o cualquier otra razón legítima o condición necesaria.

Complementariamente, la UIT y la FIGI también recomiendan que las empresas operadoras adopten las siguientes reglas internas:

- Ante una solicitud de reposición, se deberían enviar notificaciones vía SMS, IVR o *Push USSD* a la *SIM card* o teléfono del abonado, a fin de verificar si realmente la línea está defectuosa, dañada o perdida, o si se encuentra en posesión de una persona distinta al solicitante.
- Luego de enviar las notificaciones, se debería esperar entre 2 y 4 horas antes de activar la nueva *SIM card.*
- Se recomienda que en el proceso de validación o autenticación de una solicitud de reposición se incluyan preguntas “reto”, tal como preguntar acerca de la última recarga o el último número al que se llamó, con la finalidad de que el asesor pueda detectar cualquier comportamiento sospechoso.
- Proveer a los bancos la posibilidad de verificar si el número del usuario ha tenido una solicitud de reposición reciente.

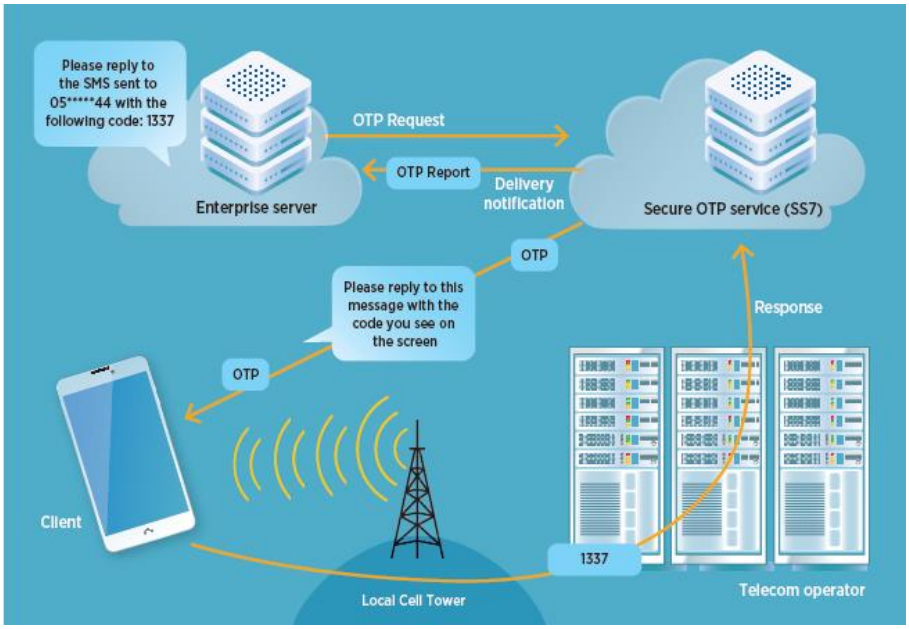
Cabe señalar que la UIT y la FIGI también proponen recomendaciones a las mismas empresas de servicios digitales financieros. Específicamente, se propone que estas empresas desarrollen en enfoque distinto al SMS OTP[30], y adopten, en cambio, una autenticación bidireccional que consiste en recibir la OTP del usuario, no enviarlo. Esto requiere remitir el código OTP en un recurso de visualización (por ejemplo, página web) y enviar un SMS al usuario para que replique el código que observa en el recurso de visualización. Este flujo permite que el proveedor del servicio digital financiero pueda verificar, a partir de su conexión en la red móvil, si el SMS ha sido originado por el legítimo usuario o por un atacante.

Al respecto, es importante enfatizar que estas recomendaciones han sido formuladas por la Unión Internacional de Telecomunicaciones (ITU), que es la agencia especializada de las ONU en el área de las telecomunicaciones, la información y las tecnologías de información y, por tanto, revela la preocupación internacional sobre la ocurrencia de este tipo de fraudes, y que, por ello, no se pueden asumir de manera simplista como un problema de los bancos. Esto se puede realizar a través de la revisión

[30] OTP es One Time Password

de una meta data SCCP[31] a partir del SMS replicado y verificar el Global Title (GT), e identificar si el SMS ha sido enviado desde la ubicación del usuario legítimo y de su red local. En la siguiente ilustración se describe el proceso:

Figura N° 3
DETECCIÓN Y MITIGACIÓN DE LA INTERCEPTACIÓN DEL SMS



Fuente: UIT-FIGI (2019)

5.2. Regulación del registro de abonados en el Perú

Las intervenciones del OSIPTEL para mitigar un mal registro de abonados han sido constantes, iniciando con los apagones de servicios para usuarios que contaban con más de 10 líneas prepago sin reconocer, estos servicios fueron suspendidos hasta determinada fecha; luego de dicha fecha, se anularon definitivamente las líneas que se mantengan sin reconocimiento.

La regulación del registro de abonados en el Perú ha sufrido de varias mejoras en los últimos años, los primeros cambios se presentaron mediante la Resolución N° 056-2015-CD-OSIPTEL, mediante la cual se impuso por primera vez la obligación de utilizar verificación biométrica, al menos en contrataciones prepago. Asimismo, se impuso la obligatoriedad de realizar un registro de distribuidores autorizados, así como el envío de mensajes de texto a todos los números registrados por el usuario para informar sobre la nueva contratación del servicio.

Cabe señalar que, mediante Resolución N° 96-2018-CD-OSIPTEL, se amplió la obligatoriedad a servicios públicos móviles postpago y control.

Asimismo, mediante la Resolución N° 006-2020-CD/OSIPTEL se han realizado modificaciones adicionales con la finalidad de conseguir una buena identificación del usuario que solicita un trámite, la confirmación del código proporcionado mediante un mensaje de texto (SMS) previo a efectuar la portabilidad, entre otros. En el cuadro N° 3 se podrá observar un resumen de los principales cambios realizados por las resoluciones citadas en el párrafo anterior.

[31] SCCP es Signalling Connection Control Part

Cuadro N° 3
CAMBIOS NORMATIVOS RELACIONADOS A LA VERIFICACIÓN DE LA IDENTIDAD EN LA CONTRATACIÓN DE LÍNEAS MÓVILES Y OTROS TRÁMITES

Obligaciones	056-2015-CD-OSIPTEL	96-2018-CD-OSIPTEL	N° 006-2020-CD/OSIPTEL
Verificación biométrica	Se implementa el uso de los sistemas de verificación biométrica solo para abonados prepago	Se adiciona el uso de los sistemas de verificación biométrica para todo el servicio público móvil, es factible utilizarlo en otros servicios. No es necesario la exhibición del DNI	
Registro de abonados	Se añade el registro de la fecha de instalación y/o activación del servicio. En ningún caso, la empresa operadora trasladará al abonado la responsabilidad de registrar la información de sus datos personales.	Se registra la nacionalidad de los abonados	-
Registro de distribuidores	Se implementa la obligatoriedad de realizar un registro de distribuidores autorizados	-	-
Cuestionamientos de titularidad	Se describe el procedimiento para cuestionamientos de titularidad	-	-
Confirmaciones adicionales	-	-	La portabilidad o cambio de titularidad requiere del envío de un código por SMS.
Información a los usuarios	Cuando se contrata un nuevo servicio, se obliga a remitir un SMS	Procedimiento para usuarios que no pueden usar la huella	
Renteseg	-	Se precisa la información que contendrá el Registro de Terminales Móviles	Ante portabilidades sin consentimiento, se registrará el código IMEI en la Lista Negra del RENTESEG.

Fuente: Resoluciones N° 056-2015-CD-OSIPTEL, 96-2018-CD-OSIPTEL y N° 006-2020-CD/OSIPTEL.

6. DEFINICIÓN DEL PROBLEMA

6.1. Planteamiento del problema

Durante el primer semestre del 2021, se han realizado 13.3 millones de contrataciones (altas y portabilidad) en el servicio público móvil. En este mismo período, se registraron 23 007 reclamos por contrataciones no solicitadas, de las cuales 8765 resultaron fundados[32]. Esto implica que ha habido 6.6 reclamos fundados en contrataciones no solicitadas por cada 10 000 contrataciones; no obstante, se debe señalar que la dimensión del problema de contratación no solicitada es mucho mayor, si se considera que los usuarios tienen una alta tasa de no reclamo.

En efecto, según el INEI, el 34.2% de las víctimas de hechos delictivos no denuncia porque considera que sería una pérdida de tiempo; y según el Estudio de Satisfacción de los usuarios en los servicios públicos de telecomunicaciones, solo el 27% de los usuarios que experimentaron inconvenientes presentan su reclamo. Esto implica que, en realidad, la probabilidad de ocurrencia de una contratación no solicitada podría ser mucho mayor.

Por otra parte, en el primer semestre del 2021, Telefónica del Perú S.A.A. (en adelante, Telefónica) es la que tiene la mayor tasa de resoluciones fundadas en contrataciones no solicitadas, 15.2 casos por cada 10,000 contrataciones, le siguen Entel Perú S.A. (en adelante, Entel), América Móvil Perú S.A.C. (en adelante, América Móvil), y Viettel Perú S.A.C. (en adelante, Viettel) con 6.3, 3.7 y 0.3 resoluciones fundadas por cada 10000 contrataciones, respectivamente. Cabe señalar que en Entel el 56.1% de los reclamos por contrataciones no solicitadas resultaron fundados[33], el 37.9% en Telefónica, el 26.5% en Viettel y el 26.1% en América Móvil.

Si bien, la cantidad de reclamos por contratación no solicitada, observada en el primer semestre del 2021, ha disminuido en 6,6% respecto al primer semestre del 2020; se debe señalar que los casos que se vienen observando, en este año, revelan que las empresas operadoras todavía siguen teniendo prácticas comerciales no seguras para los usuarios, en lo que se refiere a la contratación de servicios, lo cual resulta bastante preocupante para el OSIPTEL.

Al respecto, se debe mencionar que estas contrataciones no solicitadas podrían ser resultado de fallas administrativas por parte del personal asignado por las empresas operadoras para atender estas solicitudes; pero también se deben a un enfoque mercantilista que prioriza las ventas y no le da la debida importancia a la seguridad de los usuarios.

En efecto, a partir de la revisión de los casos, se han encontrado que algunos usuarios refieren que varios asesores o vendedores de las empresas operadoras los han abordado fuera de las oficinas comerciales, en la vía pública, y que, aprovechando el contexto, les han inducido a realizar portaciones y contrataciones no solicitadas. Existen casos en los que, de manera engañosa, han ofrecido una *SIM card* de regalo con la finalidad de realizar la verificación biométrica y concretar una contratación.

Incluso, en muchos casos, los usuarios no son conscientes de haber contratado una línea móvil, y recién llegan a enterarse de ello cuando las empresas operadoras les remiten notificaciones de deudas por líneas que no usan. La mayoría de los usuarios que han sufrido esta estafa, refieren que sospechosamente el vendedor ambulante de

[32] No se incluyen los reclamos fundados por razones comerciales, ni los parcialmente fundados.
[33] No se consideran los reclamos fundados por razones comerciales, ni los parcialmente fundados.

la empresa operadora le hizo pasar la verificación biométrica, aduciendo que el sistema no leía su huella dactilar.

Por otra parte, el OSIPTEL recibe constantemente las denuncias de usuarios que refieren tener la titularidad de líneas que no han contratado y que, respecto a ello, la empresa operadora habría actuado con cierto grado de indiferencia. Específicamente, en el primer semestre del 2021, se han recibido 1121 casos, de los cuales 58.2% corresponden a altas sin portabilidad, 25.4% a portabilidad y 16.4% migración de plan. Cabe señalar que, si se incluyen los cambios de titularidad no autorizados, la cantidad de casos se incrementa a 1220 casos.

Cabe señalar que la gravedad de los casos identificados no se limita a la existencia de líneas contratadas a nombre de usuarios que no las solicitaron, sino que también abarca al uso que se hace de esas líneas. En efecto, se ha verificado que esas líneas, a veces, han sido vendidas a terceros, los cuales desconocen que la titularidad la tiene otra persona; también se ha encontrado que esos terceros, al hacer uso de la línea les generan deudas a las víctimas. En el peor de los casos, los terceros que usan estas líneas podrían ser delincuentes, y cometer delitos en los que el usuario podría verse involucrado como cómplice (secuestros, extorsiones, etc.).

De manera colateral a los problemas en la contratación no solicitada, también se han identificado casos en los que se han vulnerado los procedimientos de reposición de la *SIM card*. Específicamente, entre enero y agosto del 2021, se han reportado al OSIPTEL 394 usuarios que han denunciado que las empresas operadoras cometieron el error de aprobar la solicitud de reposición de la *SIM card* presentada por terceros. Este error les generó a 23 usuarios una perdida promedio de S/ 10 065, a parte que hay 120 casos en los que los estafadores se enfocaron a robar el bono que está entregando el gobierno para atender la situación de extrema pobreza generado por la pandemia del Covid 19. Asimismo, la empresa Viettel reportó 40 casos adicionales, en los que la pérdida promedio fue de S/ 7113.

En este contexto, resulta importante señalar que los robos que se han producido a través de la reposición fraudulenta de la SIM card tienen un impacto muy grande en la economía familiar, dado que usualmente los delincuentes logran apoderarse del ingreso mensual del hogar y, en algunos casos, de los ahorros familiares.

Sin embargo, es necesario evitar concebir este problema como un asunto meramente relacionado con la seguridad ciudadana o los problemas de seguridad en las transacciones financieras. Ello debido a que, todos los casos, que se describirán en las siguientes secciones, tienen como factor común una falla en los procesos de contratación de líneas de telefonía móvil, reposiciones de la SIM card que no cumplen con los protocolos de seguridad, etc. Es decir, en gran medida, estos casos de fraudes podrían evitarse si se implementan medidas de seguridad adicionales, o si por lo menos las empresas operadoras cesan de comercializar sus servicios en la vía pública.

En efecto, es necesario considerar que, en la actualidad, un terminal móvil y la línea permiten a los usuarios realizar no solo llamadas, enviar SMS o correos electrónicos; sino también realizar transacciones bancarias, compras on line, etc; servicios que se prestan a través de aplicativos. Todo este desarrollo tecnológico ha incrementado el valor del servicio público móvil, y por ello es importante que se brinde el servicio con mayores medidas de seguridad. Por ello, no resulta aceptable asumir que la responsabilidad de las empresas operadoras no se extienda también a garantizar que ningún individuo ajeno se apodere de la línea del usuario, o que se usen esas líneas con fines delictivos. En ese sentido, es parte de la responsabilidad de las empresas y

del regulador procurar que los procesos de autenticación y verificación de identidad en la contratación de líneas nuevas, reposición de SIM card o cambio de titularidad se realicen en un entorno seguro y confiable.

Asimismo, estas nuevas amenazas se han venido dando debido a que los estafadores han innovado y han encontrado brechas de seguridad en los protocolos de contratación y reposición de líneas móviles. Particularmente, se han tenido los siguientes hallazgos:

- Se han registrado casos de falsos representantes o apoderados que han realizado trámites a nombre de otros usuarios. Estos estafadores se han aprovechado de que, en las normas vigentes, no se indica explícitamente que la empresa operadora deba hacer la verificación biométrica del representante o aplicar otras medidas de seguridad. Es decir, la ocurrencia de estos casos también refleja la poca proactividad por parte de las empresas operadoras para evitar la vulneración de sus procesos de contratación y reposición.
- También se ha encontrado que los estafadores estarían vulnerando el proceso de verificación biométrica mediante la clonación de la huella dactilar. Esta nueva modalidad de ataque resulta preocupante, porque se esperaba que la verificación biométrica sea el método de autenticación más seguro; sin embargo, los hechos indican que se necesitaría de mayores medidas de seguridad.

Otro aspecto a considerar es que los cambios tecnológicos y el aislamiento social obligatorio, decretado por el gobierno para enfrentar a la Covid 19, ha impulsado el uso de herramientas *on line* para la presentación de solicitudes y las compras por *delivery*; por lo que resulta pertinente evaluar que dichas modalidades de contratación se realicen de manera segura.

Por otro lado, las fallas de seguridad en los procesos de contratación de líneas, reposición de SIM card y cambio de titularidad generan problemas que trasciende el ámbito de las telecomunicaciones, por lo que la UIT y la FIGI han formulado diversas recomendaciones a las empresas de telecomunicaciones, empresas de servicios digitales financieros, reguladores del sector y reguladores del sector financiero. En particular, al sector telecomunicaciones se le recomienda desarrollar regulaciones que incentiven a las empresas de telecomunicaciones a implementar medidas de seguridad y asuman su responsabilidad; mientras que se recomienda que las empresas de servicios digitales financieros desarrollen sistemas que puedan identificar la localización de emisor de un SMS de confirmación, a fin de poder identificar si ello coincide con los datos o la información del usuario legítimo.

El OSIPTEL, en línea con las recomendaciones de los organismos internacionales sobre la necesidad de adopción de medidas intersectoriales, para afrontar la problemática de fraudes en la contratación y el SIM swapping, mediante carta C.185-PD/202134 solicitó a la Presidencia del Consejo de Ministros lidere las coordinaciones con las distintas entidades públicas (como el Ministerio del Interior, el Ministerio Público, el RENIEC, la Defensoría del Pueblo, la Superintendencia de Banca, Seguros y AFP, y el Banco de la Nación) y organizaciones representativas del sector privado como ASBANC y AFIN, que se encuentran involucradas con dicha problemática.

En dicha comunicación, se informan los avances realizados por el OSIPTEL respecto Al sector de telecomunicaciones al fiscalizar que la contratación del servicio se lleve a

[34] De fecha 30 de noviembre de 2021.

cabo en ambientes controlados, y las coordinaciones realizadas con el Banco de la Nación y el Ministerio de Desarrollo e Inclusión Social – MIDIS.

Del mismo modo, se presentó unas propuestas de medidas de seguridad que podrían implementar las empresas del sector financiero, según las mejores prácticas y recomendaciones emitidas por organismos internacionales, que buscan combatir el fraude producto del SIM swapping, en el momento de la autenticación de los clientes al usar los servicios financieros.

De otro lado, mediante carta C.186-PD/2021 el OSIPTEL realiza las coordinaciones con el Ministerio del Interior para la adopción de acciones que desincentiven las prácticas delictivas relacionadas al uso de equipos terminales móviles con IMEI adulterado.

6.2. Evidencias

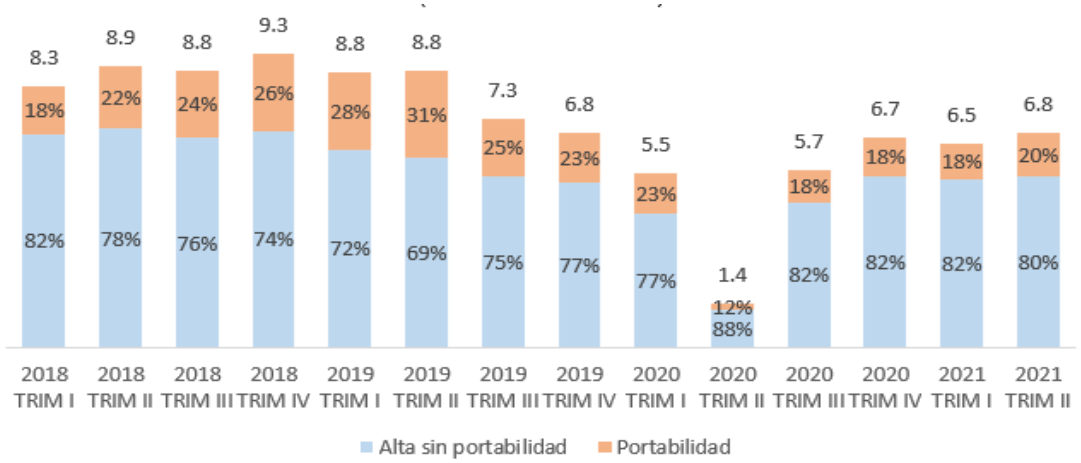
En esta subsección se presentan, con mayor detalle, las evidencias del problema planteado previamente.

a) Contrataciones en el servicio público móvil

En el Perú, el servicio público móvil es operado por seis empresas operadoras, cuatro son operadores móviles de red y dos operadores móviles virtuales (OMV). Los OMR son Telefónica, América Móvil, Entel y Viettel; y las OMV son Flash Servicios Perú S.R.L. (en adelante, Flash) Guinea Mobile S.A.C. (en adelante, Cuy Mobile). Estas empresas operadoras, en conjunto, tienen 41,22 millones de líneas en servicio a junio del 2021, y proveen de conectividad a 38% de los centros poblados del país.

En el gráfico N° 1 se reporta la cantidad trimestral de contrataciones en el servicio público móvil, en el período 2019 - 2021. Se puede apreciar que, en promedio, el 78% de las contrataciones de las empresas operadores es por un alta nueva o un nuevo usuario; mientras que en promedio solo el 22% realiza una portabilidad. En promedio, hay cerca de 7,1 millones de contrataciones, pero sino no se considera al 2020, año típico por la pandemia, el promedio se eleva a 8 millones de contrataciones. En lo que va del 2021, se han registrado 13.3 millones de contrataciones, y se aprecia una recuperación, respecto al 2020.

Gráfico N° 1
CONTRATACIONES EN EL SERVICIO PÚBLICO MÓVIL
(Millones de solicitudes)



Fuente: PUNKU.
Elaboración: OSIPTEL.

b) Solicitudes de reposición de SIM card

De enero a agosto de 2021, América Móvil atendió 887 752 reposiciones de la *SIM card*, Viettel y Entel recibieron 299 856 y 291 346, respectivamente. Entre las 3 empresas se tiene un total de casi 1,5 millones de solicitudes de reposición de SIM card en los 8 primeros meses de este año. Si se tuviera la información de Telefónica, el total debería llegar a casi 2,4 millones, asumiendo que como mínimo debería tener tantas solicitudes como América Móvil.

Como se puede apreciar en el cuadro N° 5, el 41% de las solicitudes de reposición se tramitan a través de un distribuidor autorizado, el 24% en un centro de atención, el 18% mediante autoactivación, 16% en un punto de distribución y 1% en otros canales. En el caso de Entel y Viettel, el principal canal utilizado es el centro de atención (42% y 62%); mientras que, para América Móvil, el principal canal es el distribuidor autorizado (46%).

Cuadro N° 4
CANTIDAD DE SOLICITUDES DE REPOSICIÓN DE SIM CARD, enero – agosto 2021

Canal de atención	Entel		Viettel		América Móvil		Total	
	Cantidad	%	Cantidad	%	Cantidad	%	Cantidad	%
Centro de atención	120 848	42%	185 616	62%	54 711	6%	361 175	24%
Punto de distribución	18 140	6%	2 355	1%	212 797	24%	233 292	16%
Distribuidor autorizado	89 973	31%	107 898	36%	404 697	46%	602 568	41%
Autoactivación	52 287	18%	0	0%	212 787	24%	26 5074	18%
Otros	10 098	3%	3987	1%	2760	0%	16 845	1%
Total	291 346	100%	299 856	100 %	887 752	100 %	1 478 954	100%

Fuente: Información reportada por las empresas operadoras
Elaboración: OSIPTEL.

Sin embargo, es importante señalar que la reposición ambulatoria de *SIM card* es una realidad que este reporte parece ocultar. Esto se debe a que las ventas ambulatorias se realizan de manera informal, a través de distribuidores que supuestamente estaría haciendo sus transacciones en un local de atención presencial, pero que en realidad está ejecutando todas estas solicitudes con vendedores ambulantes y sin la debida seguridad.

Cabe indicar que, en la vía pública los activadores o vendedores, aun cuando sean autorizados por la empresa operadora, no son supervisados por algún trabajador de esta o del distribuidor, a diferencia de lo que ocurre en los puntos de venta o centros de atención. Por ello, en realidad, no se puede tener certeza que todos los trámites (reposición de *SIM card*, cambio de titularidad, contrataciones de líneas, activaciones, etc.) que declaran las empresas operadoras como presenciales hayan sido así, dado que probablemente lo hayan ejecutado vendedores ambulantes sin las debidas medidas de seguridad o requisitos mínimos de trazabilidad.

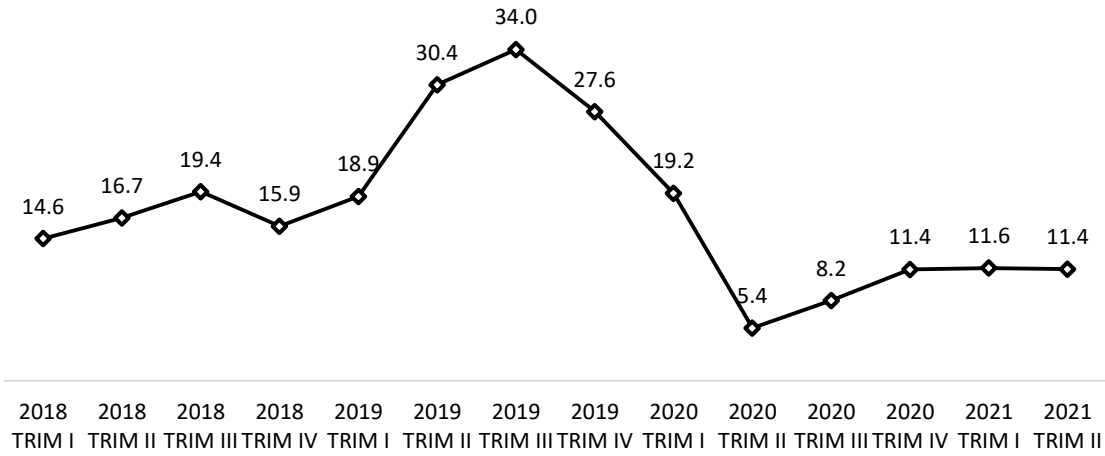
c) Reclamos por contratación no solicitada

Como se ha indicado previamente, en el Perú para solicitar la contratación de un servicio; las empresas operadoras del servicio público móvil y los usuarios tienen la obligación de cumplir con los protocolos de identificación establecido en la norma de Condiciones de Uso. No obstante, a pesar de las medidas de seguridad establecidas, todavía se reportan casos de usuarios que declaran no haber solicitado la contratación o la activación de un servicio, y que presenta un reclamo.

Al respecto, desde el 2018 se resuelve trimestralmente un promedio de 17 483 reclamos relacionados a contratación no solicitada. En el gráfico N° 2, se puede apreciar que la cantidad de reclamos resueltos por contratación no solicitada tenía una tendencia creciente hasta el tercer trimestre del 2019, luego de ese período se aprecia una tendencia decreciente.

Esta nueva tendencia se explica por la exhortación que el OSIPTEL hizo, en noviembre del 2019, a las empresas operadoras para que cesen la venta de la *SIM card*[35] mediante distribuidores no autorizados y fuera de sus locales comerciales (vía pública), debido a que esta modalidad de comercialización expone a los usuarios a riesgos de estafas. Cabe señalar que, en el año 2020 la cantidad de reclamos es atípica debido a la declaración del Estado de Emergencia a nivel nacional por la pandemia del COVID-19.

Gráfico N° 2
RECLAMOS RESUELTOS EN CONTRATACIÓN NO SOLICITADA DEL SERVICIO PÚBLICO MÓVIL 2018-2021
(En miles)



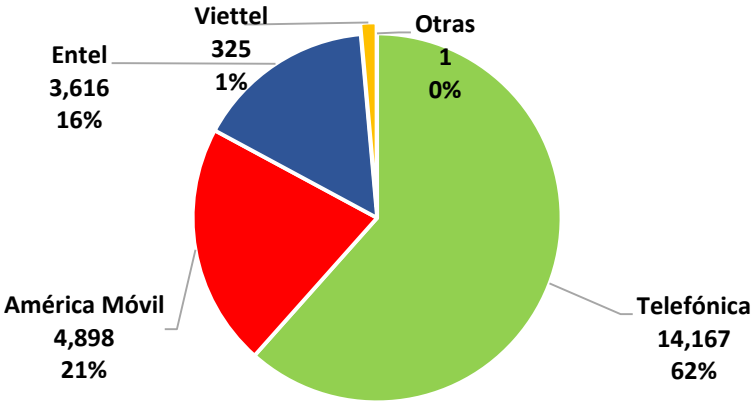
Fuente: PUNKU.
Elaboración: OSIPTEL.

De enero a junio de 2021, la empresa operadora con mayor participación de reclamos relacionados a contratación no solicitada en los servicios móviles fue Telefónica con el 62%, seguido de América Móvil, Entel y Viettel con el 21%, 16% y 1%, respectivamente. Cabe señalar que en el 2019 y 2020, Telefónica tenía el 45% y50% de todos los reclamos por esta materia, por lo se aprecia un incremento en su participación; en

[35] Cartas N° C.00800-GG/2019, C.02384-GSF/2019, C.00195-GSF/2020, C.00501-GSF/2020, C.02430-GSF/2019, C.00353-GSF/2020 y C.01273-GSF/2020

cambio, América Móvil ha reducido su participación en este tipo de reclamo, dado que en el 2019 tenía el 49% y en el 2020 el 38%.

Gráfico N° 3
RECLAMOS RESUELTOS EN CONTRATACIÓN NO SOLICITADA DEL SERVICIO PÚBLICO MÓVIL POR EMPRESA OPERADORA, I SEMESTRE 2021



Fuente: PUNKU.
Elaboración: OSIPTEL.

Cabe señalar que en el período de enero a junio de 2021, del total de reclamos en servicios móviles, el 53,3% son resueltos como infundados, el 38,1% como fundados, el 5,8% como improcedentes y 2,8% tiene otro tipo de solución[36]. La empresa operadora con mayor tasa de reclamos fundados (es decir, en los que el usuario tiene la razón) es Entel, con el 56,1%, seguido de Telefónica, Viettel y América Móvil con el 37,9%, 26,5% y 26,1%, respectivamente. Asimismo, en cuadro N° 5 se puede apreciar la tasa de reclamos fundados cada 10 mil contrataciones, donde se observa que Telefónica tiene el mayor nivel de incidencia (15.2), seguido por Entel (6.3).

Cuadro N° 5
RECLAMOS RESUELTOS EN CONTRATACIÓN NO SOLICITADA DEL SERVICIO PÚBLICO MÓVIL POR SENTIDO, I SEMESTRE 2021

	Telefónica		América Móvil		Entel		Viettel		Total	
	Cant.	%	Cant.	%	Cant.	%	Cant.	%	Cant.	%
Infundados	8671	61.2%	2138	43.7%	1323	36.6%	130	40.0%	12262	53.3%
Fundados	5371	37.9%	1279	26.1%	2029	56.1%	86	26.5%	8765	38.1%
Improcedentes(1)	0	0.0%	1080	22.0%	172	4.8%	75	23.0%	1328	5.8%
Otros(2)	125	0.9%	401	8.2%	92	2.5%	34	10.5%	652	2.8%
Total de reclamos	14167	100.0%	4898	100.0%	3616	100.0%	325	100.0%	23007	100.0%
Total de contrataciones (millones)(3)	3.52		3.44		3.24		3.07		13.33	
Tasa de reclamos fundados	15.2 cada 10 mil contrataciones		3.7 cada 10 mil contrataciones		6.3 cada 10 mil contrataciones		0.3 cada 10 mil contrataciones		6.6 cada 10 mil contrataciones	

Nota:
(1) Al total de reclamos improcedentes de Telefónica, América Móvil, Entel y Viettel, que es 1327, se le suma un reclamo improcedente de una de las OMVs, y se obtiene 1328.

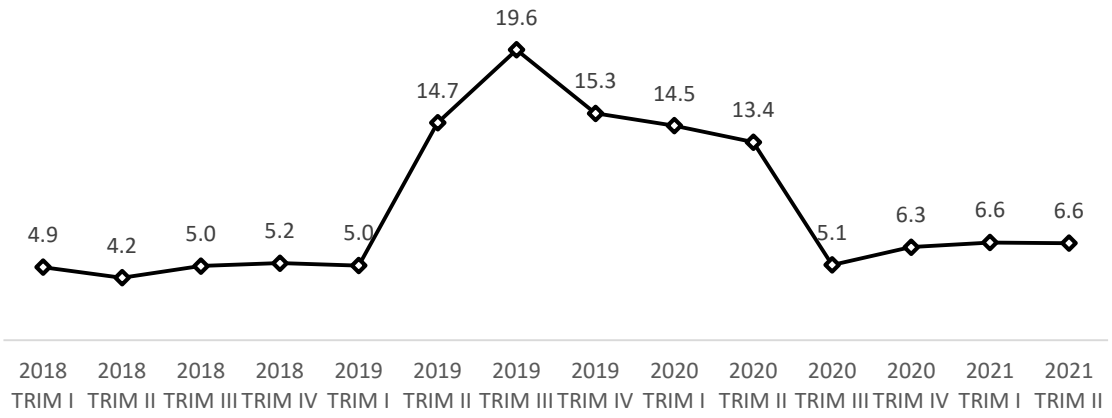
[36] Parcialmente fundados, fundados por razones comerciales, entre otros.

(2) En “Otros” se incluyen las resoluciones parcialmente fundadas y las fundadas por razones comerciales.
(3) Al total de contrataciones de Telefónica, América Móvil, Entel y Viettel se le añaden las contrataciones de las OMV (0.06 millones), y se obtiene 13.3 millones de contrataciones.

Fuente: PUNKU.
Elaboración: OSIPTEL.

A nivel de todo el mercado, la tasa de reclamos fundados en contrataciones no solicitadas ha sido de 6.6 durante el primer semestre del 2021. La evolución de este indicador ha tenido un período de incremento durante el 2019 y progresiva reducción en el 2020, como se apreciar en el gráfico N° 4. No obstante, se debe señalar la reducción de los niveles de incidencia en el 2020 se deben al confinamiento decretado en atención a la propagación del Covid 19 y la implementación de las nuevas reglas dictadas por el OSIPTEL para hacer más seguro el proceso de portabilidad numérica.

Gráfico N° 4
INCIDENCIA DE RECLAMOS FUNDADOS EN CONTRATACIONES NO SOLICITADAS
(Cada 10,000 contrataciones)



Nota: En reclamos fundados no se incluyen los reclamos fundados por razones comerciales.
Fuente: PUNKU.
Elaboración: OSIPTEL.

No obstante, se debe advertir que este indicador de incidencia solo recoge los casos identificados de los usuarios que decidieron formular su reclamo; por lo que la dimensión del problema probablemente sea mucho mayor y requiera, por tanto, de más medidas regulatorias. En ese sentido, este indicador de incidencia solo nos ayuda para mostrar el progreso que el OSIPTEL ha alcanzado; pero no puede ser utilizado para argumentar que el problema ya no existe o que se encuentre en niveles socialmente aceptables.

Al respecto, se debe señalar que los casos de contratación no solicitada podrían generar diversos problemas y riesgos a los usuarios. Por ejemplo, se han observado casos en los que se han cometido delitos (extorsiones, secuestros, etc.) con la línea contratada a nombre de usuarios que desconocían la contratación. Incluso, estos usuarios se han visto involucrados, en calidad de cómplices, y han tenido que enfrentar procesos judiciales para demostrar que ellos no habían solicitados la línea. Asimismo, también se han dado casos en los que los asesores han estado vendiendo líneas supuestamente “preactivadas”, que en realidad estaban activadas a nombre de otro

usuario, el cual lamentablemente ha tenido que asumir las deudas por el consumo de líneas que no ha contratado.

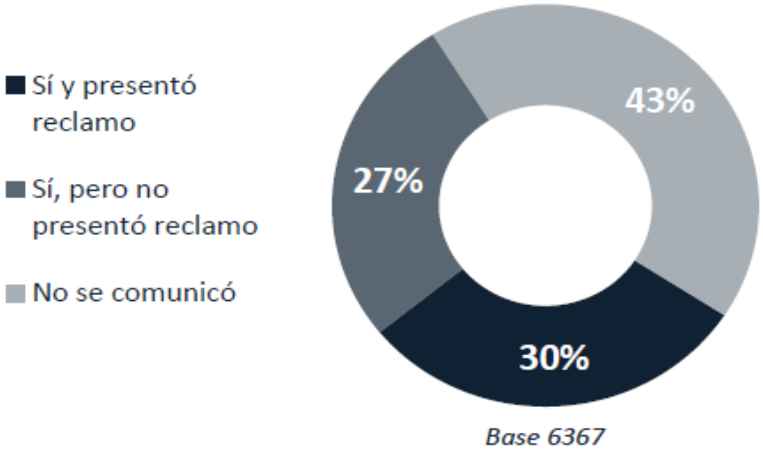
En muchos casos, la afectación generada por estos fraudes puede ser equivalente a todo el ingreso familiar del mes, o a los ahorros acumulados durante varios años. Es decir, individualmente, estos fraudes generan un daño enorme en la economía familiar, afectando directamente su capacidad de satisfacer sus necesidades básicas (alimentación, salud, etc.)

Esta afectación potencial es bastante variada entre las víctimas de contrataciones no solicitadas, y es muy probable que varios casos no hayan sido denunciados porque el usuario tuvo la suerte de no haber sufrido un problema grave; por lo que se puede asumir que al OSIPTEL solo estarían conociendo casos de usuarios con problemas complejos y mediáticamente llamativos; y que, en realidad, la contratación no solicitada tiene una escala de incidencia mucho mayor.

En efecto, entre los usuarios existe una alta tasa de no denuncia cuando enfrentan problemas de este tipo, usualmente debido a la desconfianza en la capacidad del Estado para recuperar las pérdidas sufridas. Según el INEI (2021), en el 2021, el 34.2% de las personas víctimas de algún hecho delictivo no formula una denuncia porque considera que es una pérdida de tiempo; es decir, que no va ser efectiva para recuperar lo perdido u obtener justicia.

Asimismo, en el caso del sector telecomunicaciones, evaluando la conducta de los usuarios, se ha podido observar que cuando enfrentan problemas con las empresas operadoras, en general, no suelen comunicarlo y mucho menos presentar el reclamo. Así, del Estudio sobre el nivel de Satisfacción del Usuario de telecomunicaciones y sobre el nivel de conocimiento de los derechos y obligaciones de los usuarios de los servicios públicos de telecomunicaciones 2020 (Estudio de Satisfacción 2020), se observa que, en el servicio de telefonía móvil, aproximadamente el 70% de usuarios que experimentan un problema no presentan un reclamo, el 43% ni siquiera comunica su problema a la empresa operadora (ver gráfico N° 5).

Gráfico N° 5
CONDUCTA DEL USUARIO FRENTE A UN INCONVENIENTE

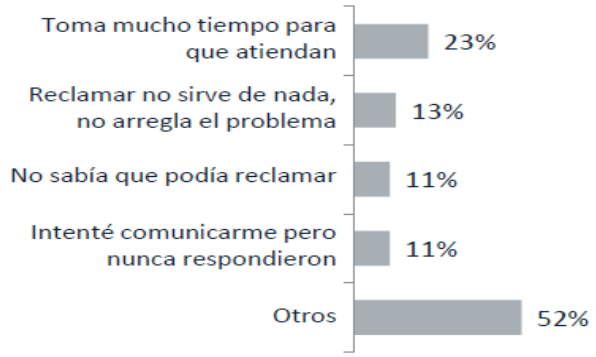


Base 6367

Nota: Pregunta: "¿Comunicó a su operador sobre este problema para que lo atienda?"
Fuente: Arellano Marketing

Por otra parte, al consultar a los usuarios el motivo de no presentar el reclamo, se identificó que tienen la percepción de que les toma demasiado tiempo la espera (23% del total de usuarios) o perciben que la empresa no solucionará el problema (13% del total). Esto evidencia que, en realidad, los usuarios no confían en el procedimiento actual de presentación de reclamos y lo consideran una pérdida de tiempo, ya que no resultará en una solución para su inconveniente (ver gráfico N° 6).

Gráfico N° 6
MOTIVOS DE NO PRESENTACIÓN DE RECLAMOS



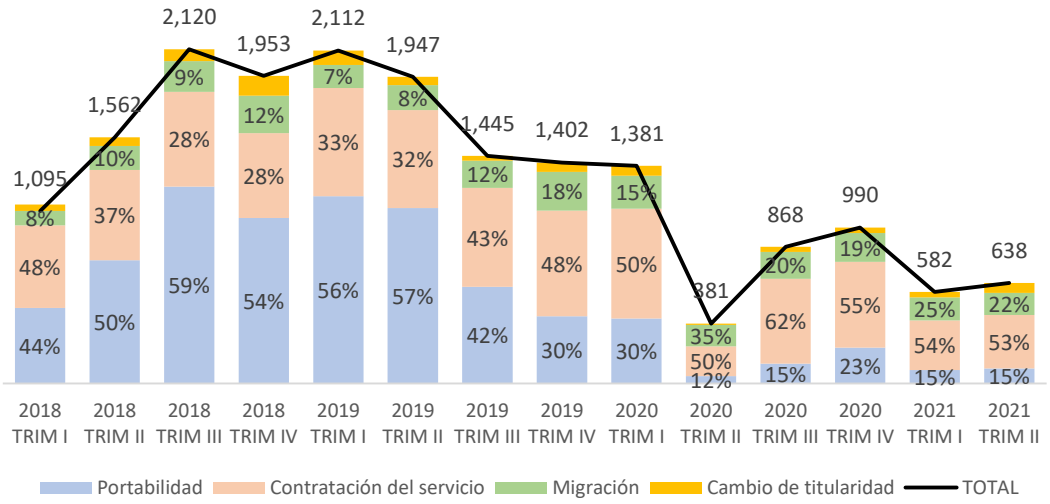
Fuente: Arellano Marketing

En consideración de lo anterior, se puede asumir que la escala del problema de contratación no solicitada es mucho mayor que lo que indicador de incidencia, antes mencionado, puede sugerir. Además, se debe considerar que los casos de contratación no solicitada que llegaron ser formulados como un reclamo se han caracterizado por tener una alta complejidad y gravedad, por lo que resulta necesario aplicar medidas regulatorias adicionales para reducir más la incidencia de estos problemas.

d) Problemas reportados al OSIPTEL

En paralelo a los reclamos presentados, varios usuarios se han dirigido directamente a las oficinas del OSIPTEL para reportar casos de contratación no solicitada en el servicio público móvil. Específicamente, entre el 2018 y 2021, se acercaron al OSIPTEL 7902 usuarios que indicaron no haber contratado un servicio, 7465 no haber sido la portabilidad, 2385 haber sido migrado a otro plan tarifario sin su autorización y a 764 les cambiaron la titularidad de su línea, un total de 18 476 casos. En el gráfico N° 7 se puede apreciar que la cantidad de este tipo de casos se ha reducido en el 2021 respecto al 2018 y 2019, dado que el promedio trimestral ha pasado de 1 705 a 610 casos.

Gráfico N° 7
PROBLEMAS DE CONTRATACIÓN NO SOLICITADA REPORTADOS AL OSIPTEL EN EL SERVICIO PÚBLICO MÓVIL



Fuente: Sistema de Atención a Usuarios (ATUS).

Cabe señalar que el progresivo control que se han logrado de las contrataciones no solicitadas se debe a las modificaciones normativas de Condiciones de Uso, implementadas en el 2018 (Resolución N° 96-2018-CD-OSIPTEL) y 2020 (Resolución N° 006-2020-CD/OSIPTEL); la emisión del TUO de Portabilidad[37] y los esfuerzos realizados en la supervisión y monitoreo por parte del OSIPTEL.

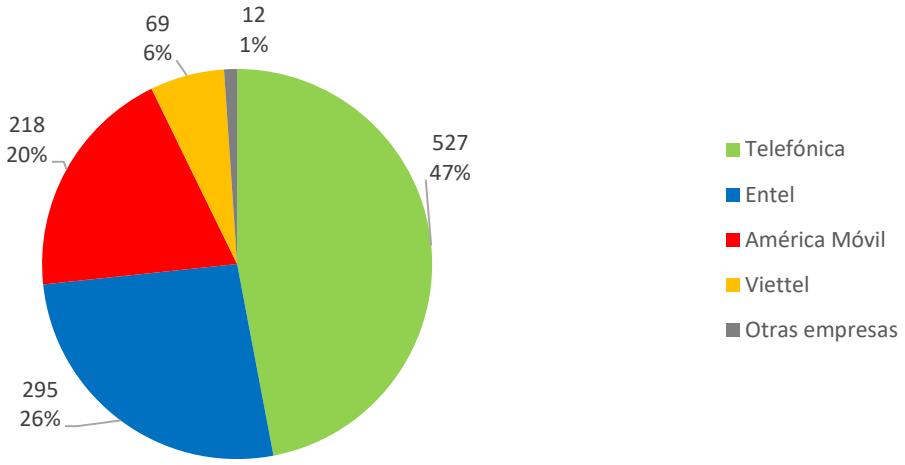
No obstante, los problemas presentados por los usuarios ante el OSIPTEL son solamente una porción del total de casos de contrataciones no solicitadas, dado que los usuarios de los servicios públicos de telecomunicaciones no suelen presentar sus reclamos o comunicar sus problemas. En efecto, según el Estudio de Satisfacción, se sabe que el 43% de los usuarios ni formula un reclamo ni lo comunica a la empresa operadora, mucho menos al regulador. En ese sentido, es probable que existan muchas más víctimas de contrataciones no solicitadas que han optado por resolver su problema sin realizar actos públicos de reclamos.

En el primer semestre 2021, se registraron 1220 denuncias de usuarios respecto a contrataciones no solicitadas en el servicio público móvil, el 53% de los casos está relacionado con altas nuevas, el 15% con la portabilidad no solicitada, 23% con migraciones de plan tarifario no autorizados y 8% en los que se hizo el cambio de titularidad.

Asimismo, considerando solo los 1121 casos de altas nuevas, portabilidad no solicitadas y migraciones, las empresas operadoras con mayor cantidad con este tipo de problema son Telefónica con el 44% del total, seguido de Entel, América Móvil y Viettel con el 27%, 20 y 8%, respectivamente. Cabe señalar que, el problema de contratación no solicitada se encuentra presente en todas las regiones del país las regiones, y las regiones con mayor cantidad de problemas son Lima, Lambayeque y Cusco con 380, 79 y 44 casos, respectivamente.

[37] Resolución N° 286-2018-CD-OSIPTEL.

Gráfico N° 8
PROBLEMAS DE SOLICITUDES DE ALTAS Y PORTABILIDAD NO SOLICITADAS POR EMPRESA OPERADORA



Fuente: ATUS.
Elaboración: OSIPTEL.

e) Casos graves de contratación no solicitada

Si bien los casos reportados al OSIPTEL son un subconjunto del total de usuarios que formularon un reclamo y de los usuarios que no denunciaron, se trata de casos que implican una mayor gravedad, debido a que han significado para los usuarios algún tipo de pérdida económica. En efecto, se han dado casos de usuarios que se han visto en graves problemas debido no solo a un error administrativo por parte de los asesores de las empresas operadoras, sino también porque inesperadamente fueron comprometidos en el pago de deudas generadas por varias líneas a su nombre o el uso de líneas a su nombre para la comisión de actos delictivos.

Al respecto, se debe recordar los casos mediáticos de las usuarias Guicela Taboada Campos y Eliana Ramos[38], quienes fueron vinculadas con procesos judiciales, dado que desde algunas de las líneas que se registraron bajo su titularidad, sin su consentimiento, se cometieron determinados delitos. En el caso de la Sra. Taboada Campos, se registraron indebidamente más de 21 mil líneas móviles bajo su titularidad[39].

En relación a estos 2 casos, desde la perspectiva del OSIPTEL, como regulador del sector telecomunicaciones, el problema subyacente es que las empresas operadoras hayan podido permitir que se contraten un número tan grande de líneas a nombre de un usuario, y que se ha vulnerado de manera sistemática el protocolo de verificación de identidad. Las consecuencias de estas fallas las sufren naturalmente los usuarios, en estos 2 casos, los afectados se han visto involucrados en procesos judiciales.

Asimismo, se tiene el caso del señor Gil de la Cruz, quien manifestó que la empresa Telefónica le ha realizado recargos por planes que no solicitó. Este usuario ha señalado

[38] Fuente: https://larepublica.pe/sociedad/947539-mafia-la-suplanta-paraobtener-chips-y-ahora-ella-puede-ir-a-prisio
[39] https://panamericana.pe/24horas/locales/207855-delincuentes-sacan21-000-lineas-nombre-mujer-policia

que lo habrían abordado en la vía ambulatoria ofreciéndole la entrega de las *SIM cards* de manera gratuita, para lo cual le solicitaron colocar su huella dactilar hasta en cuatro oportunidades, siendo informado que la solicitud no podría ejecutarse debido a que su huella no podía ser leída.

Posteriormente, el referido usuario tomó conocimiento que tenía dos líneas a su nombre con deuda pendiente, generándole un importante perjuicio económico, especialmente, considerando su situación económica. Su testimonio y detalle del caso fue expuesto en un reportaje realizado por el canal América Televisión[40].

En el caso del señor Gil de la Cruz, evidentemente resulta sorprendente cómo la empresa operadora puede contratar a nombre de este usuario otras líneas, y generar deudas por consumos que no realizó. Esto revela que la información personal que el usuario brinda a las empresas operadoras no estaría siendo debidamente protegida, y que tal vez, algún trabajador ha estado aprovechan esa información para poder realizar contrataciones. Nuevamente en este caso, no se trata solo de un problema de seguridad ciudadana, sino que existe un problema en el sector telecomunicaciones que el regulador debe abordar.

Adicionalmente, se tiene el caso del señor Eulalio Máximo Torres Pariona, quien fue sentenciado a 14 años de pena privativa de libertad por cuanto se vio involucrado con la comisión de un delito de robo agravado, siendo que los asaltantes dejaron en su huida un celular que habría tenido contacto con una línea móvil que figurada bajo su titularidad.

Al respecto, el señor Torres Pariona en su demanda de revisión de sentencia presentó como nueva prueba la resolución de Telefónica en la cual la empresa declaraba procedente su reclamo por contratación no solicitada, así como, una comunicación de la referida empresa operadora en la cual reconocía que no contaba con un mecanismo de contratación que lo vincule con tal servicio. Sin embargo, la Sala Permanente de la Corte Suprema de Justicia consideró que tales documentos no desvirtuaban el hecho que el señor Torres Pariona figure como titular de la línea móvil que recibió llamadas recurrentes del equipo terminal encontrado en la escena del crimen.

En el caso del señor Torres Pariona lo que se aprecia más son las consecuencias de las fallas en los procesos de contratación de líneas nuevas. En este caso se demuestra claramente que adquirir un servicio público móvil no es para nada semejante a comprar un caramelo, etc.; y que por ello es necesario que se contrate en condiciones de seguridad y confiabilidad.

De otro lado se observa el caso de la señora María Nunura de Gómez, adulta mayor, quien registró bajo su titularidad servicios en la empresa Telefónica, Claro y Entel, y quien pese a reclamar ante la empresa operadora Entel por dos servicios registrados indebidamente bajo su titularidad, registró posterior a ello, un nuevo servicio no contratado.

Cabe indicar que, los casos antes descritos no fueron los únicos casos públicos de suplantación de identidad en la contratación de servicios móviles, sino que se trata de una problemática que ha sido advertida, en diversas ocasiones, por los medios de comunicaciones.

[40] Mediante el siguiente enlace se puede acceder al reportaje completo: http://plataforma.ipnoticias.com/Landing?i=8rjVc38Q1fmQN9n3eazhjw%3d%3d&cac=9vwFptpXwPNrtlsp6MGOtg%3d%3d&c=X0%2bG9t64v9LyGzW3mHYSaRQrd83x9Aq37pHC%2fKIzdXE%3d&utm_source=alerta&utm_medium=correo&utm_content=video&utm_campaign=videomail

Ciertamente, muchos de estos casos podrían ser considerados como errores cometidos por parte del personal encargado por las empresas operadoras para atender este tipo de solicitudes. Sin embargo, una parte de estos casos se trata de solicitudes propiciadas por terceras personas con la intención de cometer actos delictivos que; por ello, prescindiendo de su cantidad o incidencia, resultan altamente preocupantes, debido a que podrían haber generado una considerable pérdida económica a las víctimas.

f) Casos graves que generaron robos

Los casos detallados previamente corresponden a denuncias realizadas durante el 2019 y 2020, y se caracterizan por generar afectaciones indirectas al usuario: contratación de líneas a su nombre, incriminación en delitos realizados con esas líneas, generación de deudas por el consumo realizado en esas líneas, etc. Lo que se está observando en lo que va del año 2021, es una oleada creciente de suplantaciones en los trámites de reposición de *SIM card*, cambio de titularidad y contratación de nuevas líneas que se enfocan en atentar directamente con el patrimonio y el sueldo de los usuarios, específicamente robar las cuentas bancarias, los bonos o subsidios que entrega el gobierno, etc.

Al respecto, el Banco de la Nación ha remitido la carta N° 109-2021-BN/2000, de fecha 13 de julio del 2021, en la cual indican que en el mes de marzo del 2021 se identificaron los primeros reclamos de clientes del Banco de la Nación que aseguraban haber perdido la señal de su dispositivo móvil, y que durante ese período se ejecutaron varias transferencias de dinero a través del canal Banca Móvil (app). Mediante esta modalidad, terceras personas acceden a claves secretas remitidas vía SMS y con ello sustraen parte del saldo de la cuenta de ahorros de las víctimas.

El Banco de la Nación refiere que, a partir de sus investigaciones, se encontró que las operaciones o transferencias se realizaron desde un dispositivo móvil distinto al cliente, es decir, se utilizó claves SMS remitidas al número celular del cliente; sin embargo, la línea celular del cliente había sido trasladada previamente a otro dispositivo móvil a través de la reposición fraudulenta de chip. En la referida carta, esta entidad bancaria reportó un total de 83 bonos suplantados mediante la suplantación del chip.

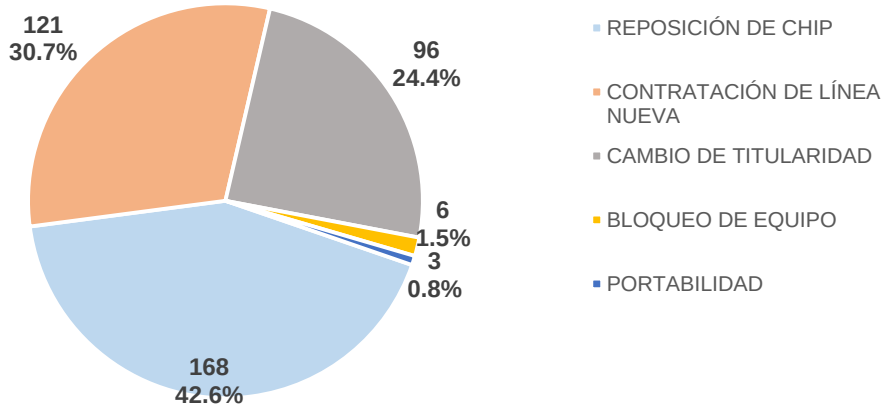
Cabe señalar que el OSIPTEL es consciente que la problemática trasciende el ámbito de las telecomunicaciones, y que es importante que los diversos organismos estatales tomen acciones para poder mitigar estas amenazas. Por ello, el OSIPTEL, mediante carta C.185-PD/202141 solicitó a la Presidencia del Consejo de Ministros lidere las coordinaciones con las distintas entidades públicas (como el Ministerio del Interior, el Ministerio Público el RENIEC, la Defensoría del Pueblo, la Superintendencia de Banca, Seguros y AFP, y el Banco de la Nación) y organizaciones representativas del sector privado como ASBANC y AFIN, que se encuentran involucradas con dicha problemática.

En ese sentido, el análisis del problema de los fraudes con SIM swap que se realiza en este informe, si bien se concentra en lo que se refiere al ámbito de las telecomunicaciones, ello no implica perder de vista que existen otros actores o entidades que intervienen y que también podrían aportar para mejorar los niveles de seguridad de los usuarios.

[41] De fecha 30 de noviembre de 2021.

En este contexto, se debe señalar que el problema de los fraudes a través de SIM swap se ha agudizado enormemente. Específicamente, entre enero y agosto del 2021, 394 usuarios se acercaron al OSIPTEL para reportar que había sufrido un fraude y el robo en sus cuentas bancarias debido a la reposición no solicitada de la *SIM card* (42.6%), la contratación no solicitada del servicio (30.7%) y cambio de titularidad (24.4% de los casos), como se puede apreciar en el gráfico N° 9.

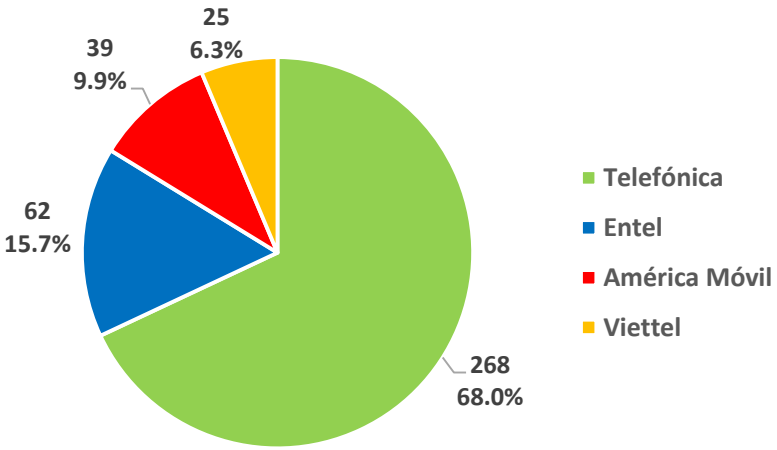
Gráfico N° 9
DENUNCIAS REPORTADAS AL OSIPTEL
PRIMER SEMESTRE DEL 2021



Fuente: Sistema de Atención a Usuarios (ATUS).
Elaboración: OSIPTEL.

Cabe señalar que del total de casos reportados al OSIPTEL entre enero y agosto del 2021, Telefónica concentra el 68% de estos casos debido a una inadecuada reposición de la *SIM card* o el cambio de titularidad. Los casos de Entel, América Móvil y Viettel, en conjunto solo significan el 31.9% de los casos, como se puede apreciar en el gráfico N° 10.

Gráfico N° 10
DENUNCIAS REPORTADAS AL OSIPTEL POR EMPRESA
PRIMER SEMESTRE DEL 2021



Fuente: Sistema de Atención a Usuarios (ATUS).
Elaboración: OSIPTEL.

Asimismo, en cumplimiento de un requerimiento de información, América Móvil, Entel y Viettel reportaron casos adicionales de usuarios que en ese período sufrieron la reposición fraudulenta del *SIM card*, una contratación o cambio de titularidad no solicitado. En el cuadro N° 6 se reportan la cantidad consolidada de estas denuncias, no se ha incluido a Telefónica porque esta empresa operadora no ha cumplido con remitir la información. Asimismo, se puede apreciar que el canal más utilizado para llevar a cabo este tipo de fraudes es el canal telefónico (62.3% de los casos). En el caso de Entel y Viettel, el canal presencial concentra el 70.3% y 97.7% de las denuncias; en cambio, en América Móvil los canales con más denuncias son el presencial y la App con el 37.6% y 38,2%, respectivamente.

Cuadro N° 6
DENUNCIAS REPORTADAS AL OSIPTEL POR EMPRESA Y CANAL DE ATENCIÓN
PRIMER SEMESTRE DEL 2021

	Entel		América Móvil		Viettel		Total	
	Cant.	%	Cant.	%	Cant.	%	Cant.	%
Presencial	130	70.3%	70	37.6%	86	97.7%	286	62.3%
App	7	3.8%	71	38.2%	0	0.0%	78	17.0%
No hay información	19	10.3%	25	13.4%	0	0.0%	44	9.6%
Telefónico	9	4.8%	16	8.6%	2	2.3%	27	5.9%
Autogestión	20	10.8%	4	2.2%	0	0.0%	24	5.2%
Total	**185**	**100%**	**186**	**100%**	**88**	**100%**	**459**	**100%**

Notas: (1) Información reportada al OSIPTEL del 1 enero al 18 de agosto del 2021.
(2) Telefónica no cumplió con remitir la información sobre estos casos.
Fuente: Sistema de Atención a Usuarios (ATUS).
Elaboración: OSIPTEL.

Sin embargo, es importante mencionar que existe un problema de trazabilidad en el canal presencia, dado que gran parte de sus contrataciones y reposiciones de SIM card que se están realizando de manera informal en la vía pública, por lo que muchas transacciones se estarían reportando como presenciales, en la realidad no serían ambulatorias.

A fin de comprender la dimensión de los problemas generados por la reposición fraudulenta de SIM card es necesario analizar los casos más recientes que han obtenido notoriedad gracias a la prensa. Por ejemplo, se tiene el caso Augusto Trelles Velásquez[42], quien refiere que entre el 8 y 11 de septiembre de este año, no tuvo o línea o su equipo móvil no funcionaba. Al percatarse de ello, llamó a Telefónica, cuyos asesores le indicaron que su *SIM card* probablemente estaba malogrado y que debía renovarlo.

Asumiendo como cierta la información errónea que el asesor de la empresa Telefónica le dio, este usuario acudió a la agencia de Real Plaza de Salaverry para solicitar la reposición de su *SIM card*. El trámite se realizó de manera regular, le entregaron una *SIM card*, y no le dieron ninguna explicación de la repentina anulación de su línea.

Posteriormente, y de manera inesperada, este usuario recibe el 14 de septiembre, un correo electrónico por la contratación de una SIM card de fecha 7 de septiembre, un día antes del período en que se encontró sin servicio. Este contrato no solicitado, se había realizado sin su firma, ni control biométrico ni presentación del DNI.

[42] https://sudaca.pe/noticia/informes/calvario-con-movistar-sim-swapping/

Cabe señalar que durante los días que este usuario no tuvo línea, los estafadores que se apropiaron de su número realizaron 10 pagos de servicio, 5 retiros de Rappicash y 2 compras internacionales, generando una pérdida de S/ 20 284.95. Todo esto fue posible, porque desde un equipo móvil se puede acceder a las cuentas bancarias.

El problema del señor Augusto Trelles Velásquez no se ha limitado a estas pérdidas económicas, sino también a que el estafador ha contratado una línea prepago a nombre de la víctima, y en el *WhatsApp* de esa línea ha puesto la foto del usuario, probablemente con el objetivo de seguir cometiendo estafas.

En este caso, las fallas cometidas en el proceso de autenticación y verificación de la identidad son las siguientes:

- Cuando el usuario consulta por la falta de servicio de su línea móvil, la empresa le indicó que la SIM car debería estar malograda. No se le informó que había una solicitud de reposición de SIM card. Se puede apreciar que esta falla se da en el personal de la empresa de telecomunicaciones, y no se trata de un problema generado por el banco.
- El usuario solicita una nueva reposición y la empresa operadora acepta el trámite, no se menciona nada sobre la anterior reposición de SIM card. Nuevamente se aprecia que la falla está en las empresas de telecomunicaciones.

Otro caso, más reciente, es el de la profesora Solange Palacios, quien refiere que el 22 de octubre de este año, extrañamente no tuvo servicio en su teléfono móvil, ella no pensó que su línea había sido bloqueada por un estafador. Cuando se acercó al Banco de la Nación para retirar su sueldo, le indicaron que su tarjeta estaba bloqueada, por lo que solicitó la información de sus transacciones. Habían realizado 2 giros a través del a App del banco por un monto total de S/ 2500 a una persona llamada Ángela Quispe. La señora Solange refiere que la empresa América Móvil realizó la reposición de la SIM card en una tienda Tambo con una persona desconocida, y que han pasado 30 días y todavía la empresa operadora no le ha remitido la supuesta validación biométrica.

Adicionalmente, también se tiene la denuncia de la profesora Yessica Caituro que perdió S/ 3000 debido a que sufrió el cambio de la SIM card por parte de la empresa operadora, y el caso de la profesora Diana Chero Pacheco[43] que perdió S/ 5630 por la reposición de la SIM card de la empresa Entel.

Recientemente en noviembre de este año, profesora, de nombre Milagros[44] denunció el robo de S/ 3000 de su cuenta bancaria del Banco de la Nación. Ella sostiene que el sábado 23 de octubre se quedó repentinamente sin llamadas, pasaron unos minutos y le llega un correo electrónico indicando que ha realizado una actualización de sus datos. Minutos después, le llegan notificaciones sobre 5 transacciones a su nombre por montos de S/ 1500. La usuaria se sintió impotente porque no podía llamar al banco para evitar el robo, dado que su línea estaba bloqueada. Asimismo, la usuaria señala que ha formulado su reclamo a la empresa Entel, pero después de un mes, todavía la empresa no ha contestado. Cabe señalar que los delincuentes intentaron apoderarse de S/ 7500, pero felizmente S/ 3000 fueron retenidos por el banco.

Un último caso identificado es el de la profesora María Teresa Jauregui[45], la cual sufrió la suspensión del servicio móvil de Telefónica el día 18 de noviembre. Al día siguiente,

[43] Denuncian nueva modalidad de estafa digital (ipnoticias.com)
[44] Mujer denuncia suplantación de identidad y que hampones le robaron S/3.000 de su cuenta tras quedarse sin señal telefónica | nndc | LIMA | EL COMERCIO PERÚ
[45] Aparece otra profesora víctima de robo con modalidad de chip (ipnoticias.com)

ingresa a la aplicación del Banco de Nación para revisar sus cuentas, y descubrió que le habían robado S/ 3000. La víctima refiere que Telefónica trasfirió la titularidad de su línea a una persona llamada Giovanni Cora, y que el representante de la empresa Telefónica le indicó que solo presente su incomodidad al libro de reclamaciones.

Se puede apreciar que el factor común de todas estas estafas es la facilidad que existe una gran facilidad para poder bloquear la línea de un usuario (primera falla del lado de la empresa de telecomunicaciones) y solicitar la reposición del SIM card o el cambio de titularidad (segunda falla del lado de la empresa de telecomunicaciones); lo que viene después, es decir la vulneración de las cuentas bancarias, ciertamente son fallas del lado de las empresas financieras.

Por lo tanto, a partir de estos casos resulta evidente que este un problema que atañe al sector telecomunicaciones, no es mero problema de las empresas financieras o algo debe ser abordado como un problema de seguridad ciudadana; sino que, por el contrario, estos casos revelan la falta de seguridad y confiabilidad que tienen las empresas operados de telefonía móvil, y que necesariamente debe ser abordado y evaluado por el OSIPTEL, como el regulador del sector.

Por otra parte, considerando la información de fraudes reportados al OSIPTEL y a las empresas, se ha estimado la afectación o pérdida económica a partir de 63 casos; no obstante, no se debe interpretar que en los otros casos no hubo pérdida económica, dado que en la mayoría de los casos los usuarios afirman haber sufrido un robo, pero no detallan el monto. Como se puede apreciar en el cuadro N° 7, la pérdida promedio en los casos reportados al OSIPTEL ha sido S/ 10 065, y en los reportados a las empresas operadoras (Viettel) ha sido S/ 7113.

Cuadro N° 7
PÉRDIDA PROMEDIO DE LOS USUARIOS POR REPOSICIÓN FRAUDULENTA DE SIM CARD

Empresa	Pérdida promedio (Soles)	Cantidad de afectados
Reportados al OSIPTEL	10 065	23
Reportados por Viettel	7113	40

Fuente: Sistema de Atención a Usuarios (ATUS).
Elaboración: OSIPTEL.

Por otra parte, en las columnas A y B del cuadro N° 8 se reportan las denuncias recibidas por el OSIPTEL y las reportadas por las empresas operadoras, se aprecia que existe una relación de 3.8 a 1 entre estas dos magnitudes, por lo que se puede asumir que en el caso de Telefónica debería también cerca de 893 casos, de manera que se estima que en el período de enero a agosto del 2021 ha habido 1466 denuncias.

En las columnas “C”, “D” y “E” del cuadro N° 8 se reportan las cantidades estimadas de denuncias presentadas (i) al OSIPTEL, las que (ii) solo se presentan ante las empresas y las que (iii) no se denuncian. La estimación de los afectados que no denuncian se realiza considerando que, según el Estudio de Satisfacción 2020, solo el 57% de los usuarios comunica o formula su reclamo respecto a algún incumplimiento de la empresa. Así, a partir de estos supuestos, se estima que en un año se podría llegar a tener cerca 3858 afectados, de los cuales 1659 no van denunciar, 591 probablemente termine acercándose al OSIPTEL por la gravedad del daño y 1608 solo recurran a las

empresas operadoras. Estas estimaciones nos permiten apreciar más la dimensión del problema de los fraudes financieros realizados mediante la suplantación de los usuarios en los trámites de reposición de *SIM card*, contratación de servicio o cambio de titularidad.

Cuadro N° 8
ESTIMACIÓN DE LA CANTIDAD ANUAL DE AFECTADOS POR FRAUDE

Empresa	Denuncias presentadas de enero a agosto 2021		Ratio	Estimado anual de afectados por fraude			
	Ante el OSIPTEL (A)	Ante las empresas y el OSIPTEL (B)		Denuncian ante el OSIPTEL (C) [2]	Denuncian solo ante las empresas (D)[3]	No denuncian (E)[4]	Total (F)
Telefónica[1]	268	1007*		402	1109	1140	2650
América Móvil	39	186	4.8	59	221	210	489
Entel	62	185	3.0	93	185	209	487
Viettel	25	88	3.5	38	95	100	232
Total	**394**	**1466**		**591**	**1608**	**1659**	**3858**
Promedio			**3.8**				

Notas:
(1) La cantidad de denuncias presentadas ante Telefónica se obtuvo multiplicando el ratio promedio (3.8) con la cantidad de denuncias recibidas por el OSIPTEL para esta empresa (268), y se obtuvo un estimado de 1007.
(2) Se obtiene multiplicando el promedio mensual por 12 meses.
(3) Se obtiene multiplicando por 12 a la cantidad resultante de B menos A.
(4) Considerando que, según el Estudio de Satisfacción, la tasa de comunicación o denuncia es 57%, se estima que el total de afectados (F) es igual a la división de (C+D)/0.57, y el total de casos no denunciados a F menos (C+D).
Fuente: Información reportada por las empresas operadoras
Elaboración: OSIPTEL.

Considerando las cantidades anuales de afectados estimados en el cuadro N° 8, se ha procedido a distribuir estas cantidades respecto a dos tipos de fraudes, los casos de robos de bonos y los casos de robo de cuentas de ahorros o compras *on line*. En el cuadro N° 9 se reportan la cantidad estimada de afectados por tipo de fraude y respecto a los escenarios de denuncia (ante el OSIPTEL, las empresas o no denunció).

Cuadro N° 9
ESTIMACIÓN DE LA CANTIDAD ANUAL DE AFECTADOS POR TIPO DE FRAUDE

Tipo de fraude	Denuncias de enero a agosto 2021		Estimado anual de afectados por tipo de fraude			
	Ante el OSIPTEL	%	Denuncian ante el OSIPTEL (A)	Denuncian solo ante las empresas (B)	No denuncian (C)	Total
Bonos	120	30%	180	490	505	1175
Ahorros	274	70%	411	1118	1154	2683
Total	**394**	**100%**	**591**	**1608**	**1659**	**3858**

Notas:
(1) Para estimar la cantidad de afectados para las columnas A, B y C por tipo de fraude se aplican los porcentajes obtenidos: 30% para casos de bonos y 70% para ataques a las cuentas de ahorro.
Fuente: Información del ATUS y de las empresas operadoras.
Elaboración: OSIPTEL.

Finalmente, considerando que la pérdida promedio de los usuarios que denunciaron ante el OSIPTEL ha sido de S/ 10 065 y de los usuarios que solo denunciaron ante las empresas fue de S/ 7113, se ha estimado que la afectación anual asciende a casi S/ 12.8 millones. Cabe señalar que en el caso de la afectación de los denunciantes que

solo se acercaron a las empresas se asume que su perdida debería ser menor que la de los denunciantes que se dirigieron al OSIPTEL. Asimismo, se está asumiendo que las víctimas que no denunciaron tuvieron una pérdida de S/ 100. En el caso de los fraudes en bonos, la pérdida de S/ 600, y se asume que la causa de no denuncia puede ser incluso el desconocimiento de haber sido beneficiario del bono.

Cuadro N° 10
AFECTACIÓN ANUAL ESTIMADA DE LOS FRAUDES

Tipo de fraude	Afectación promedio (Soles)			Afectación anual estimada (Soles)			
	Ante el OSIPTEL	Solo ante las empresas	No denuncian	Denuncian ante el OSIPTEL	Denuncian solo ante las empresas	No denuncian	Total
Bonos(1)	600	600	600	108 000	293 865	303 161	705 027
Ahorros(2)	10 000	7000	100	4 110 000	7 828 242	115 370	12 053 612
Total				**4 218 000**	**8 122 107**	**418 531**	**12 758 639**

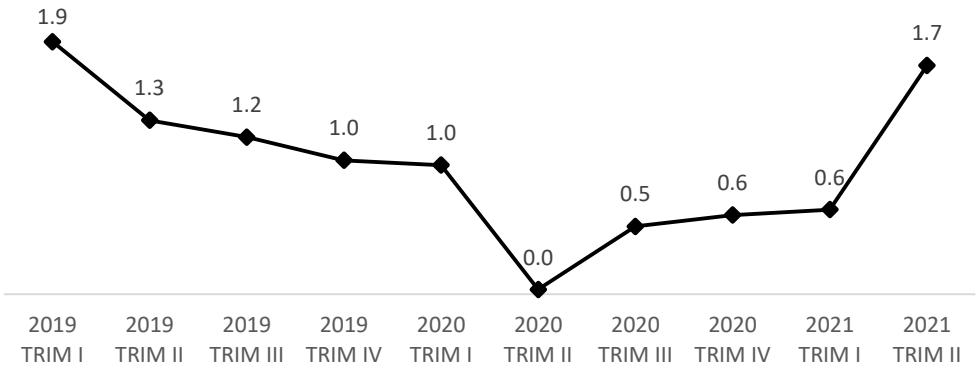
Nota: (1) El bono asignado es de S/ 600.
(2) Se asume una pérdida promedio de S/ 10 000 para los usuarios que denuncian ante el OSIPTEL, S/ 7000 para los que solo lo hacen ante la empresa y S/ 100 para los que no denuncian.
Elaboración: OSIPTEL.

Por otra parte, se debe señalar que esta pérdida podría alcanzar los S/ 50 millones[46] si no se resuelve el problema en los próximos 5 años. Incluso este nivel de pérdida podría ser mayor, dado que el crecimiento de esta práctica comercial podría incrementarse los próximos años de manera exponencial.

g) Cuestionamiento de titularidad prepago

Del 2019 al 2020, el promedio trimestral de cuestionamientos de titularidad prepago es de 932, lo que da un resultado anual de 3728 reclamos. Cabe señalar que los mencionados reclamos se redujeron en el primer semestre de 2020 como consecuencia de las restricciones impuestas durante la pandemia, sin embargo, la cantidad se viene revirtiendo y retomando los niveles anteriores.

Gráfico N° 11
CUESTIONAMIENTO DE TITULARIDAD SERVICIO PÚBLICO MÓVIL PREPAGO 2019-2021
(En miles)



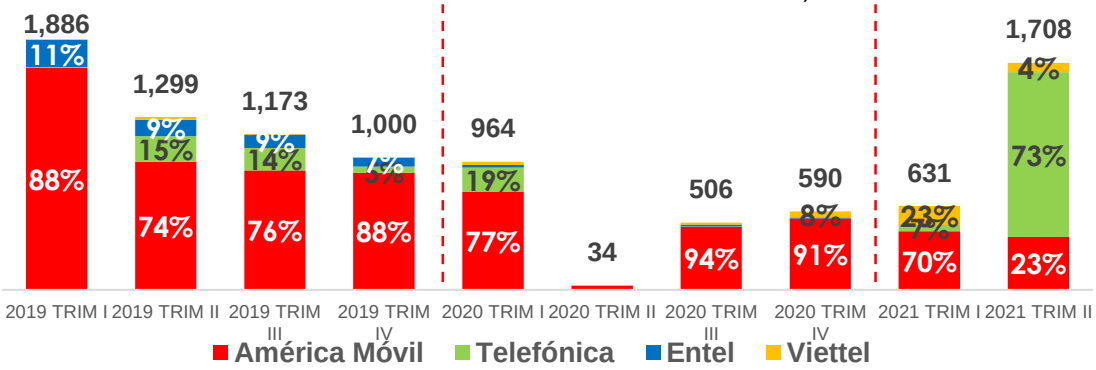
Fuente: PUNKU.
Elaboración: OSIPTEL.

[46] Este monto se obtiene aplicando una tasa social de descuento de 8.5%.

En los casos presentados en los años 2019 y 2020, si se encuentra una diferencia muy marcada por empresa operadora, la empresa operadora con una mayor cantidad de casos es América Móvil con una participación de 83% de total de cuestionamientos, seguido de Telefónica, Entel y Viettel, con el 8%, 7% y 2%, respectivamente. Sin embargo, en el año 2021, en el segundo trimestre del 2021, Telefónica incrementa su participación de 7% a 73%.

Al respecto, si bien las cantidades de cuestionamiento de titularidad son relativamente bajos, resulta importante recordar que en los servicios públicos de telecomunicaciones solo el 30% de los usuarios presenta reclamos cuando sufren un inconveniente con la empresa, y la mayoría no lo hace porque toma mucho tiempo y no sería efectiva. En ese sentido, es bastante probable que la cantidad de usuarios que sufrió el problema de una falsa titularidad de línea es mucho mayor.

Gráfico N° 12
CUESTIONAMIENTO DE TITULARIDAD SERVICIO PÚBLICO MÓVIL, I SEMESTRE 2021



Fuente: PUNKU.
Elaboración: OSIPTEL.

6.3. Agentes involucrados

Los agentes directamente involucrados son: (i) las empresas operadoras de servicios públicos de telecomunicaciones, (ii) los abonados de estos servicios y (iii) la entidad encargada de la regulación y supervisión (OSIPTEL).

6.4. Causas del problema

En esta sección se analizan las causas que explican el alto nivel de inconvenientes con las solicitudes de baja y migración. Específicamente, se han identificado 5 causas: (a) inadecuadas prácticas en la contratación de líneas móviles, (b) bajos incentivos para por parte de las empresas para adoptar soluciones efectivas a los problemas de fraude, (c) información sensible en los equipos terminales móviles, (d) limitado conocimiento de los usuarios sobre sus deberes y derechos y (e) vulnerabilidad de la verificación biométrica por existencia de bandas criminales organizadas.

a) Inadecuadas prácticas en la contratación de líneas móviles

La incidencia de reclamos por contrataciones no solicitadas y de cuestionamientos de titularidad de líneas prepago es causada por la implementación de inadecuadas formas de contratación por parte de las empresas operadoras. Al respecto, contrario a las normas establecidas por el OSIPTEL, que establecen que la contratación debería realizarse por distribuidores registrados y con dirección conocida; algunas empresas

operadoras han optado, en detrimento de los usuarios, contratar vendedores ambulantes para que recorran las calles y realicen la contratación y activación de líneas móviles en condiciones riesgosas para los usuarios.

Los riesgos de esta inadecuada e irresponsable práctica radican en que el usuario tiene que revelar sus datos personales y compartir su huella dactilar con personas desconocidas, solo identificables con chalecos de la empresa operadora. En la vía pública, los usuarios probablemente se encuentran distraídos y expuestos a que los vendedores inescrupulosos los induzcan a realizar contrataciones no deseadas, y en muchos casos, ni siquiera se les informa que están adquiriendo una nueva línea o realizando una portabilidad.

Una de las principales desventajas de contratar una línea móvil en la vía pública es que los usuarios no pueden exigir la presencia de un supervisor si en caso sospechan que el vendedor les engaña, por lo que se encuentran desprotegidos frente a una potencial estafa. Las empresas operadoras no han desarrollado protocolos especiales para garantizar que esta forma de contratar el servicio no sea riesgosa, por lo que su conducta reviste un grado de negligencia.

Al respecto, en junio del 2019, el OSIPTEL dispuso realizar acciones de monitoreo en las ciudades de Ica, Puerto Maldonado, Ucayali, Tumbes y Puno, a fin de verificar si la contratación de líneas móviles prepago mediante la venta de *chip* se venía realizando de conformidad con los requisitos y protocolos establecidos en los artículos 6 y 11-D del TUO de Condiciones de Uso. En las acciones realizadas en la ciudad, el mismo presidente del OSIPTE, Rafael Muente Schwarz pudo comprobar que la venta ambulatoria de chip no se realizaba en condiciones seguras para los usuarios.

En estas acciones de monitoreo se identificaron cinco casos[47] en los que el distribuidor de la empresa operadora América Móvil no exigió la verificación biométrica de la huella dactilar; debido a que, en realidad, las líneas ya se encontraban activas bajo la titularidad de terceras personas. Se identificó también un caso en Ica con la empresa operadora Viettel, donde se intentó comercializar un servicio público móvil activado sin realizar el registro de los datos del abonado. Estos casos se encuentran reportados en el cuadro N° 11.

Cuadro N° 11
CASOS IDENTIFICADOS EN EL MONITOREO DE JUNIO DEL 2019

Ciudad	Lugar de venta	N° telefónico	Empresa infractora	Fecha de adquisición
Ica	Plaza de Armas de Ica	977620754	Viettel	4/06/2019
Puerto Maldonado	Mercado Central Modelo	913924495	América Móvil	12/06/2019
Ucayali	Puerto Pucallpa	954167557	América Móvil	13/06/2019
Tumbes	Paseo Libertadores	969301316	Telefónica	13/06/2019

[47] Los casos mencionados y sus evidencias (videos y audios) se expusieron a los representantes de las empresas operadoras Telefónica del Perú S.A.A. (en adelante, Telefónica), América Móvil, Viettel y Entel Perú S.A. en una reunión de 26 de junio del 2019.

Puno	Alrededores del Centro Comercial Real Plaza	980458889	Telefónica	11/06/2019

Fuente: Acciones de monitoreo del OSIPTEL.
Elaboración: OSIPTEL.

En atención a este primer acercamiento con esta problemática, el OSIPTEL realizó, en el mes de julio del 2019, 109 acciones de supervisión a nivel nacional en la que se detectaron casos de contrataciones sin verificación biométrica realizadas por distribuidores itinerantes. Como resultado de estas acciones, se identificaron 96 casos con algún incumplimiento, lo que corresponde al 88% de los casos evaluados.

De este conjunto de casos identificados, América Móvil es la empresa con una mayor participación de incumplimientos (34%), le siguen Telefónica, Entel y Viettel, con 32%, 22% y 11%, respectivamente. A nivel regional, los departamentos con mayor cantidad de casos con incumplimiento son Arequipa y Ayacucho con 10 casos detectados en cada región.

Cuadro N° 12
CASOS IDENTIFICADOS EN LAS ACCIONES DE SUPERVISIÓN – JULIO DEL 2019

Empresa	Con incumplimiento		Sin incumplimiento		Total		Tasa de incumplimiento
	Casos	%	Casos	%	Casos	%	
América Móvil	33	34%	2	15%	35	32%	94%
Entel	21	22%	4	31%	25	23%	84%
Telefónica	31	32%	4	31%	35	32%	89%
Viettel	11	11%	3	23%	14	13%	79%
Total	**96**	**100%**	**13**	**100%**	**109**	**100%**	**88%**

Fuente: Acciones de supervisión en julio de 2019.
Elaboración: OSIPTEL.

En relación la casuística encontrada, se debe señalar que más del 91% de los distribuidores evaluados habrían brindado información no veraz a los usuarios solicitantes; en algunos casos, de forma inescrupulosa, los distribuidores de las empresas operadoras habrían comercializado líneas bajo la titularidad de terceras personas, para lo cual deliberadamente habrían inducido al usuario a no realizar su verificación biométrica.

Por otra parte, varios usuarios se han acercado a las oficinas del OSIPTEL para denunciar que fueron víctimas de vendedores ambulantes de *SIM card*, que les indujeron a contratar un servicio que no deseaban. A continuación, se detallan algunos casos identificados:

- **Orientación N° SAO 202136772:**

  Un usuario declara tener 2 líneas que no ha contratado, y detalla que probablemente se debe a que, en una oportunidad, un vendedor ambulante de Telefónica, lo abordó para venderle una *SIM card*. En el momento, al parecer no

se ejecutó la solicitud, pero posiblemente ese vendedor haya aprovechado para contratar 2 líneas a nombre de la víctima.

- **Orientación N° SAO 202112908:**

  Una usuaria declaró que había realizado una reposición de la *SIM card* con un vendedor ambulante de Telefónica, pero no se percató que este vendedor había solicitado un servicio postpago sin su autorización.

- **Orientación N° SAO 1902046870:**

  El usuario refiere que tiene varios números a su nombre, debido a que los vendedores ambulantes lo habrían registrado engañosamente con el lector biométrico.

- **Orientación N° SAO 1902009804:**

  El usuario indica que una vendedora ambulante, hizo que pusiera varias veces su dedo para la verificación biométrica, indicándoles que no reconocía su huella dactilar. En los meses siguientes, la empresa operadora le comunica que tiene deudas por 10 números a su nombre.

- **Orientación N° SAO 1802004021:**

  Un usuario manifiesta que le realizaron una portabilidad no solicitada, debido a que en la calle una asesora le ofreció de regalo una *SIM card*, y luego le realizaron una portabilidad no solicitada.

- **Orientación N° SAO 1902043969:**

  El usuario indica que un vendedor se le acercó bajo la premisa que le regalaría un *SIM card*, y que luego descubrió por una portabilidad no solicitada.

- **Orientación N° SAO 1802113111:**
  El usuario detalla que en la calle le ofrecieron de regalo una *SIM card*, el cual recibió sin saber que ocasionaría una portabilidad de la línea.

En los casos detallados, se aprecia que los usuarios han tenido una mala experiencia con los asesores que ofrecen la contratación del servicio en la vía pública. Específicamente, estos vendedores aprovechan que la vía pública no es un espacio adecuado para realizar la verificación biométrica o para el registro de la información personal del solicitante; por lo que, de manera engañosa, induce a los usuarios a proporcionar su huella dactilar para contratar o portar líneas que ellos no solicitan.

En efecto, la contratación realizada en la vía pública resulta más insegura que la que se hace en la oficina misma de la empresa operadora. Cuando el usuario se acerca a una oficina comercial, tiene la certeza de que los asesores que lo atienden pertenecen a la empresa operadora, además estos asesores están siendo supervisados, existen cámaras de vigilancia, sus datos personales serán registrados en los servidores de la empresa operadora, etc.

En cambio, cuando la contratación del servicio es en la vía pública, el usuario no tiene la capacidad para verificar si el vendedor realmente es de la empresa operadora, ni la forma de evitar que sus datos personales sean utilizados con otros fines y, sobre todo, no hay un supervisor cercano a quien pedir explicaciones cuando el comportamiento del vendedor es sospechoso. En ese sentido, realizar las contrataciones en la vía pública es una práctica irresponsable y meramente mercantilista por parte de empresas operadoras que no ponen la seguridad de sus usuarios como prioridad.

El carácter mercantilista de esta práctica comercial radica en que las empresas operadoras que venden las *SIM card* solo quieren obtener nuevos clientes, pero pretenden que los riesgos inherentes de esta práctica lo asuman los usuarios. En efecto, cuando un usuario luego de un tiempo descubre que, con sus datos personales, los vendedores de estas empresas han contratado varías líneas, tiene que asumir el costo de demostrar que esa contratación ha sido irregular.

Asimismo, se revisó la información de los expedientes de los reclamos resueltos en primera instancia por las empresas operadoras, en dicha revisión se encontró casos de usuarios que declararon que su huella dactilar fue tomada en la calle, y esta se utilizó para realizar operaciones y contratar servicios que ellos no requirieron:

- **Reclamo N° OFR-269618-2021, del 09.06.2021:**

  El usuario declara que paso la verificación biométrica en la calle porque deseaba comprar un chip prepago de Telefónica y, le dijeron que su huella no pasaba, por ende, no le dieron el chip. No obstante, luego se percata que tiene la titularidad un número postpago y una deuda que desconoce.

- **Reclamo N° OFR-234332-2021, del 21.05.2021:**

  El usuario declara que un asesor de Telefónica le ofreció un chip de recarga que no le entregaron indicándole que su huella biométrica no es legible; no obstante, días después descubre que tiene la titularidad de una línea postpago.

- **Reclamo N° PORT-92283-2019, de 10.01.2019:**

  El usuario declara que realizaron una portabilidad numérica sin su consentimiento; y que ello se realizó cuando engañosamente le regalaron un chip prepago que debía ser una nueva línea, y no una portabilidad.

- **Reclamo N° 190227571, del 03.09.2019:**

  El usuario declara que se le está cobrando el monto de una factura de S/ 108, cuando nunca quiso adquirir dicho plan de la empresa América Móvil. Refiere que le entregaron un chip gratis en la calle y nunca se le informó que tendría plan.

- **Reclamo N° 190233321:**

  El usuario declara que le prometieron que le iban a regalar un chip de la empresa América Móvil; no obstante, en el momento le dijeron que no había señal y no le dieron el chip. Afirma que se quedaron con el chip, y que nunca tuvo el servicio postpago de América Móvil.

- **Reclamo N° 190243914:**

  El cliente indica que le dieron un chip de América Móvil en la calle, pero no le indicaron que era una línea postpago; por lo que no reconoce que haya contratado el plan Max Ilimitado 65.

Por lo tanto, la contratación de líneas móviles en la vía pública constituye una práctica inadecuada, debido a que las empresas operadoras no la han venido realizando con los protocolos de seguridad establecidos por el OSIPTEL. Este tipo de práctica es una de las principales causas de que se generen contrataciones no solicitadas, e incluso filtraciones de la información personal de los usuarios.

b) Bajos incentivos por parte de las empresas para adoptar soluciones efectivas

El OSIPTEL ha requerido la actuación de manera voluntaria por parte de las empresas operadoras con la finalidad de prevenir la ocurrencia de contrataciones no solicitadas y de fraudes financieros. Sin embargo, las empresas operadoras no han mostrado una actitud proactiva, resolutiva y homogénea que permita subsanar las fallas en el proceso de contratación que podrían incrementar el riesgo de incidencia de actos delictivos.

En relación con el problema de la contratación o activación del servicio en la vía pública, América Móvil, Entel y Viettel solo han aceptado restringir que un usuario solo pueda contratar una vez cada 30 días o dos veces cada 120 días en el canal ambulatorio, mientras que Telefónica ha accedido a quitar la autorización a sus distribuidores de ofrecer en la vía pública las *SIM card*. En contraste, solo América Móvil, Entel y Viettel han accedido a implementar la verificación biométrica de los asesores previo a cada contratación y la denuncia penal de los distribuidores que incurran en alguna ilegalidad; pero Telefónica no ha adoptado estas medidas.

De igual manera, con la finalidad de prevenir la ocurrencia de casos de usuarios que indiquen que han sido víctimas de fraudes bancarios, se exhortó a las empresas operadoras para que, de forma voluntaria, dispongan la realización de trámites de reposición de la *SIM card* exclusivamente en los centros de atención y puntos de venta designados para atención de usuarios en provincias, que han sido previamente reportados al OSIPTEL; esto es, se restrinja el uso de autoservicios, *delivery* u otra forma de atención no presencial de dicha solicitud. Asimismo, se requirió considerar la implementación de un procedimiento que se diseñó con la finalidad de incrementar las medidas de seguridad de este trámite.

Sin embargo, las empresas operadoras no han adoptado de manera voluntaria la inclusión de estas medidas, siendo que, en el mejor de los casos, solo han adoptado como máximo 6 de las 16 medidas propuestas. Asimismo, existen recomendaciones que ya habían sido consideradas por la misma empresa operadora, otras que han implementado parcialmente y otras en las que han implementado medidas alternativas.

Cabe precisar que, los motivos que expresan las empresas operadoras para no efectuar algunos criterios son que (i) ellos ya se encuentran cumpliendo con la normativa vigente, (ii) existen complicaciones de procedimiento, (iii) solo aplican recomendaciones o brindan información adicional a solicitud del usuario o situaciones específicas, entre otras. Sin embargo, también existen casos en los que no se pronuncian sobre las recomendaciones planteadas.

Respecto al primer argumento para no implementar recomendaciones debido a que actualmente ya cumplen con lo que establece la norma, es importante precisar que esta posición evidencia lo relevante que resulta la intervención del regulador, ya que ante nuevas situaciones que evidentemente perjudican al usuario, las empresas son renuentes a adoptar medidas que solucionen el problema, debido a que no existe una norma que los obligue. Esta afirmación resulta complementaria al segundo argumento que plantean, ya que podrían aplicar (y aplican) ciertas recomendaciones, siempre y cuando las recomendaciones planteadas no les genere cambios en el procedimiento que ya han establecido para efectuar las contrataciones, toda vez que limitan su responsabilidad a cumplir con los lineamientos ya establecidos sin ser solidarios con la problemática que los abonados vienen atravesando con estas nuevas modalidades de actos delictivos.

Esta argumentación de las empresas operadoras la presentan principalmente ante las recomendaciones que proponen aplicar controles o filtros en el procedimiento de contratación. En cambio, respecto a las recomendaciones que son vinculadas a brindar capacitación a sus asesores o información a los usuarios, las empresas operadoras cuentan con otra actitud, indicando en la mayoría de los casos que se han implementado (o ya estaban implementadas). Sin embargo, estas son recomendaciones que tienen un impacto menor para mitigar la problemática que los usuarios presentan. Asimismo, estas recomendaciones son las más difíciles de verificar posteriormente por el regulador.

En ese sentido, esta situación no hace más que evidenciar que una de las principales causas de la permanencia del problema es la escasa predisposición que tienen las empresas operadoras para implementar voluntariamente recomendaciones que podrían atender de manera efectiva problemáticas que van presentándose en el mercado.

Cuadro N° 13
MEDIDAS DE SEGURIDAD PROPUESTAS POR EL OSIPTEL PARA PREVENIR EL FRAUDE EN LA CONTRATACIÓN DE SERVICIOS

Medidas de seguridad	Telefónica.	América Móvil	Entel.	Viettel
1. Previo al trámite				
1.1. Identificar, individualizar y capacitar los canales en los cuales se llevan a cabo contrataciones, portabilidad numérica, cambios de titularidad del servicio, y reposición de la *SIM card*, incluyendo al personal específico que interviene en dichos trámites	Lo implementó.	Se encontraba implementado.	Lo implementó.	Lo implementó.
1.2. Contar con información actualizada, a través de todos los canales de atención (telefónica, presencial, entre otros), sobre los trámites de nuevas contrataciones, portabilidad numérica, cambios de titularidad y reposición de la *SIM card* de los abonados, a fin de que puedan ser consultados en línea por los asesores	Se encontraba implementado.	Se encontraba implementado.	Se encontraba implementado.	Lo implementó.
1.3. Establecer un máximo de 5 intentos de verificación biométrica por persona en el día	Lo realizará una vez que estimen el plazo de implementación.	Se está evaluando para implementarlo de manera voluntaria.	Implementado	Implementado
1.4. Atender los trámites de reposición de la *SIM card* exclusivamente en los centros de atención y puntos de venta designados para atención de usuarios en provincia, que han sido previamente reportados al OSIPTEL.	No, indica que lo aplica en *delivery*.	No, indica que lo aplica en autogestión y ATM presencial	No, indica que lo aplica en auto-activado y en app mayorista	Implementado

Medidas de seguridad	Telefónica.	América Móvil	Entel.	Viettel
1.5. Informar al público que acude a los centros de atención y puntos de venta designados para atención de usuarios en provincia y distribuidores autorizados que estos cuentan con cámaras de seguridad. Conservar dicha información por un periodo mínimo de 6 meses.	No, indica que no se encuentran legalmente permitido.	No, indica que por el volumen de información lo conservan solo unas semanas.	No, solo lo conservan 60 días	No se pronuncia sobre esta recomendación.
1.6. Contar con datos de contacto de notarías a nivel nacional, para consultas de sus asesores.	No, debido a limitaciones funcionales.	No, debido a limitaciones funcionales.	No, indican que recurren a otras verificaciones.	No se pronuncia sobre esta recomendación.
2. Durante el trámite				
2.1. Ante solicitudes de contratación de un nuevo servicio, portabilidad numérica, cambio de titularidad, reposición de la *SIM card* por representación, adicional a la presentación de carta poder con firma legalizada ante notario público, debe validarse la identidad del apoderado mediante verificación biométrica de huella dactilar, y proceder con el trámite solo en caso el resultado sea exitoso, según la información que proporcione la RENIEC. Conservar dicha verificación biométrica conforme al plazo establecido en el TUO de las Condiciones de Uso respecto de la información del abonado.	No, indica que lo realizará según normativa	Lo implementó voluntariamente.	Se encontraba implementado.	No se pronuncia sobre esta recomendación.
2.2. Consultar la autenticidad del poder presentado con la notaría respectiva.	Ídem a 1.6	Ídem a 1.6	Parcialmente, lo realiza según el caso reportado.	No se pronuncia sobre esta recomendación.

Medidas de seguridad	Telefónica.	América Móvil	Entel.	Viettel
2.3. Previo a la captura de la huella dactilar, el asesor debe verificar que la mano del abonado o apoderado se encuentre libre de cualquier elemento externo. Ante la negativa de la persona suspender el trámite, informando el motivo.	No, indica que es complejo.	Parcialmente, lo implementará sin suspender la atención.	Parcialmente, lo implementará sin suspender la atención.	No se pronuncia sobre esta recomendación.
2.4. En todos los casos, requerir la exhibición del documento de identidad y verificar la coincidencia de rasgos de la fotografía incluida en dicho documento con la persona que exhibe el documento de identidad. Dicho requerimiento, debe realizarse inclusive en los casos que se efectúe la verificación biométrica de huella dactilar, según lo previsto en la normativa vigente. Ante la negativa de la persona de exhibir su documento de identidad o falta de coincidencia de principales rasgos suspender el trámite, informando el motivo.	No, indican que no es factible.	No, indican que no es factible.	No indican si lo implementarán, solo que realizan la captura de la imagen del DNI.	No, indican que al contar con el 100% de canales con la detección de la “huella viva”, se encuentran exentas a solicitar DNI.
2.5. Ante solicitudes de contratación de un nuevo servicio, portabilidad numérica, cambio de titularidad, reposición de la *SIM card*, previo a su ejecución, debe remitirse un mensaje de texto a todos los servicios móviles bajo titularidad del abonado y correo electrónico registrado por el abonado en los sistemas de la empresa operadora, informando sobre el trámite, con detalle de fecha y hora de la solicitud, lugar de presentación de la solicitud, y datos de contacto de la empresa operadora para que el abonado pueda informar si desconoce dichos intentos y solicite el bloqueo inmediato de ese tipo de trámites por un periodo de tiempo, de considerarlo necesario.	No, requiere viabilidad técnica para implementarlo.	No, requiere evaluar el impacto para implementarlo.	Evaluará la posibilidad de implementarlo en sus sistemas comerciales	No se pronuncia sobre esta recomendación.

OSIPTEL DAPU H.GUSUKUMA
OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU M.GONZALEZ

Medidas de seguridad	Telefónica.	América Móvil	Entel.	Viettel
2.6. Ante solicitudes de contratación de un nuevo servicio, portabilidad numérica, cambio de titularidad, reposición de la *SIM card* rechazadas o no atendidas, por intentos fallidos de verificación biométrica de huella dactilar, informar de ello al abonado mediante mensaje de texto a todos sus servicios móviles bajo su titularidad y a través del correo electrónico registrado.	No, requiere viabilidad técnica para implementarlo.	No, requiere evaluar el impacto para implementarlo.	Evaluará la posibilidad de implementarlo en sus sistemas comerciales	No se pronuncia sobre esta recomendación.
3. Posterior al trámite				
3.1. Si el abonado se comunica consultando por la falta o inoperatividad de su servicio o *SIM card*, el asesor de la empresa operadora, a través de cualquier canal de atención, debe verificar en línea la información actualizada del servicio a fin de identificar si existe una suspensión del servicio, baja del servicio, cambio de titularidad, portabilidad numérica o reposición de la *SIM card*, e informar de ello al usuario, con detalle de fecha, hora, lugar y/o medios de presentación de la solicitud.	Indican que adecuarán sus procesos para implementarlo	Solo a solicitud del usuario	No indican si lo implementarán, indican que lo reforzarán con su personal	No se pronuncia sobre esta recomendación.
3.2. En caso el abonado desconozca la realización de una nueva contratación de un servicio y/o reposición de la *SIM card,* el asesor -a través de cualquier canal de atención- debe brindar al abonado la opción de suspender de manera inmediata el servicio, informando que con ello terceros dejarán de tener activo el servicio.	Indican que adecuarán sus procesos para implementarlo	No, indica que es inviable	No indican si lo implementarán, indican que lo reforzarán con su personal	No se pronuncia sobre esta recomendación.
3.3. Asimismo, el asesor comercial debe informar lo siguiente: • Respecto del desconocimiento de una nueva contratación del servicio público móvil: (…). • Con relación al desconocimiento de cambio de titularidad: (…). • Respecto del desconocimiento de la reposición de la *SIM card*, (…).	Se encontraba implementado.	Lo implementó.	Lo implementó.	Se encontraba implementado.

OSIPTEL DAPU H.GUSUKUMA
OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU M.GONZALEZ

Medidas de seguridad	Telefónica.	América Móvil	Entel.	Viettel
3.4. Proporcionar al abonado que desconoce los trámites antes mencionados: copia del mecanismo de contratación y/o solicitud correspondiente al trámite cuestionado; y, copia del detalle de llamadas y envío de mensajes de texto, entrantes y salientes, con indicación del código IMEI, correspondiente al periodo que el abonado desconoce que el servicio se encontró bajo su uso. Ello, de forma adicional a las constancias respectivas, según el procedimiento de reclamo y cuestionamiento de titularidad. Dichos documentos deben contar con sello de la empresa a fin de que el abonado pueda emplearlos en la vía judicial.	Parcialmente, ya que requiere ciertas validaciones y la entrega sería de manera posterior.	No, indican que no resulta viable.	No, indican que está evaluando la posibilidad de remitir el detalle de llamadas vinculado al IMEI	No se pronuncia sobre esta recomendación.

Elaboración: OSIPTEL.

Como se mencionó previamente, el artículo 11-D del TUO de las Condiciones de Uso, se emite mediante la Resolución N° 056-2015-CD/OSIPTEL, publicada el 5 de junio del 2015, como parte de la modificación que se realizó a dicha norma, con la finalidad de abordar la problemática de la falta de seguridad en la contratación de los servicios públicos de telecomunicaciones, en línea con lo señalado en el Decreto Supremo N° 023-2014-MTC.

Cabe precisar que, mediante la Resolución N° 056-2015-CD/OSIPTEL se modificó el TUO de las Condiciones de Uso incorporando el artículo 11-D, que requiere que la comercialización del servicio público móvil por parte de los distribuidores autorizados se realice a través de puntos de venta habilitados por la empresa operadora y ubicados en una dirección específica.

Al respecto, es de considerar que entre el año 2017 y 2020 se impusieron 21 multas a las empresas operadoras móviles por no seguir el procedimiento de contratación establecido, de conformidad con lo establecido en el TUO de las Condiciones de Uso.

Cuadro N° 14
MULTAS IMPUESTAS POR INCUMPLIMIENTO DE LAS NORMAS DE CONTRATACIÓN EN EL SERVICIO PÚBLICO MÓVIL

Año en que quedó firme	Cantidad de Multas	Suma de Multas impuestas en UIT	Suma de Multas en (Soles)
Total 2017	**1**	**151**	**611 550**
Viettel	1	151	611 550
Total 2018	**6**	**1004**	**4 164 525**
Entel	3	565	2 342 675
Viettel	3	439	1 821 850
Total 2019	**6**	**1257**	**5 278 560**
América Móvil	2	471	1 977 360
Entel	2	302	1 268 400
Telefónica	2	484	2 032 800
Total 2020	**8**	**1178**	**5 064 540**
América Móvil	3	453	1 947 900
Entel	3	423	1 818 040
Telefónica	1	151	649 300
Viettel	1	151	649 300
Total general	**21**	**3589**	**15 119 175**

Fuente: Resoluciones publicadas en la página web del OSIPTEL.
Elaboración: OSIPTEL.

A pesar de las medidas sancionadoras impuestas por el OSIPTEL, descritas en los párrafos precedentes, se observó que las empresas operadoras continúan incumpliendo con los mecanismos de contratación y realizan de manera incorrecta la verificación biométrica, entre otros aspectos.

Los datos presentados confirman que la falta de incentivos de las empresas operadoras por mejorar, de manera voluntaria, sus procesos de verificación y autenticación en los procesos de contratación o activación de servicios es una de las causas de la incidencia de contrataciones no solicitadas y de cuestionamientos de titularidad de líneas prepago.

Asimismo, se debe señalar que las multas impuestas solo se calculan respecto al beneficio obtenido o costo evitado por parte de las empresas infractoras, y no en relación al daño generado a los usuarios. En ese sentido, el monto acumulado de S/ 15 millones en multas es un monto mínimo de la afectación generada a la sociedad por la negligencia de comercializar las líneas móviles en condiciones no seguras.

Por otra parte, el OSIPTEL fiscalizó durante los años 2019 y 2020 la comercialización de los servicios públicos por parte de la empresa operadora, y como resultado de las acciones de supervisión realizadas, se iniciaron 24 Procedimientos Administrativos Sancionadores (PAS) y se emitieron 12 Medidas Cautelares, a fin de disuadir a las empresas operadoras Telefónica, América Móvil, Entel y Viettel para que cesen la contratación de servicios en puntos de venta no reportados al OSIPTEL, esto es, de forma ambulante en la vía pública.

En tales procedimientos se verificó que la contratación se llevaba a cabo en la vía pública y que en dicho escenario no se brindaba información clara, veraz, detallada y precisa sobre el servicio contratado, en temas relevantes para el usuario como la velocidad de navegación por Internet o el procedimiento de baja del servicio contratado bajo la modalidad prepago.

Asimismo, los distribuidores que se encontraban en la vía pública, realizando la contratación del servicio de forma ambulatoria, se negaron a identificarse ante el supervisor del OSIPTEL y a suscribir las actas respectivas.

Si bien dicha situación no afecta la validez del acta de supervisión, este tipo de situaciones podría dificultar que el supervisor identifique adecuadamente a qué empresa operadora corresponde el distribuidor que realiza la comercialización ambulatoria del servicio público móvil, obstaculizando las supervisiones inopinadas que realiza este Organismo para verificar el cabal cumplimiento de la normativa vigente.

En el anexo N° 3, se muestra el detalle de los expedientes de fiscalización, procedimientos sancionadores y medidas cautelares, iniciados en el contexto antes señalado.

En ese sentido, se advierte la necesidad de implementar las siguientes medidas a fin de obtener una mejor trazabilidad de la contratación del servicio y que no se obstaculice la función fiscalizadora del OSIPTEL:

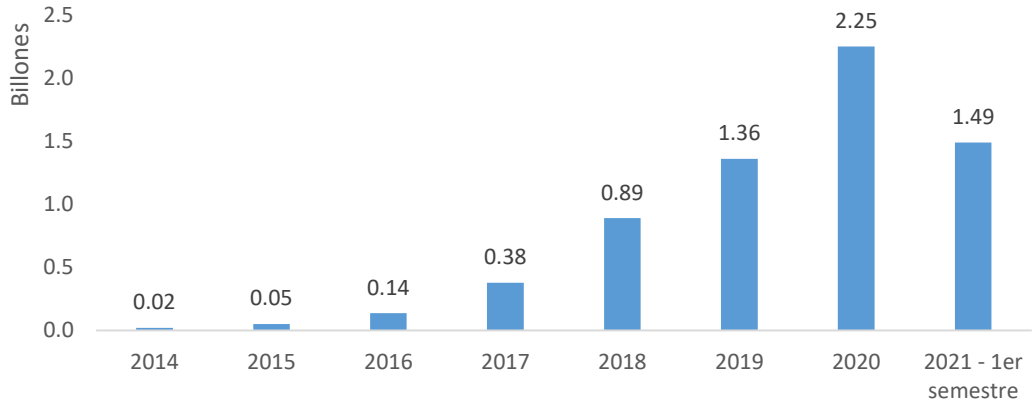
- **Identificación plena de quien participa en la contratación:** A través de un código de la persona natural que participa en la contratación (vendedor) que sea único para cada vendedor y distinto al código del distribuidor y al del punto de venta, a fin de saber exactamente quién realizó la venta de la línea. Si este código se incluye en el proceso de comercialización del SIM Card, facilitaría la verificación de quién realizó la venta, al momento de solicitar el *log* de la transacción a la empresa, constatándose que era una persona autorizada.
- **Información georeferenciada del punto de venta:** Con la finalidad de identificar plenamente los lugares en los cuales se realiza contratación del servicio y el personal de fiscalización del Osiptel pueda programar sus supervisiones inopinadas

c) Información sensible en los equipos terminales móviles

En la actualidad, el uso cotidiano e intensivo del servicio público móvil se refleja en la creciente cantidad de líneas en servicio, mayor tiempo de uso diario del internet móvil y mayor volumen de información compartida a través de los aplicativos que se encuentran en los *smartphones*.

En efecto, este servicio ha logrado pasar de ser concebido solo para realizar llamadas, a utilizarse actualmente para compartir archivos multimedia, ver videos en *streaming*, realizar reuniones de trabajo, efectuar todo tipo de comercio electrónico, realizar transacciones bancarias y una variedad de utilidades que brindan actualmente las aplicaciones móviles. Evidencia de la intensidad del uso de este servicio, es la evolución que ha tenido el tráfico de internet móvil en los últimos años, la misma que cuenta con una tendencia exponencial, tal como se puede apreciar en el gráfico N° 13.

Gráfico N° 13
EVOLUCIÓN DEL TRÁFICO DE DATOS DE INTERNET MÓVIL
(Billones de MB)

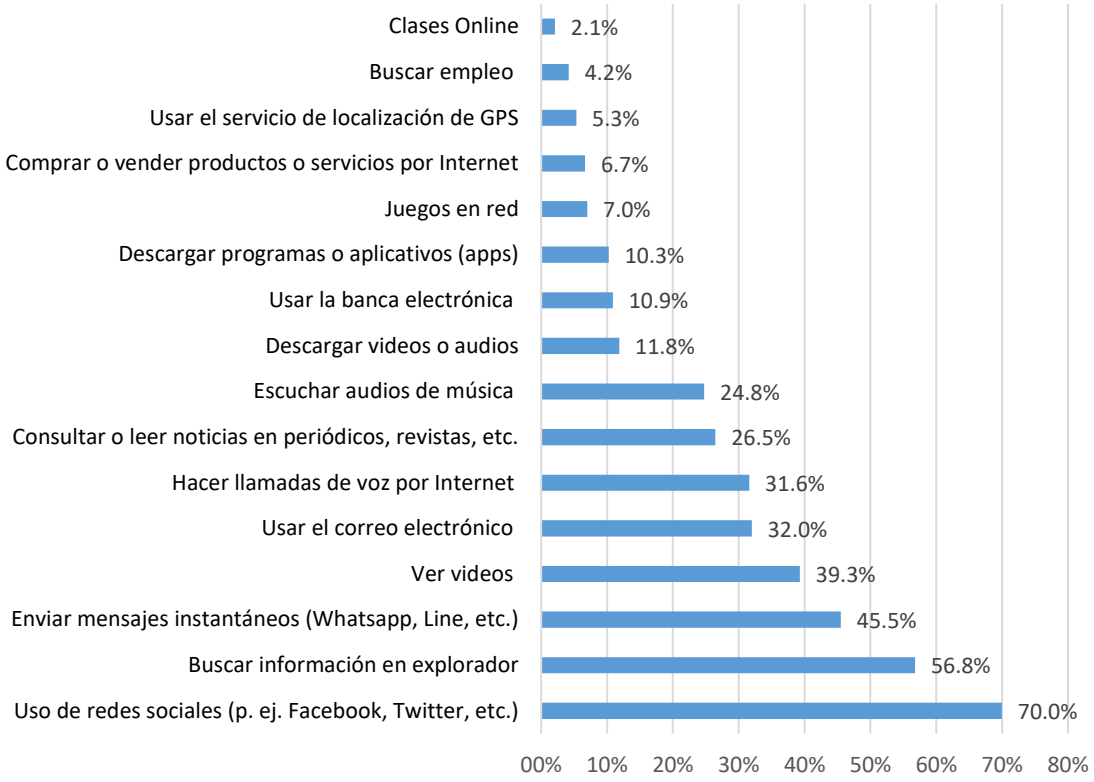


Fuente: Punku.
Elaboración: OSIPTEL.

Ahora bien, una práctica común en el uso de las funcionalidades que brinda el acceso a internet móvil a través de los aplicativos móviles, es que hoy en día, la mayoría de estas requieren el inicio de sesión o autentificación de un usuario, con la finalidad de brindarle una experiencia más personalizada en función de sus gustos y preferencias. Es decir, ahora este uso intensivo del servicio de internet significa también mantener la sesión de datos personales iniciada por todo el tiempo que se utiliza cualquiera de las distintas funcionalidades.

Asimismo, para lograr mayor experiencia de uso y acceso a otras funcionalidades, algunos servicios permiten realizar compras por internet, en el cual el usuario debe tener una cuenta bancaria autorizada para ello. En efecto, las funcionalidades que hoy en día usan los usuarios son diversas, pero casi todas tienen en común que (i) requieren contar con una sesión de usuario iniciada y (ii) permiten realizar compras digitales por internet. Tal es así que hoy en día, el equipo terminal móvil puede tener registrada información sensible del usuario de datos personales o de tarjetas de crédito, tanto en aplicativos especializados de banca móvil como en otros aplicativos que no necesariamente se tratan de este rubro, como, por ejemplo, la red social *Facebook*.

Gráfico N° 14
PORCENTAJE DEL TIPO DE USO DEL SERVICIO DE INTERNET MÓVIL



Nota: Se les solicitó a los usuarios que usan el servicio de internet a través de una conexión móvil, cuáles de todas estas funcionalidades usa.
Fuente: ERESTEL 2019
Elaboración: OSIPTEL.

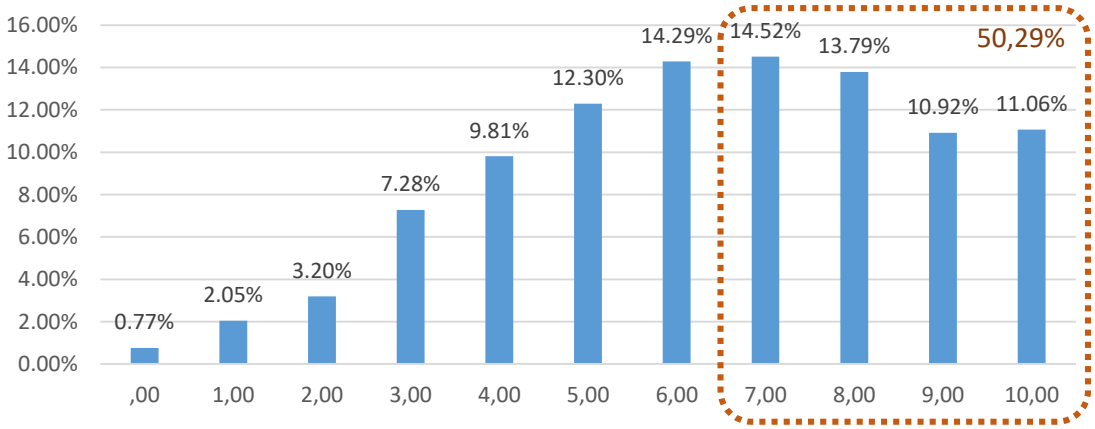
En efecto, de los principales tipos de uso que el usuario realiza a través de una conexión de internet móvil durante el 2019, se podría apreciar que, bajo ciertas circunstancias, cada una de ellas puede requerir datos personales o de tarjetas de crédito. Es decir, en todos los tipos de uso del servicio se requiere compartir información que resulta sensible. Ahora bien, esta situación podría haberse intensificado, ya que producto del estado de emergencia que inició el año 2020, las actividades realizadas a través de medios digitales han incrementado.

Sin embargo, este desarrollo tecnológico y uso de medios digitales que tienen como principal finalidad brindarle una mayor satisfacción al usuario, puede resultar riesgoso debido a la existencia de personas inescrupulosas que aprovechan la disponibilidad de esta información en los equipos terminales móviles para poder realizar actos delictivos, como el de suplantar la identidad del usuario para poder utilizar sus cuentas bancarias, acto conocido como el fraude bancario. En ese sentido, así como han incrementado todas estas funcionalidades que generan satisfacción al usuario, también lo han hecho las actividades delictivas que se pueden realizar a través y con el uso de estos dispositivos.

d) Limitado conocimiento de los usuarios sobre sus deberes y derechos

Otro aspecto a tener en cuenta, es que los usuarios de los servicios públicos de telecomunicaciones cuentan con un limitado conocimiento de sus deberes y derechos. Tal es así que en la última encuesta de satisfacción solo el 50.29% de los usuarios conocen por lo menos 7 de los 10 deberes y derechos básicos[48]. Es decir, solo la mitad de los usuarios conocen derechos que son básicos para la utilización de su servicio, que va desde la contratación hasta la baja del mismo.

Gráfico N° 15
NIVEL DE CONOCIMIENTO DE LOS USUARIOS DE LOS SERVICIOS PÚBLICOS DE TELECOMUNICACIONES SOBRE SUS DEBERES Y DERECHOS



Nota: Corresponde a la nota del nivel de conocimiento de los usuarios sobre diez de sus deberes y derechos básicos.
Fuente: Encuesta de Satisfacción 2020
Elaboración: OSIPTEL.

En ese sentido, considerando el limitado nivel de conocimiento de los usuarios respecto a temas básicos, se puede inferir que el conocimiento de aspectos relacionados a los controles de seguridad de los mecanismos de contratación (como el uso de biometría y otros aspectos), así como los posibles riesgos vinculados a la contratación en espacios públicos, es aún menor, lo que correspondería a una causa latente de permanencia del problema.

Otro aspecto característico de la conducta de los usuarios, y que probablemente explique la ocurrencia de los fraudes y las contrataciones no solicitadas, es su bajo nivel de uso de mecanismos de prevención o control. Así, por ejemplo, la herramienta “Checa tu línea”, diseñada por el OSIPTEL para que los usuarios puedan revisar periódicamente cuántas han sido contratadas a su nombre, solo tiene un uso promedio mensual de 140 187 revisiones. Considerando que en el mercado móvil hay 41.2 millones de líneas y asumiendo que cada revisión de “Checa tu línea” la realiza un usuario distinto, se obtiene que esta herramienta está siendo consultada solo por 34 usuarios por cada 10 000 líneas, lo cual es bastante poco.

En ese sentido, los usuarios suelen tener un sesgo conductual en lo que se refiere a la medición del riesgo de fraude, por lo que no suelen ser cuidadosos y precavidos. Esta situación exacerba el interés de la delincuencia por vulnerar los procesos de

[48] Se consideran derechos básicos a la obligación de la empresa operadora de entregar el contrato, la posibilidad de realizar portabilidad, la posibilidad de suspendes el servicio o de dar la baja al mismo sin cuestionamientos, entre otros.

contratación o reposición de *SIM card*, dado que conocen que existe altas probabilidad de que puedan cometer el delito sin ser descubiertos a tiempo. Por ello, es importante que se provea a los usuarios de mecanismos de alerta temprana de intentos de fraude, a fin de que puedan evitar el robo de sus cuentas bancarias.

e) Vulnerabilidad de la verificación biométrica por existencia de bandas criminales organizadas

En relación a la ocurrencia de estas contrataciones no solicitadas o la reposición fraudulenta de SIM card, es evidente que la agudización de estos problemas no se debe solo al interés de algunos comercializadores o distribuidores de líneas móviles por incrementar sus ventas; sino también al surgimiento de bandas criminales organizadas que han encontrado que las empresas operadoras de telecomunicaciones tienen vulnerabilidades en sus procesos de autenticación y verificación, por lo que han comenzado a explotarlas de manera sistemática.

En efecto, en los últimos meses se aprecia una ola de ataques a los profesores que tienen sus cuentas bancarias usualmente en el Banco de la Nación. Todos estos ataques se han ejecutado mediante el bloqueo del equipo de la víctima, la aplicación de una reposición fraudulenta de la SIM card y el posterior uso de la nueva SIM card para ingresar a las cuentas bancarias.

Particularmente, la DIRINCRI-PNP también ha remitido al OSIPTEL el Oficio N° 8341-2021-DIRINCRI PNP/DIVINDAT-DEPIDCATC, de fecha 8 de septiembre del 2021, en el cual señala que, en el registro de denuncias criminales, algunos agraviados han señalado que sus líneas telefónicas han sido bloqueadas con el fin de realizar fraude informático. Cabe señalar que las recientes investigaciones llevadas a cabo por la Policía Nacional de Perú (PNP) respecto a estos casos de fraude señalan que probablemente el personal que labora en las diferentes operadoras de telefonía móvil han facilitado sus claves de acceso a las cuentas o han permitido realizar este tipo de gestiones y otorgar los chips de manera indebida.

Asimismo, se debe señalar que estos casos de fraude no son cometidos por delincuentes que actúan de manera individual, sino que usualmente forman parte de bandas criminales organizadas. En efecto, en agosto del 2021, la Policía Nacional de Perú desbarató una organización criminal que robó al menos S/ 300 a 100 ciudadanos mediante la modalidad SIM Swapping[49]. Esta banda ha sido denominada como “Los Ciberpericos” y operaban mediante el envío de correos masivos (*phishing*) con el objetivo de obtener la identidad de las víctimas, y con esa información ingresar al Reniec y obtener el registro de la huella dactilar. Luego, imprimían la huella dactilar en alto relieve; para luego secar en una silicona, y encima de una delgada lámina se impregnaba la huella.

Con la huella dactilar clonada, los delincuentes procedían a llamar a la empresa de telefonía móvil para solicitar el bloqueo del equipo y la posterior reposición de la *SIM card*. Mediante esta modalidad, los delincuentes han logrado vulnerar el sistema de verificación biométrica, debido a que los vendedores de las empresas operadoras no se toman el trabajo de verificar si los rasgos del solicitante coinciden con la foto del DNI.

Cabe señalar que cuando los delincuentes bloquean la línea de la víctima y gestionan la reposición de una nueva SIM card, la víctima suele pensar que no hay señal, y

[49] Desbaratan banda criminal que vació las cuentas de al menos 100 personas tras bloquear el chip de sus celulares nndc | LIMA | EL COMERCIO PERÚ

asumen que el problema se resolverá en las próximas horas, sin imaginar que están siendo víctimas de un fraude.

Una vez que esta banda criminal obtenía el control sobre la línea móvil de la víctima, procedían a descargar los aplicativos de los bancos donde la víctima tiene cuentas, y a gestionar las claves de acceso, para así comenzar el robo de los ahorros de los usuarios o realizar compras masivas por internet.

Esta banda criminal, según refiere el diario El Comercio, tenía como centro de operaciones en un local del centro comercial Polvos Azules y en otro en el centro comercial El Hueco. En el operativo de Polvos Azules se incautaron 101 envoltorios de papel con anotaciones de número de DNI, huellas dactilares de silicona, 40 chips de diferentes operadoras, lectores de huellas, 3 *modems* y 5 celulares; mientras que en El Hueco detuvieron a un individuo que se encargaba de elaborar huellas dactilares de silicona, se decomisó un quemador de sellos y una máquina artesanal para fabricar huellas de polímero. En las investigaciones se determinó que habían adquirido 25 *chip* a nombre de un ingeniero, y las utilizaban para extorsionar.

Como se ha indicado previamente, los fraudes se vienen realizando por vulnerabilidades ocurridas en el ámbito de las empresas de telecomunicaciones, y vulnerabilidades del lado de las empresas de servicios bancarios o financieros. En este informe estamos abordando lo que los aspectos que están bajo la responsabilidad de las empresas de telecomunicaciones; no obstante, se es consciente que se necesita medidas adicionales que se adopten del lado del sector financiero. Por ello, el OSIPTEL ha remitido la carta C.185-PD/2021[50], mediante la cual se solicita a la Presidencia del Consejo de Ministros lidere las coordinaciones con las distintas entidades públicas (como el Ministerio del Interior, el Ministerio Público, el RENIEC, la Defensoría del Pueblo, la Superintendencia de Banca, Seguros y AFP, y el Banco de la Nación) y organizaciones representativas del sector privado como ASBANC y AFIN, que se encuentran involucradas con dicha problemática.

6.5. Permanencia del problema en caso de no intervención

Considerando que uno de los principales factores que influyen en la ocurrencia de contrataciones no solicitadas es la modalidad de venta en la vía pública, resulta necesario que se mejoren las condiciones de seguridad o se establezcan restricciones. En cualquier caso, si el OSIPTEL no adopta medidas para garantizar a los usuarios que sus solicitudes de contratación serán evaluadas con adecuados protocolos de seguridad, es probable que los casos de contratación no solicitada se incrementen de manera exponencial.

Al respecto, cuando la delincuencia encuentra brechas de seguridad, por ejemplo, una calle no vigilada o un deficiente proceso de identificación de visitas; intensifica el uso de esos descuidos para maximizar su beneficio ilícito. En los casos más graves de contratación no solicita o reposición fraudulenta de la *SIM card*, los ejecutores de las estafas no son aficionados, sino bandas u organizaciones delictivas que actúan a nivel internacional, por lo que ellos no van cesar sus ataques, si el Estado y el regulador no toman medidas apropiadas.

Usualmente, las empresas operadoras minimizan la importancia de estos problemas, debido a que, en el momento inicial, los casos suelen ser pocos. Ello se debe a un enfoque reactivo y no proactivo, que busca actuar solo cuando el problema ha escalado

[50] De fecha 30 de noviembre de 2021.

a un nivel en el cual, se empieza a convertir en un problema social, tal y como sucedió con el robo de celulares. Cuando se llega a un escenario de este tipo, lo que suele suceder es que se cuestiona la actuación del regulador y de las empresas operadoras.

En general, adicionalmente a la afectación económica a los usuarios afectados, el no atender este tipo de problemas conlleva un riesgo a la reputación del mercado, las empresas operadoras y el regulador; y podría motivar decisiones inmediatistas, sin un sustento técnico y con rango de ley. En cambio, cuando el regulador atiende de manera oportuna estos problemas, se logra fortalecer la institucionalidad del mercado de las telecomunicaciones.

7. OBJETIVO DE LA INTERVENCIÓN Y BASE DE LEGAL

7.1. Objetivo de la intervención

Reducir el riesgo de los usuarios de ser víctimas de estafas mediante la contratación o activación no solicitada de servicios, la presentación fraudulenta de una reposición de la *SIM card* o el cambio de titularidad, u otra solicitud.

7.2. Objetivos específicos

- Reducir la probabilidad de que las empresas operadoras aprueben solicitudes de trámites (contratación, activación, reposición, cambio de titularidad, etc.) presentadas sin el consentimiento de los usuarios o abonados, mediante falsos representantes o verificaciones biométricas fraudulentas.
- Incrementar los niveles de comunicación entre las empresas operadora y el abonado o usuario cuando se presentan solicitudes de contratación, reposición de *SIM car*d o cambio de titularidad, con el objetivo de lograr una identificación temprana de intentos de fraude.
- Promover que la contratación, activación y reposición de la *SIM card* se realice en canales de comercialización que garanticen a los usuarios niveles adecuados de seguridad frente a los intentos de robo de datos personales.

7.3. Base legal

La base legal para la intervención del OSIPTEL respecto de la problemática analizada está dada por los siguientes artículos:

- Artículo 3 de la Ley N° 27332 - Ley Marco de los Organismos Reguladores de la Inversión Privada en Servicios Públicos – modificada por las Leyes Nº 27631 y Nº 28337, el cual establece que el OSIPTEL tiene asignada, entre otras, la función normativa, que comprende la facultad de dictar, en el ámbito y en materia de sus respectivas competencias, los reglamentos, normas que regulen los procedimientos a su cargo, otras de carácter general y mandatos u otras normas de carácter particular referidas a intereses, obligaciones o derechos de las entidades o actividades supervisadas o de sus usuarios, así como la facultad de tipificar las infracciones por incumplimiento de obligaciones.
- Artículo 18 del Reglamento General del OSIPTEL, aprobado por Decreto Supremo N° 008-2001-PCM y modificatorias, este Organismo tiene la facultad de regular y normar el comportamiento de las empresas operadoras en sus relaciones con los usuarios.

- Artículo 24 del Reglamento General, el Consejo Directivo del OSIPTEL es el órgano competente para ejercer de manera exclusiva la función normativa y conforme al inciso b) del artículo 75 del citado Reglamento dispone que es función del Consejo Directivo del OSIPTEL, el expedir normas y resoluciones de carácter general o particular, en materia de su competencia.
- Artículo 120 del TUO de las Condiciones de Uso, la empresa operadora tiene la obligación de suministrar al abonado y al OSIPTEL, cuando le sea requerido, la información que acredite la solicitud y/o aceptación de los actos señalados en el artículo 117, incluye la contratación del servicio, migración de planes tarifarios y baja del servicio.

A continuación, se plantean los argumentos que sustentan la legalidad y razonabilidad de la intervención del OSIPTEL en lo que se refiere a las medidas de seguridad para la contratación de servicios, cambio de titularidad y reposición de *SIM card*.

7.4. Legalidad de la intervención

Para el referido análisis, es pertinente considerar el marco normativo que contempla las facultades y atribuciones conferidas por ley al OSIPTEL tanto para emitir normas de carácter general, como la facultad para imponer sanciones y medidas cautelares; así como aquellas disposiciones que regulan la contratación de servicios públicos móviles.

En ese sentido, se tiene que mediante el Decreto Legislativo N° 702[51], cuyo texto y modificatorias fueron recopilados en el Texto Único Ordenado de la Ley de Telecomunicaciones, aprobado mediante el Decreto Supremo N° 013-93-TCC (en adelante, Ley de Telecomunicaciones), se creó al OSIPTEL, atribuyéndole el rol de regular el comportamiento de las empresas operadoras de servicios públicos de telecomunicaciones, a través de resoluciones expedidas por su Consejo Directivo, conforme a lo siguiente:

> ***Artículo 76.-*** *La Comisión Reguladora de Tarifas de Comunicaciones será sustituida por el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL), que se encargará de regular el comportamiento de las empresas operadoras, así como las relaciones de dichas empresas entre sí, de garantizar la calidad y eficiencias del servicio brindado al usuario y de regular el equilibrio de las tarifas.*
>
> ***Artículo 77.-*** *El poder regulatorio que esta Ley concede a OSIPTEL en relación a materias de su competencia será ejercido a través de resoluciones expedidas por su Consejo Directivo. (Subrayado agregado)"*

Posteriormente, la Ley N° 27332, Ley Marco de Organismos Reguladores de Servicios Públicos, así como su modificatoria, sistematizó las diversas funciones de los organismos reguladores; estableciendo respecto de las funciones normativa, supervisora y fiscalizadora, lo siguiente:

> ***"Artículo 3.- Funciones***
>
> *3.1 Dentro de sus respectivos ámbitos de competencia, los Organismos Reguladores ejercen las siguientes funciones:*
>
> *(…)*

[51] Que aprobó las Normas que regulan la Promoción de Inversión Privada en Telecomunicaciones.

a) Función supervisora: *comprende la facultad de verificar el cumplimiento de las obligaciones legales, contractuales o técnicas por parte de las entidades o actividades supervisadas, así como la facultad de verificar el cumplimiento de cualquier mandato o resolución emitida por el Organismo Regulador o de cualquier otra obligación que se encuentre a cargo de la entidad o actividad supervisada; (…)*

c) Función Normativa: *comprende la facultad de dictar en el ámbito y en materia de sus respectivas competencias, los reglamentos, normas que regulen los procedimientos a su cargo, otras de carácter general y mandatos u otras normas de carácter particular referidas a intereses, obligaciones o derechos de las entidades o actividades supervisadas o de sus usuarios;*

d) Función fiscalizadora y sancionadora: *comprende la facultad de imponer sanciones dentro de su ámbito de competencia por el incumplimiento de obligaciones derivadas de normas legales o técnicas, así como las obligaciones contraídas por los concesionarios en los respectivos contratos de concesión; (…)".*

Más recientemente, la Ley N° 29158, Ley Orgánica del Poder Ejecutivo estableció las siguientes reglas, respecto de los organismos reguladores:

*"**Artículo 32.- Organismos Reguladores***

Los Organismos Reguladores:

1. *Se crean para actuar en ámbitos especializados de regulación de mercados o para garantizar el adecuado funcionamiento de mercados no regulados, asegurando cobertura de atención en todo el territorio nacional.*

   (…)

3. *Dentro de sus respectivos ámbitos de competencia, tienen funciones supervisoras, reguladoras, normativas, fiscalizadoras y sancionadoras; y de solución de controversias y reclamos, en los términos previstos por la Ley de la materia.*

   (…)

7. *Defienden el interés de los usuarios con arreglo a la Constitución Política del Perú y la ley.*

(…)".

De lo anterior, se desprende que este Organismo Regulador se encuentra facultado para dictar de manera exclusiva y dentro del ámbito de su competencia, reglamentos y normas de carácter general, aplicables a todos los administrados que se encuentren en las mismas condiciones. Asimismo, se indica que tales reglamentos pueden definir los derechos y obligaciones entre las empresas operadoras y de estas con los usuarios.

De la misma manera, se faculta al OSIPTEL a supervisar y fiscalizar el cumplimiento de las disposiciones normativas en el marco de su competencia; así como a sancionar el incumplimiento de las mismas por parte de los agentes del mercado, de ser el caso.

De otro lado, con relación a las disposiciones aplicables a la contratación de servicios públicos móviles, es de considerar que, a través de los Decretos Supremos N° 022-

2014-MTC[52] y N° 023-2014-MTC[53], se establecieron obligaciones a las empresas operadoras, respecto a la contratación de los servicios públicos móviles, con la finalidad de prevenir conductas que puedan afectar la normal prestación de los referidos servicios, cautelar el derecho de los usuarios y salvaguardar la seguridad ciudadana. Asimismo, se facultó al OSIPTEL a realizar la adecuación de las normas necesarias a las disposiciones establecidas en dichos Decretos.

> *"**Tercera. - Adecuación de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones***
>
> *El OSIPTEL adecuará el Texto Único Ordenado de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, aprobado por Resolución de Consejo Directivo N° 138-2012-CD/OSIPTEL, a las disposiciones contenidas en la presente norma, en un plazo no mayor a la entrada en vigencia del presente Decreto Supremo".*

Por otro lado, el 6 de enero de 2017, en el diario oficial El Peruano, se publicó el Decreto Legislativo N° 1338, Decreto Legislativo que crea el Registro Nacional de Equipos Terminales Móviles para la seguridad, orientado a la prevención y combate del comercio ilegal de equipos terminales móviles y al fortalecimiento de la seguridad ciudadana.

Conforme se establece en su artículo 1, la finalidad del referido Decreto Legislativo es el fortalecimiento de la seguridad ciudadana garantizando la contratación de los servicios públicos móviles de telecomunicaciones[54]. En esa línea de fortalecimiento de la seguridad ciudadana, el Decreto Legislativo N° 1338 establece obligaciones a las empresas operadoras de servicios públicos móviles referidas a la contratación de los referidos servicios, tal como la obligación verificar plenamente la identidad de quien contrata el servicio público móvil de telecomunicaciones[55].

Adicionalmente a ello, el Decreto Legislativo N° 1338 como su Reglamento establecen que el OSIPTEL puede establecer las normas complementarias que resulten necesarias para la implementación de las disposiciones, tal como se indica a continuación:

[52] Decreto Supremo que modifica el Decreto Supremo N° 023-2007 -MTC que aprueba el Reglamento de la Ley N° 28774, Ley que crea el Registro Nacional de Terminales de Telefonía Celular, establece prohibiciones y sanciones.

[53] Decreto Supremo que modifica el Decreto Supremo No 024-2010-MTC que aprueba el procedimiento para la subsanación de la información consignada en el Registro de Abonados Pre Pago.

[54] *"**Artículo 1. Objeto y finalidad***

1.1 El presente decreto legislativo tiene por objeto la creación del Registro Nacional de Equipos Terminales Móviles para la Seguridad – RENTESEG, con la finalidad de prevenir y combatir el hurto, robo y comercio ilegal de equipos terminales móviles, dentro del marco del fortalecimiento de la seguridad ciudadana; garantizando la contratación de los servicios públicos móviles de telecomunicaciones. (…)

[55] *"**Artículo 8. Empresas operadoras de servicios públicos móviles de telecomunicaciones***

8.1 Las empresas operadoras de servicios públicos móviles de telecomunicaciones tienen las siguientes obligaciones:

a) Verificar plenamente la identidad de quien contrata el servicio de servicios públicos móviles de telecomunicaciones mediante el sistema de verificación biométrica de huella dactilar. Las excepciones a dicha verificación son establecidas en el reglamento del presente decreto legislativo. (…)"

Decreto Legislativo N° 1338	**QUINTA. Normativa complementaria** El OSIPTEL, el Ministerio del Interior y la Policía Nacional del Perú, en el marco de sus competencias, dictan las normas complementarias que resulten necesarias para la implementación de las disposiciones establecidas en el presente decreto legislativo y su reglamento.
Decreto Supremo N° 009-2017-IN (derogado)	**Artículo 30.- Obligaciones de las empresas operadoras** Son obligaciones de las empresas operadoras: (…) o) Otras obligaciones que establezca el presente Reglamento y la normativa complementaria aprobada por el OSIPTEL.
Decreto Supremo N° 007-2019-IN (vigente)	**Artículo 32.- Obligaciones de las empresas operadoras** Son obligaciones de las empresas operadoras: (…) o) Otras obligaciones que establezca el presente Reglamento y la normativa complementaria aprobada por el OSIPTEL.

Precisamente, a través del Decreto Legislativo N° 1338 se faculta al OSIPTEL a establecer la normativa necesaria que coadyuve al cumplimiento de la finalidad de la seguridad ciudadana relacionada a la contratación del servicio público móvil.

En suma, considerando el marco normativo antes citado, es posible inferir que el OSIPTEL se encuentra facultado a solicitar el cumplimiento de las obligaciones vigentes que aseguren que la contratación de los servicios públicos móviles garantice el fortalecimiento de la seguridad ciudadana, así como a establecer la regulación aplicable a las contrataciones de servicios públicos, que coadyuve al cumplimiento de la referida finalidad.

Ahora, considerando que la empresa operadora es responsable de todo el proceso de contratación del servicio, y siendo este un servicio público regulado, es viable que el OSIPTEL establezca disposiciones que delimiten los canales de contratación y establezca reglas mínimas respecto de ellos, a fin de identificarlos adecuadamente y se brinde mayor seguridad en el proceso de validación de identidad del usuario, entrega de información del servicio y contratación del mismo.

7.5. Razonabilidad de la intervención

Frente a la problemática evidenciada, se han evaluado las medidas regulatorias necesarias a la luz del principio de razonabilidad, para lo cual ha sido imprescindible identificar las aristas y causas subyacentes que estarían involucradas.

Asimismo, en tanto que las medidas propuestas podrían implicar ciertas restricciones para las empresas operadoras, generando un posible conflicto entre el interés privado de dichas empresas y el interés público de los consumidores y la administración, se ha otorgado prevalencia a este último.

Con relación a la prevalencia del interés público, resulta pertinente considerar que, uno de los pronunciamientos del Tribunal Constitucional Peruano advierte lo siguiente[56]:

> "*El interés público tiene que ver con aquello que beneficia a todos; por ende, es sinónimo y equivalente al interés general de la comunidad. Su satisfacción constituye uno de los fines del Estado y justifica la existencia de la organización administrativa. La administración estatal, constituida por órganos jerárquicamente ordenados, asume el cumplimiento de los fines del Estado teniendo en cuenta la*

[56] Fundamento N° 4 de la Sentencia expedida el 05 de Julio del 2004 en el EXP. Nº 0090-2004-AA/TC

pronta y eficaz satisfacción del interés público. El interés se expresa confluyentemente como el valor que una cosa posee en sí misma y como la consecuencia de la inclinación colectiva hacia algo que resulta atractivo, apreciable y útil. De allí que Fernando Sainz Moreno ["Reducción de la discrecionalidad: el interés público como concepto jurídico", Revista española de Derecho Administrativo, disco compacto, Madrid, Civitas Ediciones, Revista N.º 008, enero - marzo de 1976] plantee que la noción interés público se entienda como expresiones del valor público que en sí mismo tienen ciertas cosas; o bien como expresión de aquello que únicamente interesa al público (…) En ese aspecto, Emilio Fernández Vásquez ("Diccionario de derecho público". Buenos Aires: Astrea, 1981) enfatiza que "El Estado no puede tener más que intereses públicos"; razón por la cual éste está comprendido en un régimen de Derecho Público."

En la misma línea, uno de los pronunciamientos de nuestro Tribunal Constitucional[57] señala que:

1. "El interés público, es típicamente un concepto indeterminado. Es decir, se trata de un concepto que hace referencia a una esfera de la realidad cuyos límites no aparecen precisados en su enunciado, pero que sin embargo podrá ser concretizado en cada caso en atención a las circunstancias. Así, no se trata de un concepto librado enteramente a la discrecionalidad de la Administración, pues ello supondría en muchos casos justificar la arbitrariedad, sino que se trata de un concepto cuyo contenido deberá ser explicitado en cada caso en atención a circunstancias concretas (…)."

Asimismo, el autor español Nicolás López Calera señala que:

"El interés público es un concepto y un valor recurrente en la legislación, en la jurisprudencia y en las acciones de gobierno en todos los niveles, un concepto y valor del que se echa mano para resolver conflictos o para justificar actuaciones de especial entidad en la vida jurídica y política (…). El concepto de interés se debe relacionar con el deseo fuerte de algo que se reconoce como especialmente necesario y valioso (…). No obstante, la práctica humana pone de relieve que puede haber intereses enormemente "valiosos", esto es, intereses que no se reducen a una unívoca o inmediata atracción hacia algo o a una satisfacción del propio yo, como también hay valores que, por su fuerza atractiva inmediata para una voluntad individual o colectiva, podrían calificarse como "intereses". En todo caso, cuando se trata de intereses, estamos refiriéndonos a cosas, a situaciones sociales, a relaciones sociales que engendran un deseo fuerte, una necesidad fuerte e incluso una pasión. (….) En suma, cuando los intereses son compartidos por unos amplios sectores de una colectividad, cuando los intereses tienen contenidos que la mayoría social considera necesidades primarias, prioritarias o fundamentales, se puede hablar de un interés público. El interés público se refiere a intereses que se consideran muy necesarios e importantes para la supervivencia o el bienestar de la sociedad como tal. El interés público es un fin fundamental de todo ordenamiento jurídico, porque dar a la sociedad "lo suyo" es un precepto de justicia elemental"[58].

Como se puede advertir, el interés público es el motor de la actividad de la Administración Publica, una categoría jurídica que incide no solo en el actuar de la

[57] Fundamento N° 7 de la Sentencia expedida el 10 de Octubre del 2006 en el EXP. Nº 2488-2004-AA/TC
[58] López Calera, Nicolás. El Interés Público: entre la ideología y el Derecho. "Revista Anales de la Cátedra Francisco Suarez N° 44", 2010. p. 123-129.

Administración, sino también en la esfera privada del administrado toda vez que es bien conocido que el interés privado siempre cederá frente al interés público; este último se constituye como un límite a aquel.

Respecto de los mencionados intereses públicos que el OSIPTEL estaría protegiendo con las medidas propuestas, se debe señalar que el artículo 65 de la Constitución Política del Perú establece que el Estado defiende el interés de los consumidores y usuarios; velando particularmente por la salud y la seguridad de la población. Asimismo, el artículo IV del Título Preliminar del Código de Protección y Defensa del Consumidor – Ley Nº 29571, establece que es el Estado quien protege la salud y seguridad de los consumidores a través de una normativa adecuada, promoviendo el establecimiento de normas reglamentarias para la producción y comercialización de productos y servicios. En ese sentido, si bien las empresas operadoras cuentan con las libertades de empresa e iniciativa privada, de acuerdo a los artículos 58 y 59 de la Constitución Política del Perú, estas no tienen un carácter absoluto, dado que deben ser ejercidas en respeto al orden público.

> ***Articulo 58.- Economía Social de Mercado***
>
> *La iniciativa privada es libre. Se ejerce en una economía social de mercado. Bajo este régimen, el Estado orienta el desarrollo del país, y actúa principalmente en las áreas de promoción de empleo, salud, educación, seguridad, servicios públicos e infraestructura.*
>
> ***Articulo 59.- Rol Económico del Estado***
>
> *El Estado estimula la creación de riqueza y garantiza la libertad de trabajo y la libertad de empresa, comercio e industria. El ejercicio de estas libertades no debe ser lesivo a la moral, ni a la salud, ni a la seguridad pública. El Estado brinda oportunidades de superación a los sectores que sufren cualquier desigualdad; en tal sentido, promueve las pequeñas empresas en todas sus modalidades*.

Por otro lado, el Texto Único Ordenado de la Ley de Telecomunicaciones, aprobado mediante el Decreto Supremo Nº 013-93-TCC, establece a los servicios de telefonía móvil como servicios públicos, por lo que, se debe cautelar que dichos servicios sean prestados por las empresas operadoras de manera eficiente y respetando los derechos de los usuarios, siendo el ente encargado de velar dicho comportamiento, el OSIPTEL. En efecto, el Reglamento General del OSIPTEL, señala que uno de los objetivos específicos de este Organismo es la de establecer políticas adecuadas de protección de los usuarios de los servicios públicos de telecomunicaciones, y que tiene competencia en las actividades que involucran la prestación de los servicios públicos de telecomunicaciones; encontrándose facultada a ejercer la función normativa, entre otros, respecto del tema de la contratación del servicio.

> **Reglamento General del OSIPTEL**
>
> ***Artículo 19.- Objetivos específicos del OSIPTEL***
>
> *Dentro del marco del objetivo general, son objetivos específicos del OSIPTEL:*
>
> *(…)*
>
> *f) Establecer políticas adecuadas de protección para los usuarios, y velar por el acceso a los servicios con tarifas razonables.*

Artículo 20.- Competencia del OSIPTEL

El OSIPTEL ejerce las funciones precisadas en el presente Reglamento sobre las actividades que involucran la prestación de los servicios públicos de telecomunicaciones. La inclusión de una actividad dentro de la competencia del OSIPTEL no implica necesariamente la existencia de regulación sobre dicha actividad.

Artículo 25.- Reglamentos que pueden dictarse en ejercicio de la función normativa

En ejercicio de la función normativa puede dictarse reglamentos o disposiciones de carácter general referidos a los siguientes asuntos: (…) i) Condiciones de acceso a servicios y redes e interconexión entre los mismos, incluyendo la oportunidad, la continuidad y en general los términos y condiciones de contratación, pudiendo excepcionalmente aprobar los formatos de contratos, de ser ello necesario. (…)

En ese sentido, es de mencionar que la protección de los referidos intereses públicos, impactan en otros bienes jurídicos tutelados como el de seguridad ciudadana. Sobre el particular, es de considerar que la seguridad ciudadana es un bien jurídico que el Estado busca cautelar desde diferentes ámbitos. Por tal motivo, a través del Decreto Legislativo N° 1338 se creó el Registro Nacional de Equipos Terminales Móviles para la Seguridad - RENTESEG, con la finalidad de prevenir y combatir el hurto, robo y comercio ilegal de equipos terminales móviles, dentro del marco del fortalecimiento de la seguridad ciudadana; así como a fin de garantizar la contratación de los servicios públicos de telecomunicaciones.

La implementación y administración de este Registro, así como la expedición de las normas complementarias que resulten necesarias para el adecuado cumplimiento de su finalidad se encuentran a cargo del OSIPTEL. Además, dicho cuerpo normativo, entre otras obligaciones referidas a la implementación del referido Registro, establece la obligación de la empresa de telefonía móvil de verificar la identidad de la persona que contrata este servicio, mediante el uso del sistema de identificación biométrico por huella dactilar.

Asimismo, de acuerdo a lo establecido en el artículo 37 del Reglamento del Decreto Legislativo N° 1338 (aprobado por Decreto Supremo N° 007-2019-IN), las empresas operadoras son responsables de todo el proceso de contratación del servicio público móvil que provean y se establece expresamente la prohibición de comercializar chips, SIM cards y cualquier otro dispositivo similar con el servicio activado antes de registrar los datos de identificación del abonado en el registro de abonados[59].

[59] Cabe mencionar que, dicha obligación ya se encontraba prevista desde el año 2010 en el Decreto Supremo Nº 024-2010-MTC, el cual en su artículo indicaba lo siguiente: Artículo 9°.- Responsabilidad de las empresas operadoras en la contratación del servicio Las empresas operadoras serán responsables de todo el proceso de contratación de un servicio público de telecomunicaciones. Para tal efecto se entenderá que las modalidades de contratación incluyen la venta de chips, tarjetas *SIM Card* y cualquier otro similar destinado a la adquisición del servicio. (…) Del mismo modo, se mencionó en el Decreto Supremo N° 023-2014-MTC que modificó el referido artículo. Artículo 9°.- Responsabilidad de las empresas operadoras en la contratación del servicio Las empresas operadoras son responsables de todo el proceso de contratación de los servicios públicos de telecomunicaciones que provean, que comprende la identificación y el registro de los abonados que contratan sus servicios. (…) Las empresas operadoras se encuentran prohibidas de comercializar chips, *SIM Card* y cualquier otro dispositivo similar con el servicio activado antes de registrar los datos de identificación del abonado en sus Registros Privados de Abonado."

*"**Artículo 37.- Responsabilidad en el proceso de contratación***

37.1. Las empresas operadoras son responsables de todo el proceso de contratación del servicio público móvil que provean, que comprende la identificación y el registro de los abonados que contratan sus servicios. (…)

37.4. Las empresas operadoras se encuentran prohibidas de comercializar chips, SIM cards y cualquier otro dispositivo similar con el servicio activado antes de registrar los datos de identificación del abonado en el registro de abonados."

Bajo este contexto normativo, se desprende que el OSIPTEL tiene una función tuitiva con relación a los derechos de los usuarios y abonados del servicio público de telecomunicaciones, a efectos de resguardar que sus contrataciones se enmarquen en un ámbito de seguridad. Asimismo, dicha función tuitiva se extiende para aquellas transacciones y/o solicitudes que involucren la prestación del servicio público.

Negar dicho aspecto, implicaría serias repercusiones en la esfera de los abonados y usuarios, pues considerando que el TUO del Reglamento de la Ley de Telecomunicaciones establece que el titular del servicio es responsable por el uso que se haga del mismo[60], cualquier tipo de responsabilidad que se desprenda de su uso le podría ser atribuido.

8. ANÁLISIS DE LAS ALTERNATIVAS DISPONIBLES

8.1. Descripción de las alternativas disponibles

De conformidad con lo expuesto previamente, se han identificado dos alternativas para abordar el problema de las solicitudes de baja y migración.

- Alternativa 1: Mantener el esquema regulatorio vigente.
- Alternativa 2: Reglas de seguridad adicionales para la identificación temprana de intentos de fraude por canal de comercialización.

A continuación, se describe y evalúa cada una de las alternativas formuladas.

a) Alternativa N° 1: Mantener el esquema regulatorio vigente

Descripción

Las principales características del actual esquema regulatorio son:

(i) Verificación biométrica de la huella dactilar: Consiste en verificar la correspondencia de la impresión dactilar con la base de datos biométrica del RENIEC.

- Es obligatoria para la contratación del servicio público móvil.
- Conservar y almacenar el reporte de verificación por 10 años, e incluir esta información en el registro de abonados.
- Remitir SMS a todas las líneas del abonado, señalando el número de documento de identidad, número del servicio contratado, modalidad de contratación, derecho de reclamo o cuestionamiento.

[60] "Artículo 15.- Responsabilidad del abonado
El abonado titular de un servicio público de telecomunicaciones, es responsable del uso que se haga del mismo.

(ii) Reposición de la *SIM card*:

- La reposición solo se puede solicitar por sustracción, perdida, extravío, fallas o nuevo modelo.
- Se presenta de manera personal en oficinas, centros de atención y puntos de venta.
- Se debe realizar la verificación biométrica, y conservar la copia de la verificación.
- Cuando lo solicita un representante, se debe presentar un poder.
- La empresa puede habilitar otros mecanismos presenciales si se realice la verificación biométrica o la activación con contraseña única.

(iii) Registro de distribuidores autorizados:

- Se debe otorgar un código único de distribuidor.
- Validación previa del código de distribuidor en cada contratación.
- Remitir el registro de los distribuidores autorizados, precisando código y dirección de puntos de venta.

Ventajas

a. Las empresas ya se han adecuado a estas obligaciones, y han desarrollado los protocolos para cumplir con ellos.

b. Se han desarrollado actividades para que los usuarios conozcan cómo realizar estos trámites, cambiar las reglas podría requerir implementar una nueva campaña de información.

c. De alguna manera, las reglas vigentes han logrado reducir la incidencia de reclamos por contratación no solicitada; no obstante, existen nuevos problemas que no estarían siendo atendidos.

Desventajas

a. No brinda medidas adecuadas para evitar que el usuario se entere a tiempo de que desconocidos están intentado realizar trámites con sus líneas.

b. No plantea un enfoque colaborativo con las víctimas de fraudes, dado que no hay la obligación de remitir la información de las contrataciones no solicitadas, reposiciones fraudulentas, etc.

c. Las reglas para realizar trámites mediante un representante son vulnerables, debido a que se puede realizar con una simple carta y mostrando el recibo de pago.

d. Las reglas para verificación biométrica no contemplan la existencia de la adulteración o clonación de líneas.

e. Las reglas son susceptibles de perder su validez, dado que constantemente surgen nuevas amenazas al proceso de verificación biométrica.

f. El actual esquema no ha precisado las reglas de validación para las contrataciones en las ferias itinerantes y la auto-activación.

g. Los trámites realizados mediante representante son susceptibles de suplantación, dado que solo se exige presentar una carta simple y el último recibo.

b) Alternativa N° 2: Reglas de seguridad adicionales para la identificación temprana de intentos de fraude por canal de comercialización.

Descripción

Esta propuesta consiste en añadir reglas adicionales de seguridad para garantizar a los usuarios y abonados que no se ejecutarán fraudes mediante la suplantación en la contratación, cambio de titularidad y reposición de la *SIM card*. El objetivo de estas reglas es lograr que a los usuarios se les advierta, de manera preventiva, cada vez que se inician solicitudes de contratación, activación, cambio de titularidad o reposición de la *SIM card*; y sin en caso, se hubiese aprobada alguna de estas solicitudes, la empresa debería informar al usuario previo a cualquier trámite posterior.

Asimismo, considerando los diferentes canales de atención, se propone definir reglas que permitan identificar a los distribuidores y al personal encargado de tramitar las contrataciones, así como determinar medidas de seguridad para que la correcta identificación de los usuarios en el canal presencial, telefónico, *web*, auto-activación y ferias itinerantes.

(i) Reglas para la identificación temprana de solicitudes aprobadas sin el consentimiento del abonado o usuario:

- Obligación de informar al abonado sobre las solicitudes y trámites aprobados.
- Informar si la falta de operatividad se debe a la ejecución de una solicitud.
- La empresa debe suspender el servicio de manera inmediata cuando se presente un reclamo por desconocimiento de contratación o reposición a través del canal telefónico o el presencial, y en un día en los otros canales.
- Para la reactivación del servicio se requiere una resolución firme o que hubiera causado estado en el caso de reclamos por contratación no solicitada, y mediante una nueva reposición en el caso de desconocimiento de reposición.
- Obligación de proporcionar información en el caso de desconocimiento o cuestionamiento de la contratación, la portabilidad, el cambio de titularidad o reposición de la *SIM card*. La información de la fecha y hora de la solicitud o contratación se debe presentar inmediatamente, mientras que la copia del mecanismo de contratación o la solicitud se debe presentar como máximo en 5 días hábiles, con el sello o distintivo de la empresa para ser usado en la vía judicial.

(ii) Reglas para la identificación temprana de intentos de reposición fraudulenta de *SIM card*:

- En el caso de las reposiciones de la *SIM card*, se debe aplicar las siguientes reglas:
  - Prepago: se debe validar los nombres y apellidos, número de documento de identidad y tener al menos una respuesta válida

OSIPTEL DAPU H.GUSUKUMA

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU M.GONZALEZ

sobre la fecha de la última recarga o el monto de la última recarga.

- Postpago: se debe validar los nombres y apellidos, número de documento de identidad y tener al menos dos respuestas válidas sobre la fecha de vencimiento del recibo, monto del plan tarifario, o dirección de la facturación.

- Para tal efecto, la empresa debe registrar y conservar las constancias de las preguntas realizadas y las respuestas obtenidas de dicha validación.
- En el caso de las reposiciones de la *SIM card*, se debe enviar un SMS, locución y correo electrónico en el momento de presentada la solicitud, y a las 2 horas luego del primer envío.

  El mensaje debe incluir fecha y hora de la solicitud, lugar de presentación y datos de contacto de la empresa.

  Para validar el eventual bloqueo se debe aplicar las siguientes reglas:

  - Prepago: se debe validar los nombres y apellidos, número de documento de identidad y tener al menos una respuesta válida sobre la fecha de la última recarga o el monto de la última recarga.
  - Postpago: se debe validar los nombres y apellidos, número de documento de identidad y tener al menos dos respuestas válidas sobre la fecha de vencimiento del recibo, monto del plan tarifario, o dirección de la facturación.
- En el caso de una reposición con representante, además de presentar el poder, se debe realizar la verificación biométrica y exhibir el documento de identidad.
- La activación del SIM se realizará a las 4 horas de presentada la solicitud.
- En los casos en los que la solicitud es denegada por intentos fallidos en la verificación biométrica, la empresa tiene la obligación de enviar SMS, correo electrónico y locuciones.

(iii) Reglas para garantizar la seguridad de los abonados en los canales de comercialización:

- La contratación del servicio se realiza en los centros de atención, en la dirección específica del punto de venta, previamente reportado al OSIPTEL, mediante el canal telefónico, de forma virtual o en la dirección indicada por el solicitante y excepcionalmente en ferias itinerantes.
- En el caso de los distribuidores, solo se puede contratar con aquellos que se encuentran autorizados por la empresa y reportados al OSIPTEL, y en el punto de venta con dirección específica.
- La empresa tiene la obligación de otorgar un código único de identificación al distribuidor, punto de venta y al personal.
- Los puntos de venta pueden ser gestionados por la empresa operadora o distribuidor autorizado.

- La persona natural que interviene en cada contratación del servicio, sea el personal del centro de atención o punto de venta, el distribuidor autorizado o su personal u otro, valida su identidad mediante verificación biométrica de huella dactilar o con el uso de una contraseña, previo a la contratación.
- En el registro de distribuidores se debe incluir: nombre y apellidos del distribuidor, tipo y número de documento de identidad, código único del distribuidor, código único de cada punto de venta, fecha de inicio de cada punto de venta, dirección específica de cada punto de venta (distrito, provincia, departamento y georeferenciado), y datos del personal del distribuidor (nombres, apellidos, tipo y número de documento de identidad y código único de identificación. Adicionalmente, se debe incluir en dicho registro los puntos de gestionados sin distribuidor.

  La empresa debe comunicar al OSIPTEL cualquier modificación en el referido registro.

  La empresa debe establecer supuestos de suspensión temporal y cese definitivo de distribuidores por tener contrataciones no solicitadas.
- Las ferias itinerantes solo se realizan en centros poblados rurales sin oficinas, centros de atención o puntos de venta, o en otras ferias itinerantes autorizadas previamente por el OSIPTEL en los que la empresa cuente con cobertura y la autorización municipal. Se debe avisar con 10 días hábiles de anticipación, las fechas y lugares donde se llevará a cabo.
- La empresa debe tener identificado al personal dedicado a la entrega a domicilio. La *SIM card* es entregado de manera personal y en la dirección indicada por el solicitante. Se solicita brindando la información indicada en el artículo 11 y la dirección de entrega. La *SIM card* se entrega de manera personal en la dirección indicada con la exhibición del documento de identidad y la captura de la imagen del mismo.
- La empresa debe tener el registro de los establecimientos que venden SIM card para auto-activación, con el nombre comercial, razón social, dirección específica, código de identificación. La empresa debe comunicar este registro el último día hábil de cada mes.

  Solo se puede realizar una sola activación o portabilidad numérica en el mes.
- En el caso del mecanismo de auto-activación, la empresa operadora como mecanismo de seguridad realiza de manera aleatoria dos (2) de cualquiera de las siguientes preguntas de validación: a) nombre del padre, b) nombre de la madre, c) lugar de nacimiento, y/o d) fecha de nacimiento. Para una validación exitosa se requiere que se brinde el número del documento de identidad y la fecha correcta de su emisión, así como que ambas preguntas de validación sean contestadas de forma correcta.
- La contratación del servicio público móvil se puede realizar mediante el canal telefónico usando la contraseña única.
- La empresa debe tener identificado y registrado en canal o medio a través del cual se contrató el servicio y el distribuidor o personal que participó en la contratación, así como el medio por el cual validó la identidad del abonado y se adquirió la *SIM card*.

- La empresa operadora tiene la carga de la prueba de la validación de identidad exitosa de la persona natural que interviene en la contratación de cada uno de sus servicios.

(iv) Reglas de seguridad para los trámites con representantes:

- Un representante ya no podrá ser acreditado con carta simple, copia de DNI y recibo de pago, dado que será obligatorio tener un poder legalizado por notario.
- El representante debe realizar la verificación biométrica para todo servicio y trámite.

(v) Reglas de seguridad para la verificación biométrica de la huella dactilar:

- Se limita a un máximo de 5 intentos por transacción.
- Previo a la captura de la huella dactilar, la empresa operadora debe verificar que la mano del solicitante del servicio o representante se encuentre libre de cualquier elemento externo.
- Además del SMS, se debe enviar una locución, correo electrónico y mensaje de texto.
- Mediante el uso de la contraseña única se sustituye la verificación biométrica de la identidad para la realización de trámites, salvo para nuevas contrataciones de servicios principales, cambio de titularidad y reposición de SIM Card.
- Para la contratación de nuevos servicios principales, cambio de titularidad y reposición de SIM Card de aquellos abonados que cuentan con contraseña única, de manera adicional a las validaciones de identidad previstas en los artículos 11, 11-A y 67-B, se requiere proporcione su contraseña única de forma exitosa.

Ventajas

a. Incrementa la capacidad de los usuarios y las empresas para detectar, de manera oportuna, los intentos de suplantación en la contratación, activación, cambio de titularidad o reposición.

b. Brinda a los usuarios la oportunidad de conocer si algún impostor ha realizado trámites con su línea, y si la falta de servicio se debe a una solicitud de reposición.

c. Permite que los usuarios puedan actuar rápidamente para evitar un robo mediante la suspensión de la línea por reporte de una contratación no solicitada o una reposición fraudulenta.

d. Determina reglas de información para que los distribuidores y el personal encargado de las contrataciones puedan estar registrados de una manera que permita la trazabilidad de los trámites, y se pueda identificar a los responsables de las negligencias.

e. Habilita el canal de auto-activación, ferias itinerantes y canal telefónico para las contrataciones, pero establece reglas para brindar una mayor seguridad en la contratación del servicio y la reposición de la *SIM card*.

f. Reduce la probabilidad de que se presenten falsos representantes y realicen trámites sin el consentimiento del usuario o abonado.

Desventajas

a. En el caso de las reposiciones de la *SIM card*, los usuarios que tienen una gran urgencia en este trámite podrían verse afectados dado que la activación de la línea se dará a las 4 horas de presentada la solicitud.

b. Los usuarios que requieran realizar un trámite con un representante tiene que asumir el costo notarial de legalizar el poder.

c. Podrían darse casos especiales en los que el usuario requiera hacer más de 5 intentos en la verificación, pero ya no lo va poder efectuar.

d. La contratación en ferias itinerantes se limita a los centros poblados rurales sin oficinas, centros de atención o puntos de venta o en otras ferias itinerantes autorizadas previamente por el OSIPTEL.

8.2. Análisis de alternativas

El método más apropiado para la evaluación de propuestas de políticas públicas es el análisis Costo-Beneficio, mediante el cual se puede medir de manera cuantitativa los beneficios monetizados de la propuesta regulatoria, y contrastarlos con los costos que enfrentarían las empresas operadoras y los usuarios. Un resultado del ratio Beneficio-Costo incrementalmente superior a la alternativa de base, confirmaría que la propuesta regulatoria va contribuir con mejorar los niveles de bienestar en la sociedad, y por tanto justificaría su adopción.

El Análisis Multicriterio es una evaluación que podría ser complementaria o sustituta del Análisis Costo-Beneficio. Es complementaria cuando se busca identificar otros tipos costos y beneficios no monetarios que permitan confirmar que la medida regulatoria será beneficiosa para la sociedad. En cambio, es sustituta cuando los beneficios y costos directos no son cuantificables, no se pueden calcular de manera exhaustiva o no resultan significativos. En estos casos, resulta más práctico para el evaluador concentrarse en los aspectos cualitativos de la propuesta normativa.

En el caso de la presente propuesta normativa, se tiene un cálculo del beneficio de la norma a partir del estimado de la reducción de pérdida económica que podrían experimentar los usuarios; no obstante, este monto solo sería una aproximación muy baja de todos los beneficios de la norma, dado que no se está considerando el monto de pérdida que sufren los usuarios por otros tipos de contrataciones no solicitadas.

Asimismo, en el caso de los costos, como se verá con más detalle en las siguientes secciones, ninguno de los componentes de esta propuesta regulatoria implica para las empresas operadoras grandes costos de desarrollo informático, dado que consisten en proveer a los usuarios y al OSIPTEL de un tipo de información que, en principio, toda empresa responsable debería tener disponible. Las propuestas de mejora en las reglas para una verificación segura de la identidad de los usuarios y el personal son aspectos que generan costos marginales no significativos; dado que la principal inversión, que es la verificación biométrica, ya se ha realizado previamente.

En atención a lo anterior, se considera que no sería un ejercicio práctico estimar costos de adecuación muy específicos a cada empresa operadora, sobre todo porque en realidad, todo lo que se está exigiendo a las empresas son aspectos que ya deberían tener si fueran eficientes y socialmente responsables.

Por otra parte, se debe señalar que existen un conjunto de problemas regulatorios denominados riesgos, en los que se identifican eventos potencialmente dañinos, pero que tienen una probabilidad ocurrencia y una probabilidad de daño. La ocurrencia de estos riesgos tiene un impacto en la sociedad, que en muchos casos obliga a las entidades públicas a actuar de manera tardía, cuando ya se desató la crisis. Es decir, muchas veces las entidades públicas no actúan de manera preventiva, debido a un análisis Costo-Beneficio inmediatista; y solo terminan adoptando decisiones cuando la crisis estalla.

El análisis regulatorio de los riesgos es un marco metodológico promovido por la OECD que está orientado a evaluar las políticas públicas en función de los riesgos, y que tiene por objetivo incorporar en la evaluación económica el costo de oportunidad de prevenir un riesgo. En efecto, analizar este costo implica advertir las potenciales consecuencias de un riesgo emergente, y determinar a partir de ello, cuál el nivel más adecuado de regulación.

En el caso de contrataciones no solicitadas, las reposiciones de SIM card y los cambios de titularidad no solicitados, se puede apreciar que son eventos que tienen una probabilidad de ocurrencia. Las personas que terminan siendo víctimas de estos fraudes sigue siendo una minoría respecto al total de personas que han realizado esos trámites, pero en general, todos tienen una probabilidad de ser víctimas de estos fraudes.

Asimismo, en relación a la gravedad del daño, no todas las víctimas han sido afectadas de la misma manera. Hay casos, probablemente de los que no reportan o denuncian, donde la afectación es pequeña; mientras que hay casos en los que afectación ha tenido una magnitud que ha obligado a las víctimas a denunciar.

Un enfoque de evaluación que no considere la existen de estos riesgos, y no lo incorpore en el análisis; podría incurrir en minimizar el impacto de las medidas regulatorias; dado que solo estaría considerando los casos o las denuncias reportadas; cuando en realidad, es probable que el riesgo pueda incrementarse en la medida que los atacantes perciban que las autoridades no imponen medidas preventivas.

En efecto, cuando el regulador emite disposiciones orientadas a la prevención de riesgos, el análisis más apropiado para la evaluación económica de las medidas adoptadas es el enfoque regulatorio basado en riesgos. En el caso de la alternativa 2 que se va evaluar en esta sección, estas contienen medidas orientadas a prevenir la ocurrencia de riesgos y amenazas en los procesos de verificación y autenticación de identidad en los procesos de contratación de servicio, reposición de *SIM card* y cambio de titularidad, por lo que lo más recomendable es realizar un análisis de riesgos.

Cabe señalar que, según la OECD (2010)[61], en enfoque de regulación basado en riesgos está redefiniendo varias temáticas regulatorias anteriormente solo evaluados bajo un enfoque Costo-Beneficio. Por ejemplo, la regulación de la salud pública y del medio ambiente, ahora está siendo entendida como regulación de riesgos de salud y del medio ambientales; de manera similar, la regulación financiera, ahora se está entendiendo como una regulación de riesgos de mercado.

Este nuevo paradigma tiene 2 implicancias prácticas, la primera es definir el riesgo que se quiere o pretende abordar; la segunda es verificar que ese riesgo exista y si debería ser regulado. Este enfoque permite que la regulación sea más precisa y circunscrita,

[61] Op. Cit., pg 51.

dado que ya no se pretenderá proteger el medio ambiente, sino reducir los riesgos medioambientales. En el caso de la Alternativa 2, la propuesta regulatoria no pretende regular los procesos de contratación, reposición y cambio de titularidad, sino que busca regular los riesgos existentes en esos procesos. Es decir, las decisiones que se adopten están orientados a mitigar estos riesgos. Por ello, en el análisis multicriterio que se va realizar, el análisis de riesgo va ser el principal criterio en la evaluación.

a) Definición formal de análisis multicriterio

Un análisis multicriterio (AMC) permite identificar la mejor alternativa a partir de evaluación de criterios (o atributos). La influencia de cada criterio en la evaluación final o global se realiza asignando ponderadores o pesos que reflejan su importancia para los agentes de mercado. Cabe señalar que los criterios son las características respecto de las cuales se calificará a las alternativas disponibles, y los ponderadores son los pesos o importancia relativa que se le otorgará a cada atributo.

Una vez definidos los criterios (atributos) y las ponderaciones se procede a calificar a las alternativas en cada uno de estos criterios con un puntaje ordinal.

Posteriormente se realiza la suma ponderada de calificaciones y se obtiene un total para cada alternativa, siendo la alternativa elegida la de mayor puntaje ponderado. La suma ponderada se representa matemáticamente de la siguiente manera:

$$MAX\ [Si\ =\ w_1 s_{i1} + =\ w_2 s_{i2}\ + w_3 s_{i3}\ + \cdots +\ w_n s_{in} = \sum w_j s_{ij}\ n_j = 1\ ] \qquad (1)$$

Donde w_1,…., w_n representan las ponderaciones para cada criterio (atributo) y s_{i1},….., s_{in}, representan las calificaciones (puntajes) otorgadas, a la alternativa i, en cada uno de los criterios (atributos), desde el criterio 1 hasta el criterio n.

b) Supuestos del Análisis Multicriterio (AMC)

<u>Criterios de evaluación</u>

Para esta propuesta normativa se propone la evaluación de los siguientes criterios o atributos:

- **Criterio 1: Facilidad de implementación**

Considerando que no se disponen de los costos específicos que asumirían las empresas operadoras en cada una de las reglas adicionales propuestas en la Alternativa 2, se ha visto pertinente evaluar este criterio a través de una matriz en la cual cada componente de la propuesta tiene de una calificación respecto al grado de dificultad en su implementación, según los siguientes criterios:

OSIPTEL DAPU H.GUSUKUMA

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU M.GONZALEZ

Cuadro N° 15
CRITERIOS PARA EVALUAR EL ATRIBUTO DE COSTOS

Criterio	Calificación	Valor
"Solo es una precisión de lo que ya existía en la norma"	Ninguna	0
"Solo se debe remitir información que ya dispone en sus bases de datos"	Muy baja	1
"Debe remitir información a través de SMS, locución y correos, o realizar verificaciones adicionales"	Baja	2
"Requiere modificar sus bases de datos y sistemas de registros ya existentes"	Mediana	3
"Requiere hacer inversiones adicionales en su infraestructura de información"	Alta	4
"Requiere hacer inversiones adicionales en su infraestructura de información y crear un nueva área de gestión"	Muy alta	5

Elaboración: OSIPTEL.

- **Criterio 2: Nivel de afectación a los usuarios**

Para la calificación de este criterio se aplica la siguiente fórmula:

$$Calificación = \frac{Afectación\ inicial - Afectación\ residual}{Afectación\ inicial} \quad (2)$$

- **Criterio 3: Manejo del riesgo**

En la metodología del Análisis de Riesgo es necesario identificar cada proceso vinculado con los factores de riesgo y establecer su nivel de exposición. En el caso de las suplantaciones en los procesos de contratación, activación de línea, reposición de SIM card y cambio de titularidad, se ha procedido a identificar las características de estos trámites y las interacciones que se dan entre el usuario y la empresa operadora. Cabe señalar que para realizar este análisis, se va tomar en cuenta las recomendaciones metodológicas del ISO 31000:2009[62] y la matriz de riesgos que se usa en el ISO 27001:2013, la cual servirá para calificar el grado de exposición nivel de riesgo de los procesos que se están evaluando.

En atención a lo anterior, se va determinar el nivel de riesgo con base a 2 parámetros:

- Probabilidad de ocurrencia:

Cuadro N° 16
CALIFICACIÓN POR PROBABILIDAD DE OCURRENCIA

Probabilidad de ocurrencia	Calif.
Raro	1
Improbable	2
Posible	3
Probable	4
Casi cierto	5

[62] ISO 31000:2009. *Risk management – Principles and guidelines*, Geneva.

- Nivel de impacto individual:

Cuadro N° 17
CALIFICACIÓN POR NIVEL DE IMPACTO

Probabilidad de ocurrencia	Calif.
Muy bajo	1
Bajo	2
Moderado	3
Alto	4
Muy alto	5

La calificación global de ambos atributos se obtiene multiplicando la calificación de probabilidad de ocurrencia con la calificación de nivel de impacto. Por ello, la calificación del riesgo es una métrica que se encuentra en el intervalo de 5 a 25. En el cuadro N° 18, se puede apreciar la matriz de calificación de exposición al riesgo, donde, por ejemplo, se califica en 25 cuando el riesgo es casi cierto y su nivel de impacto es alto; mientras que se califica en 1 cuando el riesgo es raro y su impacto es muy bajo. En color verde están los escenarios de riesgo muy bajo, en amarillo los de riesgo bajo, en naranja los de riesgo moderado y en rojo los de riesgo alto.

Cuadro N° 18
MATRIZ DE CALIFICACIÓN DE EXPOSICIÓN AL RIESGO

		Nivel de impacto				
		Muy bajo	Bajo	Moderado	Alto	Muy alto
Probabilidad de incurrencia	Casi cierto	5	10	15	20	25
	Probable	4	8	12	16	20
	Posible	3	6	9	12	15
	Improbable	2	4	6	8	10
	Raro	1	2	3	4	5

Riesgo muy bajo | Riesgo bajo | Riesgo moderado | Riesgo alto

- **Criterio 4: Trazabilidad de las contrataciones**

Al respecto, la trazabilidad es la habilidad de una organización para retener la identidad del producto, su origen y uso diario (Khabbazi y otros; 2010), con el objetivo de mantener el control y supervisar los procesos de producción[63]. Para lograr la trazabilidad del proceso es necesario disponer de un sistema de control que garantice que la información sea precisa, oportuna, necesaria, fácil de usar, confiable y significativa. Según Dharmendra y otros (2015), la trazabilidad se evalúa hacia adelante (*track*), es decir dónde se encuentra y a dónde se dirige; pero también se puede evaluar hacia atrás (conocido como *trace*), es decir cómo ha sido elaborado y cómo ha sido hecho.

Considerando estas definiciones, se ha determinado que las 2 alternativas sean evaluadas en relación con su capacidad de lograr para el usuario la adecuada trazabilidad de las contrataciones, activaciones, reposiciones de SIM card y cambios de titularidad, para ello se están adoptando los siguientes criterios:

[63] Se puede consultar también la definición del ISO/9000-2005: http://www.praxiom.com/iso-definition.htm#Traceability

- Identificación del lugar del trámite
- Identificación del personal que participó de la solicitud
- Identificación del suplantador

La escala utilizada para el presente análisis será del 0 al 1, tal como se señala en el siguiente cuadro, dónde 0 representa un muy mal desempeño y 1 representa un desempeño muy bueno.

Cuadro N° 19
ESCALA DE PRESENTACIÓN DE RESULTADOS DE LAS ALTERNATIVAS

Valor	0.00 a 0.09	0.10 a 0.29	0.30 a 0.49	0.50 a 0.69	0.70 a 0.89	0.90 a 1.00
Tipo de desempeño	Muy malo	Malo	Poco malo	Un poco bueno	Bueno	Muy bueno

Elaboración: OSIPTEL

Ponderación de los atributos

En relación con los ponderadores de los atributos, se ha considerado pertinente otorgar el mayor peso al manejo del riesgo, dado que esta regulación se ha motivado principalmente por las amenazas que actualmente existen en la contratación, activación, reposición de *SIM card* y cambio de titularidad. En segundo lugar, se está asignando un peso de 20% a la reducción de la pérdida económica de los usuarios que han sufrido alguna estafa. Finalmente, se está otorgando un peso de 15% a los atributos de facilidad de implementación y trazabilidad para el usuario, ello debido a que se trata de atributos complementarios.

Cuadro N° 20
PONDERACIÓN DE LOS CRITERIOS

Criterio	Ponderación
Facilidad de implementación	15%
Reducción de la afectación de los usuarios	20%
Manejo del riesgo	50%
Trazabilidad para el usuario	15%

Elaboración: OSIPTEL.

Escala de calificación AMC

Al respecto, una vez obtenida la calificación en cada atributo, se realiza un cambio de escala mediante la siguiente fórmula:

$$I_{AMC\ i} = \frac{I_{Atributo\ i} - 0.5}{0.5} \quad (3)$$

Matriz de Componentes y acciones de la alternativa 2

La alternativa 2 se va analizar respecto a 5 tipos de controles o reglas de seguridad adicionales, cada uno de estos implican acciones que se tienen que implementar. En el cuadro N° 21 se presenta una matriz que se resume los componentes y las acciones de la propuesta normativa.

Cuadro N° 21
MATRIZ DE COMPONENTES Y ACCIONES DE LA ALTERNATIVA 2

Controles	Acciones
1. Identificación temprana de solicitudes aprobadas sin consentimiento del abonado.	1.1. Informar acerca de las solicitudes al usuario. 1.2. Suspender el servicio cuando se desconozca la contratación. 1.3. Facilitar la información de la contratación o reposición no reconocida.
2. Identificación de intentos de reposición fraudulenta	2.1. Implementar preguntas de validación de identidad. 2.2. Envío de SMS, locución y correo electrónico en 2 oportunidades. 2.3. Exhibir documento de identidad en el caso de un trámite con representante. 2.4. La activación se realizará a las 4 horas. 2.5. Enviar SMS, correo y locución en el caso de intentos fallidos.
3. Reglas en los canales de comercialización	3.1. Se puede contratar con distribuidores autorizados por la empresa y reportados al OSIPTEL, y en el punto de venta con dirección específica. 3.2. Códigos de identificación al distribuidor y personal encargado. 3.3. Antes de la contratación, el distribuidor deben pasar por la verificación biométrica o usar contraseña única. 3.4. Registro de distribuidores que permita la trazabilidad del trámite. 3.5. La empresa debe establecer supuestos de suspensión o cese de distribuidores que realizan contrataciones no solicitadas. 3.6. Las ferias itinerantes solo es para centros poblados sin oficina, centro de atención o punto de venta, o en otras ferias itinerantes autorizadas previamente por el OSIPTEL y donde la empresa disponga de cobertura. 3.7. Auto-activación: El SIM card se entrega de manera personal en la dirección indicada con la exhibición del documento de identidad y la captura de la imagen del mismo. Debe realizar al menos 2 preguntas de validación. 3.8. La empresa debe comunicar este registro el último día hábil de cada mes de los establecimientos que brindan auto-activación. 3.9. La contratación del servicio público móvil se puede realizar mediante el canal telefónico usando la contraseña única. 3.10. La empresa debe tener identificado y registrado en canal o medio a través del cual se contrató el servicio y el distribuidor o personal que participó en la contratación, así como el medio por el cual validó la identidad del abonado y se adquirió el SIM card. 3.11 La empresa tiene la carga de la prueba de la validación de la identidad exitosa de la persona natural que interviene en la contratación de cada uno de los servicios.

OSIPTEL DAPU H.GUSUKUMA
OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU M.GONZALEZ

Controles	Acciones
4. Reglas de seguridad para los trámites con representantes	4.1. Un representante ya no podrá ser acreditado con carta simple, copia de DNI y recibo de pago, dado que será obligatorio tener un poder legalizado por notario. 4.2. El representante debe realizar la verificación biométrica para todo servicio y trámite.
5. Reglas de seguridad para la verificación biométrica de la huella dactilar	5.1. Se limita a un máximo de 5 intentos por transacción. 5.2. Además del SMS, se debe enviar una locución y correo electrónico. 5.3Verificar que la mano del solicitante se encuentre libre de cualquier elemento externo. 5.4 La contraseña única no sustituye la verificación biométrica en caso de nuevas contrataciones, cambio de titularidad y reposición de *SIM card*.

Elaboración: OSIPTEL.

c) Criterio 1: Facilidad de Implementación

En relación con el criterio de facilidad de implementación, se debe señalar que la Alternativa 1 (situación inicial) no implica ningún tipo de implementación, por lo que tiene la máxima calificación (1.0). En cambio, en el caso de la Alternativa 2, las empresas operadoras tendrían que asumir ciertas acciones de implementación en cada uno de los componentes descritos previamente.

Considerando los puntajes y criterios establecidos en el cuadro N° 15, se ha realizado una evaluación de la facilidad de implementación en los 5 componentes de esta propuesta regulatoria, la cual se reporta en el cuadro N° 22. Los resultados obtenidos señalan que, en promedio, la implementación de estos componentes es de 2,6 en una escala del 1 al 5; ello debido a que ninguna de las acciones comprendidas dentro del proyecto normativo supone un cambio radical en la forma en que las empresas operadoras vienen realizando la verificación de identidad, sino que perfeccionan la forma en que actualmente se viene trabajando.

En efecto, la alternativa 2 propone, entre otras cosas, adoptar medidas de seguridad para la identificación temprana, debido a que se han reportado casos en los que los usuarios erróneamente inician una reactivación de línea, pensando que su *SIM card* se encuentra malograda; y la empresa operadora no les advierte que recientemente se ha realizado una reposición. Esta medida seguridad, por ejemplo, no debería suponer un mayor costo para las empresas operadoras, dado que ellas disponen de esa información.

Por otra parte, en relación al uso de controles biométricos para el personal de la empresa o el distribuidor, se debe señalar que estos ya no son mecanismos de control desconocidos, y dada las amenazas existentes, no se perciben como extremos, más bien como necesarios. Incluso, en otros sectores, los controles biométricos están en camino de convertirse en un estándar. En ese contexto, resulta importante incluir medidas que permitan la confiabilidad de la verificación biométrica, y disuadan la ocurrencia de clonación de huellas.

De manera similar, en el caso de las exigencias de códigos únicos para distribuidores y vendedores, y contraseña para los usuarios; todas estas medidas de seguridad no son extrañas en otros sectores (clínicas, hospitales, bancos, aseguradoras, etc.); por lo

que, en realidad, la implementación de estos mecanismos de control forma parte de la modernización del sector.

Por lo tanto, en promedio, las actividades que se llevaron a cabo para implementar la Alternativa 2 han obtenido una calificación promedio de 2,6, normalizando este valor en una escala del 0 al 1, se obtiene una calificación de 0,52, lo cual significa que los costos de implementación deberían ser de mediano a bajos. Finalmente, aplicando la fórmula (3), se obtiene una calificación para la Alternativa 2 de -0.04 en la escala del -1 al 1, como se puede apreciar en el cuadro N° 22.

Cuadro N° 22
CALIFICACIÓN DE LAS ALTERNATIVAS EN EL ATRIBUTO 1: FACILIDAD DE LA IMPLEMENTACIÓN

Alternativa	Facilidad de implementación	Calif. en AMC
Alternativa 1	1.00	1.00
Alternativa 2	0.48	-0.04

Elaboración: OSIPTEL.

Cuadro N° 23
MATRIX DE FACILIDAD EN LA IMPLEMENTACIÓN DE LA ALTERNATIVA 2

Componente	Acciones	Calificación	Valor Calif.
1. Identificación temprana de solicitudes aprobadas sin consentimiento del abonado.	1.1. Informar acerca de las solicitudes al usuario. 1.2. Suspender el servicio cuando se desconozca la contratación. 1.3. Facilitar la información de la contratación o reposición no reconocida.	**Respecto a 1.1.:** Se considera que informar sobre las solicitudes no debería significar un gran costo para las empresas operadoras, dado que es una información que ya existe en sus bases de datos. Además, si en caso esa información no estuviese debidamente organizada, esta norma va colaborar en mejorar la productividad y eficiencia de las empresas. **Respecto a 1.2.:** En realidad, para el cumplimiento de esta obligación las empresas solamente tendrían que instruir a sus asesores a cumplir con esta solicitud. **Respecto a 1.3.:** Colaborar con los usuarios en facilitar la información tampoco debería significar un gran costo para las empresas operadoras, dado que es una información que ya disponen. Solo tendrían que modificar algunos protocolos de trabajo.	2

Componente	Acciones	Calificación	Valor Calif.
2. Identificación de intentos de reposición fraudulenta	2.1. Implementar preguntas de validación de identidad. 2.2. Envío de SMS, locución y correo electrónico en 2 oportunidades. 2.3. Exhibir documento de identidad en el caso de un trámite con representante. 2.4. La activación se realizará a las 4 horas. 2.5. Enviar SMS, correo y locución en el caso de intentos fallidos.	**Respecto 2.1.:** Para el desarrollo de preguntas de validación es posible que las empresas operadoras tengan que desarrollar algún tipo de herramienta de información que proporcione a los asesores de las empresas las preguntas que tienen que hacer, y cuál es la respuesta correcta. Esta medida podría tener algún tipo de costo. No obstante, en el mercado muchas entidades, financieras principalmente, ya lo tienen, por lo que se esperaría que no habría dificultad en identificar a un proveedor de una solución. **Respecto 2.2.:** En este caso, las empresas operadoras van a tener que esperar 4 horas para la activación de la línea, implementar preguntas de validación y enviar SMS y correos cuando ocurran intentos fallidos; todo lo cual, en alguna medida, va implicar modificar sus sistemas de registro para poder añadir campos de información relacionados con estas actividades. En ese sentido, esta medida sí podría tener algún costo operativo medido por cantidad de SMS, locuciones y correos. No obstante, se debe señalar que las empresas operadoras diariamente remiten SMS, locuciones y	3

Componente	Acciones	Calificación	Valor Calif.
		correos de propaganda, por lo que ya disponen de la infraestructura para realizar estas acciones. **Respecto 2.3. y 2.5:** Exhibir el documento de identidad no genera costos a las empresas operadoras **Respecto 2.4.:** La activación en 4 horas tampoco genera costos a las empresas operadoras.	
3. Reglas en los canales de comercialización	3.1. Se puede contratar con distribuidores autorizados por la empresa y reportados al OSIPTEL, y en el punto de venta con dirección específica. 3.2. Códigos de identificación al distribuidor y personal encargado. 3.3. Antes de la contratación, el distribuidor deben pasar por la verificación biométrica o usar contraseña única. 3.4. Registro de distribuidores que permita la trazabilidad del trámite. 3.5. La empresa debe establecer supuestos de suspensión o cese de distribuidores que realizan contrataciones no solicitadas. 3.6. Las ferias itinerantes solo son para centros	**Respecto 3.1.:** No debería generar costos porque solo busca que los distribuidores estén autorizados y registrados. **Respecto 3.2., 3.4, 3.8, 3.10:** El desarrollo de códigos de identificación, bases de datos y otros aspectos sí podrían requerir del desarrollo de una solución informática. No obstante, se supone que este registro ya existe, por lo que se está hablando de una mejora. **Respecto 3.3:**	3

OSIPTEL DAPU H.GUSUKUMA
OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU M.GONZALEZ

Componente	Acciones	Calificación	Valor Calif.
	poblados sin oficina, centro de atención o punto de venta, o en otras ferias itinerantes autorizadas previamente por el OSIPTEL y donde la empresa disponga de cobertura. 3.7. Auto-activación: El SIM card se entrega de manera personal en la dirección indicada con la exhibición del documento de identidad y la captura de la imagen del mismo. Debe realizar al menos 2 preguntas de validación. 3.8. La empresa debe comunicar este registro el último día hábil de cada mes de los establecimientos que brindan auto-activación. 3.9. La contratación del servicio público móvil se puede realizar mediante el canal telefónico usando la contraseña única. 3.10. La empresa debe tener identificado y registrado en canal o medio a través del cual se contrató el servicio y el distribuidor o personal que participó en la contratación, así como el medio por el cual validó la identidad del abonado y se adquirió el SIM card. 3.11 La empresa tiene la carga de la prueba de la validación de la identidad exitosa de la persona natural que interviene en la contratación de cada uno de los servicios.	Considerando que las empresas operadoras ya tienen desarrollada la verificación biométrica, es posible que realizar la verificación de los vendedores sea un costo marginal no significativo. **Respecto 3.6. 3.7, 3.9 y 3.10:** Se trata de facilidades y reglas que se están estableciendo para que las contrataciones sean seguras en los diferentes canales.	

Componente	Acciones	Calificación	Valor Calif.
4. Reglas de seguridad para los trámites con representantes	4.1. Un representante ya no podrá ser acreditado con carta simple, copia de DNI y recibo de pago, dado que será obligatorio tener un poder legalizado por notario. 4.2. El representante debe realizar la verificación biométrica para todo servicio y trámite.	**Respecto a 4.1 y 4.2:** De manera similar que, en los casos anteriores, la mayoría de estas obligaciones son informacionales; no obstante, es posible que las empresas operadoras requieren realizar algún tipo de adecuación en sus bases de datos. Por lo tanto, este componente se califica como de mediana dificultad.	3
5. Reglas de seguridad para la verificación biométrica de la huella dactilar	5.1. Se limita a un máximo de 5 intentos por transacción. 5.2. Además del SMS, se debe enviar una locución y correo electrónico. 5.3Verificar que la mano del solicitante se encuentre libre de cualquier elemento externo. 5.4 La contraseña única no sustituye la verificación biométrica en caso de nuevas contrataciones, cambio de titularidad y reposición de *SIM card*.	**Respecto a 5.1, 5.2, 5.3 y 5.4:** En este caso, la medida no requiere cambios en las bases datos, dado que implica limitar el número de intentos, y remitir una locución y un correo electrónico; por lo que se califica este componente de bajo costos de implementación.	2

Elaboración: OSIPTEL.

d) Criterio 2: Reducción de la afectación de los usuarios

En el cuadro N° 10 se estimó la afectación que genera a los usuarios la ocurrencia de los fraudes financieros realizados mediante la suplantación en los trámites de reposición de *SIM card*, cambio de titularidad y contratación de servicios. En síntesis, se estimaron los siguientes montos:

- Para los usuarios que denuncian ante el OSIPTEL: S/ 4 218 000 en un año.
- Para los usuarios que denuncian ante las empresas: S/ 8 122 107 en un año.
- Para los usuarios que no denuncian: S/ 418 531 en un año.

De esta manera, la afectación total es S/ 12 758 639 al año.

En la Alternativa 2 se asume que la efectividad para la medida será de 90% para los casos más graves que suele presentarse ante el OSIPTEL, de 70% para los casos que se presentan ante las empresas y de 30% en los usuarios que no denuncian. Asumiendo que la pérdida promedio individual es S/ 10000 para el grupo de usuarios que denuncian ante el OSIPTEL, S/ 7000 para los que solo denuncian ante la empresa, S/ 100 para los no denuncia y S/ 600 para los usuarios que pierden el bono, se estima que la afectación residual de la Alternativa 2 es S/ 3 151 404. El detalle se reporta en el cuadro N° 24.

Cuadro N° 24
ESTIMACIÓN DE LA AFECTACIÓN RESIDUAL DE LA ALTERNATIVA 2

Tipo de fraude	Cantidad estimada de afectados al año			Afectación anual estimado (soles)			
	Ante el OSIPTEL	Solo ante las empresas	No denuncian	Ante el OSIPTEL	Solo ante las empresas	No denuncian	Total
Bonos	18	147	354	10 800	88 160	212 213	311 173
Ahorros	41	335	808	411 000	2 348 473	80 759	2 840 232
Total	59	482	1161	421 800	2 436 632	292 972	3 151 404
Efectividad	90%	70%	30%				

Elaboración: OSIPTEL.

Aplicando la fórmula (2), se obtiene para la Alternativa 2 una calificación de 0.75, que resulta de dividir S/ 9 607 235 entre S/ 12 758 639. Cabe precisar que el numerador es la resta entre la afectación inicial y la afectación residual. De otro lado, con relación a la Alternativa 1, se debe señalar que el OSIPTEL viene trabajando con las empresas operadoras soluciones voluntarias, y que precisamente, este enfoque no ha tenido resultados efectivo; por lo que al Alternativa debería calificarse con 0. Finalmente, aplicando la fórmula (3), se obtiene una calificación de -1 para la Alternativa 1 y de 0.51 para la Alternativa 2, como se puede apreciar en el cuadro N° 25.

Cuadro N° 25
CALIFICACIÓN DE LAS ALTERNATIVAS EN EL ATRIBUTO 2: REDUCCIÓN DE LA AFECTACIÓN

Alternativa	Calificación	Calif. en AMC
Alternativa 1	0	-1.00
Alternativa 2	0.75	0.51

Elaboración: OSIPTEL.

e) Criterio 3: Manejo del riesgo

En esta sección se dará un puntaje a los riesgos presentados en los trámites de contratación de alta nueva, reposición de SIM card y cambio de titularidad, el puntaje será diferente por tipo de canal de atención (presencial, telefónico o itinerante). Cabe señalar que dentro del canal ambulante (vía pública) se está incluyendo a las ferias itinerantes o ambulatorias y todo proceso de contratación que no se realice totalmente dentro del centro de atención.

De manera previa a este análisis, se ha realizado una caracterización de los riesgos, el cual se encuentra reportado en el Anexo N° 1, En este análisis se ha encontrado que los activos comprometidos son las líneas móviles de los usuarios, las amenazas más graves son las siguientes:

- Pérdida de la titularidad de la línea.
- Adquisición de una línea por parte de un desconocido.
- Pérdida temporal del control de la línea del usuario.

Por otra parte, se ha encontrado que, en los procesos de verificación de identidad para la contratación de un servicio, reposición de SIM card y cambio de titularidad, las siguientes vulnerabilidades:

- Falta de control en la tramitación con representante o apoderado.
- Uso de huellas clonadas en la verificación biométrica.
- Dificultad para verificar la identidad del asesor, sobre todo cuando la venta es de manera ambulatoria o itinerante.

Asimismo, las consecuencias que se podrían generar cuando se pierde el control de la línea o cuando se contrata una línea sin la autorización de los usuarios son las siguientes:

- La línea móvil puede ser utilizada con fines delictivos.
- El usuario puede terminar con deudas por líneas móviles que no usa y desconoce.
- Pueden usar la línea móvil para hacer trámites en nombre del usuario.
- El estafador puede ingresar a sus cuentas bancarias y robar al usuario.

En relación a las acciones de control que las empresas operadoras aplican de manera voluntaria, se puede señalar lo siguiente:

- Se trata de un control deficiente, dado que las empresas operadoras no son proactivas en la entrega de la información sobre las suplantaciones, ni brindan el adecuado apoyo a las víctimas.
- No se puede determinar a los distribuidores y asesores que han actuado con negligencia y, tal vez, con complicidad.
- Los usuarios se enteran de manera tardía de las suplantaciones, debido a que no existen alertas cuando se inician este tipo de trámites.

Considerando las evidencias reportadas en la sección 6, se ha determinado las calificaciones para la probabilidad de ocurrencia y el nivel de impacto. La calificación se ha realizado de conformidad con las escalas determinadas en los cuadros N° 16 y 17. Cabe recordar que el nivel de riesgo se obtiene de multiplicar la calificación del nivel de probabilidad de ocurrencia con la calificación del nivel de impacto.

De esta manera, se ha calificado que todos los escenarios de riesgo que están bajo análisis tienen un nivel de impacto muy alto (5), ello debido a que las víctimas sufren considerables pérdidas cuando pierden el control de su línea móvil (en promedio S/ 10065). Incluso en los casos en que solo ha habido una contratación no solicitada, el impacto es considerable para los usuarios, dado que podrían adquirir deudas por el consumo de líneas que erróneamente están a su nombre.

Cabe señalar que el ingreso neto promedio anual de los hogares en el 2020 fue de S/ 31 046[64], y su ingreso promedio mensual es de S/ 2 587. En ese sentido, considerando que se tienen 3 grupos de víctimas:

- Las reportadas al OSIPTEL: Su pérdida promedio es de S/ 10 065, es decir 3.89 veces su ingreso mensual.
- Las reportadas a las empresas operadoras: Su pérdida promedio es de S/ 7113, es decir 2.75 veces su ingreso mensual.
- Los afectados en el bono de S/ 600: Las familias más pobres tienen un ingreso mensual de S/ 345[65], por lo que la pérdida del bono significó 2.6 veces su ingreso mensual

Por lo tanto, se considera que toda pérdida económica que sea igual al ingreso mensual debería ser catalogado como “Alto”, pero si llega por encima del ingreso mensual, entonces debe ser catalogado como “Muy Alto”. Las otras categorías de calificación (Muy, Bajo y Moderado) son apropiados para pérdidas menores al ingreso mensual del hogar.

En el caso de la probabilidad de ocurrencia, la calificación se ha realizado con base a las siguientes consideraciones:

- Comercialización en la vía pública:

  Es la manera más riesgosa para contratar líneas móviles, realizar la reposición de SIM card o hacer cambios de titularidad debido a que el Perú es un país conal ta informalidad y delincuencia, y los usuarios no están protegidos en la vía pública. En las secciones anteriores se detallaron los diversos hallazgos durante las supervisiones, en las que se encontraron cómo las empresas operadoras han estado contratando asesores que no han tenido el debido

[64] Estimado a partir de la ENAHO 2020
[65] A partir de la ENAHO 2020. El ingreso anual de este segmento es S/ 4142.

cuidado en la verificación biométrica, e incluso han generado que formulen varios reclamos por contratación no solicitada.

Asimismo, es necesario señalar que no todos los países enfrentan los mismos niveles de riesgo, y que, en el caso peruano, la informalidad es un problema que no ha estado presente en el sector telecomunicaciones, hasta que las mismas empresas operadoras decidieron salir a comercializar las líneas en la vía pública. Esta decisión comercial ha generado en contexto necesario para que la delincuencia encuentre un nuevo campo de acción, sobre todo porque estas ventas en la calle no están siendo supervisadas por las mismas empresas operadoras.

En atención a estas consideraciones, se califica que la probabilidad de ocurrencia de los riesgos bajo análisis es “Casi cierto”, calificación de 5, en las ventas realizadas en la vía pública.

- Comercialización en el canal telefónico:

  A partir de la revisión de la experiencia internacional y de las empresas que brindan soluciones de seguridad, ver sección 5.1, se tiene conocimiento que los estafadores hacen un uso frecuente del canal telefónico porque les permite atacar en gran escala. Es decir, realizar llamadas masivas a los call center de las empresas hasta encontrar a un asesor irresponsable o negligente, y entonces lograr acceder al control de la línea o realizar otra estafa.

  Además, a partir de las indagaciones de la policía, se conoce es probable que algunos de los trabajadores de las empresas operadoras actúen en complicidad con los delincuentes, por lo que este canal de atención no está exento de riesgos.

  Por lo tanto, la probabilidad de ocurrencia de este riesgo se califica como “probable”, con un valor de 4.

- Comercialización en el canal presencial

  Este canal debería tener una probabilidad de ocurrencia baja, dado que se supone que se aplica la verificación biométrica y existen jefes de tienda que supervisan a sus empleados. No obstante, la realidad nos ha mostrado un escenario diferente que se tiene que abordar.

  En primer lugar, se ha detectado que las huellas están siendo clonadas e imprimidas de manera masiva por delincuentes. Adicionalmente, también se han tenido noticias que algunos empleados de las empresas actúan en complicidad con la delincuencia y han cometido estos fraudes. No obstante, se puede apreciar el aspecto positivo del canal presencial, que es la existencia de cámaras de seguridad, las cuales efectivamente han permitido identificar y registrar estos comportamientos.

  En atención a estas evidencias, se debe calificar que este canal tiene una probabilidad de ocurrencia “posible”, con una calificación de 3, y que por tanto, requiere de medidas de prevención.

En el cuadro 26 se puede apreciar el nivel de riesgo calculado para la alternativa 1, la cual en promedio es 20. Este resultado se ha obtenido promediando el nivel de riesgo estimado para los trámites de cambio de titularidad, contratación de línea móvil y

reposición de la *SIM card*. Estos niveles de riesgo se obtienen de multiplicar las calificaciones de probabilidad de ocurrencia y nivel de impacto.

Normalizando este resultado respecto a la calificación máxima de 25, se obtiene una calificación normalizada de 0.80 en nivel de riesgo.

Cuadro N° 26
NIVEL DE RIESGO DE LA ALTERNATIVA 1 (SITUACIÓN INICIAL)

Proceso donde se identifica el riesgo	Canal identificado	Probabilidad de ocurrencia		Nivel de Impacto individual		Nivel de Riesgo
		Tipo	Nivel	Tipo	Nivel	
Cambio de Titularidad	Presencial	Posible	3	Muy alto	5	**15**
	Telefónico	Probable	4	Muy alto	5	**20**
	Ambulante	Casi cierto	5	Muy alto	5	**25**
Adquisición de línea	Presencial	Posible	3	Muy alto	5	**15**
	Telefónico	Probable	4	Muy alto	5	**20**
	Ambulante	Casi cierto	5	Muy alto	5	**25**
Reposición de Chip	Presencial	Posible	3	Muy alto	5	**15**
	Telefónico	Probable	4	Muy alto	5	**15**
	Ambulante	Casi cierto	5	Muy alto	5	**20**
Promedio						**20**

Elaboración: OSIPTEL.

Para mitigar los riesgos sobre los procesos analizados, en la Alternativa 2 se propone implementar los controles de riesgo reportados en el cuadro N° 27. Se espera que el efecto de estos controles permita que los riesgos tengan un nivel de ocurrencia raro. Es decir, no se espera que estas vulneraciones a la seguridad desaparezcan por completo, pero que sí que sean extremadamente raros y trazables.

Finalmente, resulta válido recordar lo que se ha encontrado en la revisión de la experiencia internacional, la cual señala que países en vías de desarrollo y con alta informalidad suelen tener problemas con la venta ambulatoria, como por ejemplo los países africanos y el Perú. Asimismo, a nivel global, la UIT y algunos reguladores están buscando estrategias para mitigar la incidencia de estos riesgos, por lo que intervención del OSIPTEL en estos temas se encontraría bastante justificada.

Cuadro N° 27
NIVEL DE RIESGO DE LA ALTERNATIVA 2 (SITUACIÓN FINAL)

Proceso donde se identifica el riesgo	Canal identificado	Control Actual	Valor del Nivel de Riesgo Inicial	Nivel de Riesgo	Componentes de control de la Alternativa 2	Riesgo Residual Objetivo				Nivel de Riesgo Final	Nivel de riesgo residual o Final
						Probabilidad de ocurrencia		Nivel de Impacto			
Cambio de Titularidad	Presencial	Solicitud de DNI y huella dactilar	15	Muy Alto	1. Identificación temprana de solicitudes aprobadas sin consentimiento del abonado. 3. Reglas en los canales de comercialización 4. Reglas de seguridad para los trámites con representantes 5. Reglas de seguridad para la verificación biométrica de la huella dactilar	Raro	1	Muy Alto	5	5	Bajo
	Telefónico	Solicitar datos personales y preguntas secretas	20	Muy Alto		Raro	1	Muy Alto	5	5	Bajo
	Ambulante	Solicita datos personales y huella	25	Muy Alto		Raro	1	Muy Alto	5	5	Bajo
Adquisición de línea	Presencial*	Solicitud de DNI y huella dactilar	15	Muy Alto		Raro	1	Muy Alto	5	5	Bajo
	Telefónico*	Solicitar datos personales y preguntas secretas	20	Muy Alto		Raro	1	Muy Alto	5	5	Bajo
	Ambulante*	Solicita datos personales y huella	25	Muy Alto		Raro	1	Muy Alto	5	5	Bajo
Reposición de Chip	Presencial	Solicitud de DNI y huella dactilar	15	Muy Alto	1. Identificación temprana de solicitudes aprobadas sin consentimiento del abonado. 2. Identificación de intentos de reposición fraudulenta 3. Reglas en los canales de comercialización 4. Reglas de seguridad para los trámites con representantes 5. Reglas de seguridad para la verificación biométrica de la huella dactilar	Raro	1	Muy Alto	5	5	Bajo
	Telefónico	Solicitar datos personales y preguntas secretas	20	Muy Alto		Raro	1	Muy Alto	5	5	Bajo
	Ambulante	Solicita datos personales y huella	25	Muy Alto		Raro	1	Muy Alto	5	5	Bajo
Promedio de Alternativa 1			20	Muy Alto	Promedio de la Alternativa 2					5	Bajo

Elaboración: OSIPTEL.

En cambio, no se espera que estos controles puedan atenuar el nivel de impacto, sobre todo en los casos de suplantación en la reposición de la *SIM card*; ello debido a que el monto de pérdida promedio que experimentan los usuarios solo podría reducirse si ellos mismos adoptan medidas de seguridad adicionales para proteger sus cuentas bancarias. Por lo tanto, en promedio, el nivel de riesgo residual que se obtendría con la Alternativa 2 sería bajo, calificado en 5. La normalización de esta calificación es de 0.20, ya que el máximo nivel de riesgo es 25.

A partir del análisis previo, la Alternativa 2 tiene una calificación de 0.80 en manejo de riesgo, la cual resulta de restar 1 menos el nivel de riesgo normalizado obtenido (0.2); en cambio, la Alternativa 1 tiene una calificación de 0.20, la cual resulta de restar 1 menos 0.80. La calificación aplicable al AMC se obtiene aplicando la fórmula 2, el resultado se puede apreciar en el cuadro N° 28.

Cuadro N° 28
CALIFICACIÓN DE LAS ALTERNATIVAS EN EL ATRIBUTO 3: MANEJO DEL RIESGO

Alternativa	Nivel de riesgo normalizado	Calificación	Calif. en AMC
Alternativa 1	0.80	0.20	-0.60
Alternativa 2	0.20	0.80	0.60

f) Criterio 4: Trazabilidad para el usuario

Como se ha indicado previamente, la trazabilidad que ofrecen las alternativas 1 y 2 se van evaluar respecto a los siguientes criterios:

- Identificación del lugar del trámite
- Identificación del personal que participó de la solicitud
- Identificación del suplantador

En relación al lugar del trámite, la Alternativa 1 si bien establece que los distribuidores reporten la dirección del centro de atención; existe una ambigüedad respecto a si es una explícita prohibición de realizar la verificación en la vía pública, por ello su calificación es de 0.1; en cambio, en el caso de la Alternativa 2, explícitamente se está indicando que la contratación en ferias itinerantes solo es posible en los centros poblados rurales donde la empresa operadora tiene cobertura, pero no tiene centro de atención o en otras ferias itinerantes autorizadas previamente por el OSIPTEL, por ello la calificación que le corresponde es 0.7. Además, la Alternativa 2 habilita la entrega de la *SIM card* por *delivery*, por lo que brinda facilidades a las empresas operadoras para contratar servicios fuera del centro de atención.

Respecto a la trazabilidad del personal de la empresa, la Alternativa 1 no establece reglas que obliguen a los asesores de las empresas a identificarse, por lo que la calificación que le corresponde es 0.3; en cambio, con la Alternativa 2, se está garantizando que los asesores pasen por la verificación biométrica, y se evita así, que la contratación lo realice personal no autorizado. Incluso, en caso que se haya efectuado una contratación no solicitada, la Alternativa 2 va permitir que el usuario identifique al asesor responsable de esa negligencia; por todo ello, la alternativa 2 se está calificando en 0.7 en este atributo.

Con relación a la identificación del suplantador, la Alternativa 1 o situación inicial no permite que el usuario pueda conocer anticipadamente que están intentando vulnerar su línea móvil, mucho menos se puede identificar quién ha sido el suplantador; por ello se debe otorgar una calificación de 0.1. en cambio, con la Alternativa 2, el usuario va

poder enterarse de cualquier intento de suplantación, y en caso esto sucediera, la empresa operadora debería tener la captura fotográfica de la persona que perpetró ese delito, por ello se debe calificar a esta alternativa con 0.7.

En el cuadro N° 29 se reportan los resultados de estas calificaciones y el resultado global en el criterio de trazabilidad. Cabe señalar que para el resultado global se ha aplicado ponderadores con el objetivo de dar mayor importancia a la identificación del lugar de trámite y la identificación del personal de la empresa operadora.

Cuadro N° 29
SITUACIÓN ACTUAL DE INFORMACIÓN

Actividad	Ponderador	Calif. Alter 1	Calif. Alter 2
Identificación del lugar del trámite	0.40	0.1	0.7
Identificación del personal de la empresa	0.40	0.3	0.7
Identificación del suplantador	0.20	0.1	0.7
Calificación global		0.18	0.7

Elaboración: OSIPTEL.

Finalmente, los valores normalizados para el AMC se presentan en la última columna del Cuadro N° 30, e indican que la alternativa 2 es la que garantiza un mejor nivel de control y trazabilidad de los procesos de contratación, activación de línea, reposición y cambio de titularidad.

Cuadro N° 30
CALIFICACIÓN DE LAS ALTERNATIVAS EN EL ATRIBUTO 4: TRAZABILIDAD

Alternativa	Calificación	Calif. en AMC
Alternativa 1	0.18	-0.64
Alternativa 2	0.70	0.40

Elaboración: OSIPTEL.

8.3. Propuesta de solución

En AMC que se implementado para evaluar a las alternativas 1 y 2 ha incluido 4 atributos: facilidad en la implementación, beneficios para el usuario, manejo de riesgo y trazabilidad. En 3 de estos atributos, la alternativa 2 ha resultado mejor que la alternativa 1, como se puede apreciar en el cuadro N° 31, mientras que la alternativa 1 ha resultado mejor solamente en la facilidad de implementación.

Los atributos elegidos y los pesos otorgados garantizan que esta AMC evalúe de manera equilibrada los diversos aspectos que el mercado y los usuarios valoran. En tal sentido, los resultados obtenidos permiten identificar la alternativa más recomendable o la que va generar un mayor impacto en el bienestar social.

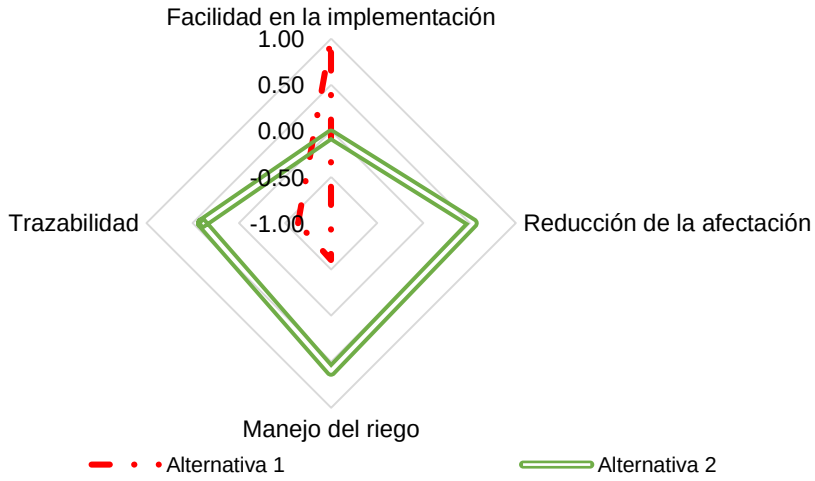
Por lo tanto, en atención a los resultados obtenidos en este AMC, se recomienda la implementación de la alternativa 2, dado que ha obtenido un puntaje de 0.46, superior a lo obtenido por la alternativa 1 (-0.45).

Cuadro N° 31
RESULTADO DEL AMC

Atributo	Alternativa 1	Alternativa 2	Ponderación
Facilidad de implementación	1.00	-0.04	0.15
Reducción de la afectación	-1.00	0.51	0.20
Manejo de riesgos	-0.60	0.60	0.50
Trazabilidad para los usuarios	-0.64	0.40	0.15
Calificación Final	**-0.45**	**0.46**	

Elaboración: OSIPTEL.

Gráfico N° 16
RESULTADOS DEL AMC



Elaboración: OSIPTEL.

9. APLICACIÓN DE LA SOLUCIÓN SELECCIONADA

9.1. Propuesta normativa

El OSIPTEL ha observado situaciones que favorecen o facilitan que el abonado se encuentre expuesto a registros de servicios no contratados bajo su titularidad y que se efectúen trámites no solicitados respecto de sus servicios públicos de telecomunicaciones, por lo que resulta necesario establecer reglas que permitan brindar mayor seguridad en tales procesos.

En ese sentido, luego de la revisión realizada por este Organismo se ha considerado necesario algunas precisiones y modificaciones al Texto Único Ordenado de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, así como la inclusión de nuevos artículos, a efectos de garantizar una adecuada información, contratación y provisión del servicio.

Los artículos que se propone modificar son: artículos 2, 11, 11-A, 11-D, 67-B, 71, 118, 119 y 128 de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, conforme al siguiente detalle:

Artículo que se propone modificar	Fundamento
Artículo 2.- Derecho de los abonados y usuarios Se propone eliminar la disposición que habilita a la empresa operadora aceptar que el poder sea otorgado mediante documento escrito, adjuntando copia simple de: (i) el documento legal de identificación del abonado, y (ii) el último recibo del servicio, de ser el caso.	Considerando que es el abonado quien asume la responsabilidad por el uso del servicio, así como el pago por el mismo, corresponde que sea éste quien realice los trámites previstos en la normativa y en todo caso, de requerir la representación de un tercero, que el poder otorgado conste en un documento de fecha cierta, que permita brindar una mayor seguridad sobre su manifestación de voluntad. En ese sentido, se propone eliminar la disposición que habilita a la empresa operadora aceptar que el poder sea otorgado mediante documento escrito, adjuntando copia simple de: (i) el documento legal de identificación del abonado, y (ii) el último recibo del servicio, de ser el caso.
Artículo 11.- Registro de abonados de acuerdo a la modalidad de contratación del servicio Se propone reducir los supuestos en los cuales no se requiere la exhibición del documento legal de identificación. Ello a fin de que la empresa operadora deba requerir la exhibición del documento de identidad en la contratación del servicio público móvil de manera adicional a la verificación biométrica, salvo para los casos de contratación de medios no presenciales de auto-activación, en el cual se realice la verificación biométrica de huella dactilar mediante tecnología de detección de huella viva.	Dado los problemas de suplantación de identidad en la contratación del servicio público móvil, así como en la reposición de SIM Card, se advierte que la verificación biométrica (proceso que se realiza en ambos casos) puede ser evadida por terceros, por lo que se establece que, como medida adicional, la empresa operadora requiera la exhibición del documento de identidad del solicitante del servicio o abonado. En ese sentido, se propone reducir los supuestos en los cuales no se requiere la exhibición del documento legal de identificación. Ello a fin de que la empresa operadora deba solicitar la exhibición del documento de identidad en la contratación del servicio público móvil de manera adicional a la verificación biométrica. Se considera como excepción los casos de contratación de servicios de distribución de radiodifusión por cable bajo la modalidad prepago, servicios de larga distancia y servicios de interoperabilidad, teniendo en

Artículo que se propone modificar	Fundamento
	cuenta su naturaleza receptiva (en el caso del servicio de radiodifusión por cable prepago) y de servicios adicionales (en el caso de servicios de larga distancia e interoperabilidad). Asimismo, se omite requerir la exhibición del documento de identidad en la contratación por medios no presenciales de auto-activación, por cuanto, en tales casos no hay una interacción directa de un representante de la empresa operadora que pueda requerir la exhibición del documento legal de identificación. No obstante, es de precisar que dicho mecanismo se propone que sea regulado en el artículo 11-D a fin de establecer disposiciones que permitan brindar mayor seguridad al mismo
Artículo 11-A.- Verificación de identidad del solicitante del servicio público móvil y para la contratación de servicios públicos móviles Se propone establecer un número máximo de intentos de verificación biométrica por persona en el día, de cinco (5) intentos por transacción. Previo a la captura de la huella dactilar, la empresa operadora debe verificar que la mano del solicitante del servicio o representante se encuentre libre de cualquier elemento externo que pueda adulterar o invalidar la verificación. Ante la negativa del solicitante del servicio o representante, la empresa operadora debe suspender el trámite, informando el motivo. La empresa operadora debe remitir inmediatamente a la activación del servicio de manera adicional al mensaje de texto actualmente previsto, una locución a cada una de las	De los casos gestionados ante el OSIPTEL, en los cuales se habría presentado una suplantación de identidad para la contratación o reposición de SIM Card, se observa que se realizan varios intentos, de los cuales solo algunos resultan exitosos, según la información remitida por el Registro Nacional de Identificación y Estado Civil – RENIEC. Por tanto, se requiere establecer un máximo de intentos de verificación biométrica en el día por transacción, a fin de evitar que el resultado de la verificación biométrica se obtenga luego de una cantidad anómala de rechazos, que resta confiabilidad al procedimiento. En ese sentido, se propone establecer un número máximo de cinco (5) intentos de verificación biométrica por persona en el día y por transacción. Asimismo, considerando que terceros emplearían huellas falsas para suplantar la identidad de los abonados en la verificación biométrica, se propone que previo a la captura de la huella dactilar, la empresa

Artículo que se propone modificar	Fundamento
líneas móviles que el abonado tiene registrado con su documento legal de identificación en dicha empresa, así como un correo electrónico a la dirección electrónica registrada por el abonado, mediante los cuales informe de la contratación del nuevo servicio. Asimismo, se propone precisar que las disposiciones establecidas sobre la verificación de identidad aplican para todos los trámites y servicios en los cuales se realice la verificación biométrica de huella dactilar.	operadora debe verificar que la mano del solicitante del servicio o representante se encuentre libre de cualquier elemento externo que pueda adulterar o invalidar la verificación. De otro lado, con la finalidad de obtener mayor efectividad respecto del aviso de la contratación de nuevos servicios, se considera necesario que adicionalmente al mensaje de texto actualmente previsto, la empresa operadora remita una locución a cada una de las líneas móviles que el abonado tiene registrado con su documento legal de identificación en dicha empresa así como un correo electrónico a la dirección electrónica registrada por el abonado, mediante los cuales se informe sobre la contratación del nuevo servicio. Asimismo, se propone precisar que las disposiciones establecidas sobre la verificación de identidad aplican para todos los trámites y servicios en los cuales se realice la verificación biométrica de huella dactilar.
Artículo 11-D.- <u>Contratación de servicios a través de los distintos canales</u> Se precisa que la empresa operadora es responsable de todo el proceso de contratación del servicio que provea, que comprende la identificación y el registro de los abonados que contratan sus servicios, independientemente del canal o medio de atención o comercialización. Se propone listar los medios para la contratación del servicio: centros de atención, en la dirección específica del punto de venta previamente reportado al OSIPTEL, mediante el canal telefónico, de forma virtual o en la dirección indicada por el	La contratación del servicio público de telecomunicaciones debe realizarse por medios previamente identificados en la normativa, siendo que se requiere que sean de conocimiento de los usuarios a fin de que puedan emplear dichos medios y no sean embaucados por terceros. Se propone listar los medios para la contratación del servicio: centros de atención, en la dirección específica del punto de venta previamente reportado al OSIPTEL, mediante el canal telefónico, de forma virtual o en la dirección indicada por el solicitante del servicio y excepcionalmente en ferias itinerantes. Cabe indicar que, se han reconocido todos los medios que actualmente las empresas emplean para la contratación de sus servicios, salvo aquél de carácter ambulatorio, que conforme se desarrolla en el presente

Artículo que se propone modificar	Fundamento
solicitante del servicio y excepcionalmente en ferias itinerantes. Se precisa que en el caso de distribuidores solo se puede contratar el servicio ante aquellos que se encuentren previamente autorizados por la empresa operadora y reportados al OSIPTEL, y en el punto de venta con dirección específica registrada. Se propone que la empresa operadora otorgue un código único que identifique al distribuidor autorizado, así como al punto de venta habilitado para realizar las contrataciones, y al personal que depende del distribuidor y participa directamente en la contratación del servicio. Asimismo, para la contratación del servicio, el distribuidor autorizado o su personal que interviene en dicha transacción, se propone que valide su identidad mediante verificación biométrica de huella dactilar o con el uso de una contraseña. La empresa operadora debe remitir al OSIPTEL el registro de distribuidores autorizados, con información del distribuidor, punto de venta y personal que interviene en la contratación del servicio. Se propone requerir que la empresa operadora establezca supuestos de suspensión temporal y cese definitivo de operaciones del distribuidor autorizado debido a contrataciones no solicitadas. Adicionalmente, se propone regular el uso de ferias itinerantes para la contratación del servicio, señalando que	informe expone al abonado a una serie riesgos con sus consecuentes perjuicios. Asimismo, se establecen reglas mínimas respecto de los mismos, a fin de que la contratación del servicio se lleve a cabo brindando información suficiente al usuario y se registre de forma adecuada la titularidad de los servicios públicos de telecomunicaciones. Las reglas sobre los distribuidores autorizados, sus puntos de venta y personal se proponen con la finalidad de tener mayor trazabilidad de la contratación a través de dichos medios, por cuanto se ha observado que no existe un control estricto sobre su actuación, pese a que el servicio que comercializan es un servicio público, de naturaleza esencial y que fue dado en concesión por el Estado para su prestación por la empresa operadora. Las problemáticas observadas por la falta de un adecuado control de los distribuidores autorizados se desarrollan en el informe que sustenta la propuesta normativa. Considerando que las empresas operadoras incluido sus distribuidores, no cuentan con puntos de venta en todas las provincias del país, se admite la realización de ferias itinerantes en dichos lugares, esto es, que se pueda comercializar el servicio en plazas, parques u otros ambientes públicos. Sin embargo, se precisa que corresponde que la empresa cuente con cobertura en la zona, puesto que se ha observado casos en los cuales las empresas operadoras realizan la comercialización del servicio en lugares donde no se encuentra declarada la cobertura, no obstante se accede al servicio por rebote o repetición de señal de una estación base cercana, y dada la asimetría de información, el usuario

OSIPTEL DAPU H.GUSUKUMA
OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU M.GONZALEZ

Artículo que se propone modificar	Fundamento
estas se llevan a cabo solo en centros poblados rurales o en provincias en las cuales no cuenta con oficinas y/o centros de atención o puntos de venta, o en otras ferias itinerantes autorizadas previamente por el OSIPTEL. En cualquier caso la empresa operadora debe contar con cobertura y la autorización municipal respectiva. La empresa operadora debe informar al OSIPTEL, con una anticipación de diez (10) días hábiles, las fechas y lugares donde se llevarán a cabo. Se propone precisar respecto del canal de comercialización del servicio mediante entrega a domicilio (*delivery),* que la empresa operadora debe tener identificado al personal que participa en la contratación, validación de identidad y/o realiza la entrega de la *SIM Card* al solicitante del servicio. Asimismo, establecer que, para el uso de este canal, el solicitante debe requerir el servicio a través del canal telefónico, página web u otro canal virtual de la empresa operadora. Se propone que la *SIM Card* sea entregado únicamente de manera personal por la empresa operadora en la dirección indicada por el solicitante del servicio público móvil, para lo cual la empresa operadora debe requerir la exhibición del documento de identidad del solicitante del servicio, debiendo conservar la captura de la imagen del mismo como constancia de su exhibición. En caso la *SIM Card* sea adquirido en establecimientos comerciales para posterior autoactivación, se propone requerir que la empresa operadora cuente con un registro de tales establecimientos, con el nombre comercial y razón	contrata los servicios con la expectativa de usarlos en la zona donde los adquirió, presentando luego problemas con la prestación del servicio, que no pueden ser atendidos. De otro lado, considerando que las disposiciones del OSIPTEL deben observar la normativa vigente, se hace mención a que la empresa debe contar con la autorización municipal respectiva. Con relación al canal *delivery*, se precisa que la empresa operadora debe tener identificado al personal que participa en la contratación, considerando que dicho personal tendrá acceso a los datos del usuario, y será quien realice la entrega del SIM Card. Con la finalidad de acreditar la entrega del SIM Card a la persona que requirió el servicio y no a un tercero, se requiere de la exhibición y almacenamiento de una imagen del documento de identidad del solicitante del servicio. Respecto de los SIM Card adquiridos en establecimientos comerciales para posterior auto-activación, se requiere un registro de dichos establecimientos, a fin de que los usuarios puedan conocer aquellos autorizados por la empresa operadora. Del mismo modo, considerando que al momento de la venta del SIM Card no se realiza alguna validación de identidad y con la finalidad de evitar la reventa de SIM Card, se propone que se limite a una sola activación o portabilidad numérica en el mes por el abonado. Cabe indicar que, las empresas operadoras que actualmente emplean este medio de comercialización aplican las referidas reglas. El servicio público móvil requiere de la verificación biométrica, lo cual demanda que la contratación se realice por medios presenciales, salvo en el caso de auto-activación que por medio virtual permite la verificación biométrica de *contact less*. Por tanto, se considera que la contratación

OSIPTEL DAPU H.GUSUKUMA
OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU M.GONZALEZ

Artículo que se propone modificar	Fundamento
social del establecimiento comercial, la dirección de cada uno de ellos, con el detalle del distrito, provincia y departamento, así como el código designado del establecimiento comercial en el cual se adquiere la *SIM Card*. Se propone que la activación del servicio público móvil mediante *SIM Card* adquirida en establecimientos comerciales se limite a una sola activación o portabilidad numérica en el mes por el abonado. Se propone detallar que la contratación de nuevos servicios por el canal telefónico de la empresa operadora no aplica para el servicio público móvil, salvo aquellos casos en los que se valide la identidad del abonado a través de la contraseña única a la que hace referencia el artículo 128. Se propone precisar que la empresa operadora debe tener identificado y registrado el canal o medio a través del cual se contrató el servicio y el distribuidor o personal que participó en la contratación, así como el medio por el cual se validó la identidad del abonado y se adquirió la *SIM Card*, conforme al presente artículo. La empresa operadora tiene la carga de la prueba de la validación de identidad exitosa de la persona natural que interviene en la contratación de cada uno de sus servicios	de nuevos servicios por el canal telefónico –medio no presencial- no sea empleada respecto del servicio público móvil. Conforme se mencionó previamente se requiere contar con la información el canal o medio a través del cual se contrató el servicio y el distribuidor o personal que participó en la contratación, así como el medio por el cual se validó la identidad del abonado y se adquirió el SIM Card, a fin de que la empresa operadora tenga mayor control respecto de ellos, de tal manera que se garantice que se sigue el procedimiento previsto en la normativa vigente.
Artículo 67-B.- Reposición de *SIM Card* y recuperación de número telefónico o de abonado del servicio público móvil	La reposición de SIM Card es un trámite relevante por cuanto permite contar con el servicio activo. En ese sentido, previo a la propagación del COVID-19, se encontraba restringido a realizarlo en los centros de atención, o por otros medios establecidos por la empresa operadora de

OSIPTEL DAPU H.GUSUKUMA
OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU M.GONZALEZ

Artículo que se propone modificar	Fundamento
Se propone que la solicitud de reposición de la *SIM Card* sea presentada: a) en forma personal por el abonado, en cualquiera de las oficinas o centros de atención de la empresa operadora y los puntos de venta o atención habilitados en virtud a lo dispuesto en el tercer y cuarto párrafo del artículo 43, previamente reportados al OSIPTEL; y b) mediante los canales de *delivery* y establecimientos comerciales para posterior autoactivación. Asimismo, se propone como medida de seguridad complementaria para validar la identidad del abonado, que la empresa operadora aplique los lineamientos establecidos para validar la condición de abonado en la presentación de reclamos. Para tal efecto, la empresa debe registrar y conservar las constancias de las preguntas realizadas y las respuestas obtenidas de dicha validación. Se precisa que corresponde realizar la verificación biométrica y requerir la exhibición del documento de identidad al representante del abonado. Se propone establecer que previo a la activación de la nueva *SIM Card*, la empresa operadora debe enviar un mensaje de texto y una locución a todos los servicios móviles bajo titularidad del abonado registrados en dicha empresa operadora, así como un correo electrónico a la dirección electrónica registrada por el abonado informando sobre el trámite, al momento de la recibir la solicitud de reposición de la *SIM Card* y luego de transcurrido dos (2) horas desde el	forma presencial. En todos los casos previa verificación biométrica de identidad. No obstante, en atención a las medidas dictadas por el Gobierno para evitar la propagación del COVID-19 se habilitó se realice el referido trámite de reposición de SIM Card en todos los puntos de venta. Al respecto, se observa el incremento considerable de fraudes en la realización de dicho trámite. Por tanto, se propone que el mismo se realice en los centros de atención y puntos designados para atención en provincias. Esto considerando que, de acuerdo a la propuesta normativa, dichos medios de adquisición de SIM Card cuentan con mayores medidas de seguridad. En la misma línea, con la finalidad de evitar fraudes en la realización del referido trámite de reposición de SIM Card se propone como medida complementaria a la verificación biométrica, el requerir la exhibición del documento de identidad del abonado y que se realicen las preguntas de validación como fecha de última recarga, monto de última recarga, en caso el servicio sea prepago, o la fecha del vencimiento del recibo, monto del plan tarifario, y dirección de facturación, en caso del servicio postpago. Considerando que, pese a la verificación biométrica, se ha advertido que terceros han logrado evadir dicho control y acceder al SIM Card activo del abonado, se propone como medida de seguridad que la activación del SIM Card se realice luego de cuatro horas de presentada la solicitud y que en dicho periodo se remitan mensajes de texto, locuciones, y correos electrónicos al abonado a fin de informar hasta en dos

OSIPTEL DAPU H.GUSUKUMA
OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU M.GONZALEZ

Artículo que se propone modificar	Fundamento
primer envío. Asimismo, se propone permitir el bloqueo inmediato de la atención de dicha solicitud por parte del abonado previamente identificado según los lineamientos establecidos para validar la condición de abonado en la presentación de reclamos. Se propone que la activación de la *SIM Card* se realice a las cuatro (4) horas de presentada la solicitud. Asimismo, se propone que la empresa operadora envíe el referido mensaje de texto y correo electrónico en los casos que la solicitud de reposición de la *SIM Card* es denegada por intentos fallidos de verificación biométrica de huella dactilar o porque el poder presentado por el representante fue observado.	oportunidades sobre el trámite requerido, y en caso desconozca dicha solicitud, requiera su bloqueo para que no se lleve a cabo. Del mismo modo, con la finalidad de que el usuario se encuentre alerta y adopte las medidas de seguridad correspondientes, se propone que se informe de los intentos fallidos de presentar dicha solicitud de reposición de SIM Card. Cabe indicar que, tales medidas de seguridad son recomendadas por distintos organismos y especialistas internacionales, considerando la relevancia del cambio o reposición de SIM Card, que incide en la continuidad de la prestación del servicio y el uso del mismo por el abonado o la persona que éste autorice.
Artículo 71.- Supuestos de suspensión del servicio Se propone establecer como causal de suspensión del servicio el hecho que el abonado desconozca o cuestione la contratación del servicio o la reposición de la *SIM Card*.	Considerando que cuando el abonado desconoce la contratación del servicio o la reposición del SIM Card no se tiene identificada a la persona que realiza el uso del servicio, y esta habría accedido al mismo de forma ilícita o sin seguir los procedimientos establecidos, corresponde realizar como medida preventiva la suspensión del servicio. Ello permitirá reducir la afectación del usuario respecto del uso que se brinde al servicio que se encuentra bajo su titularidad y no se encuentra dentro de su control y uso.
Artículo 118.- Mecanismos de contratación	Las empresas operadoras vienen empleando mecanismos de contratación que implican una auto-activación del servicio por parte del

Artículo que se propone modificar	Fundamento
Se propone incluir como mecanismo de contratación a aquél correspondiente a la Autoactivación, el cual requiere se valide la identidad del solicitante del servicio y se obtenga su manifestación de voluntad, mediante verificación biométrica de huella dactilar a través del aplicativo informático.	abonado, mediante el empleo de aplicativos informáticos que permiten validar la identidad del abonado y obtener su manifestación de voluntad. En ese sentido, se formaliza dicha figura en las Condiciones de Uso, a fin de facilitar su aplicación y uniformizar los requisitos exigidos. Por tanto, se propone incluir como mecanismo de contratación a aquél correspondiente a la auto-activación, el cual requiere se valide la identidad del solicitante del servicio y se obtenga su manifestación de voluntad, mediante verificación biométrica de huella dactilar a través del aplicativo informático. Asimismo, como mecanismo de seguridad se exige que de manera aleatoria, se formulen preguntas de validación sobre los datos del abonado.
Artículo 119.- Migración a planes tarifarios y contratación de servicios suplementarios o adicionales Se precisa que para el caso de migración a planes tarifarios, contratación de servicios suplementarios o adicionales, no será exigible la exhibición del documento legal de identificación así como la validación de identidad del abonado mediante el sistema de verificación biométrica para el caso de los servicios públicos móviles, siempre que éste se encuentre debidamente identificado por ésta última.	En la norma vigente se hace mención a que no es exigible la copia del documento de identidad del abonado en los casos de migración de planes tarifario, contratación de servicios suplementarios o adicionales. Sin embargo, es de considerar que la obligación de requerir una copia del documento de identidad y su conservación para la contratación fue suprimida en una anterior modificación normativa. Por tanto, corresponde precisar que la obligación que no se exige en tales supuestos, se encuentra referida a la exhibición del documento de identidad, que es aquella que se mantiene como requisito general para las contrataciones y se excluiría de forma excepcional para el caso de migraciones y contrataciones de servicios suplementarios o adicionales.
Artículo 128.- Contraseña Única Se propone precisar que es la empresa operadora quien se encuentra obligada a proporcionar a sus abonados la	Actualmente, la contraseña única no se encuentra difundida entre los usuarios, entre otros, por cuanto no se estaría proporcionando de oficio

Artículo que se propone modificar	Fundamento
contraseña única al momento de la contratación del servicio o en cualquier otro en que su identidad sea validada a través del sistema de verificación biométrica de huella dactilar; o a través del correo electrónico que el abonado haya indicado en dicha oportunidad. **<u>Para la contratación de nuevos servicios principales,</u>** cambio de titularidad y reposición de SIM Card de aquellos abonados que cuentan con contraseña única, de manera adicional a las validaciones de identidad previstas en los artículos 11, 11-A y 67-B, se requiere proporcione su contraseña única de forma exitosa.	en todos los casos que se realiza una nueva contratación del servicio y/o se valida la identidad del abonado mediante verificación biométrica. Considerando que el uso de la contraseña única permitiría contar con una herramienta que brinde seguridad respecto de la participación del abonado en los trámites que realice con relación a su servicio, se propone establecer de forma expresa la obligación de las empresas operadoras de proporcionar a sus abonados la contraseña única al momento de la contratación del servicio o en cualquier otro en que su identidad sea validada a través del sistema de verificación biométrica o del correo electrónico indicado en dicha oportunidad. De otro lado una vez obtenida la contraseña única corresponde sea empleada como como mecanismo de seguridad para nuevas contrataciones de servicios principales, cambio de titularidad y reposición de SIM Card, en atención a que dichos trámites son relevantes para el abonado por los efectos jurídicos que le generan. En ese sentido, se propone que la contraseña única sustituya la verificación biométrica de la identidad para la realización de cualquier trámite, salvo para nuevas contrataciones de servicios principales, cambio de titularidad y reposición de SIM Card, en tanto que en tales casos se empleará como un mecanismo de seguridad adicional. Teniendo en cuenta que la contraseña única se empleará como mecanismo de seguridad para nuevas contrataciones de servicios principales, cambio de titularidad y reposición de SIM Card, así como podrá reemplazar la biometría respecto de los demás trámites, se propone que sea generada en caso la verificación biométrica se haya realizado en cualquiera de las oficinas o centros de atención de la empresa operadora y los puntos de venta o atención habilitados para atención de usuarios en provincias.

OSIPTEL DAPU H.GUSUKUMA
OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU M.GONZALEZ

De otro lado, los artículos que se propone incluir son los artículos 6-C, 75-B y 121-B de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, conforme al siguiente detalle:

Artículo que se propone incluir	Fundamento
Artículo 6-C.- Información de solicitudes presentadas Se propone establecer la obligación expresa de la empresa operadora de informar al abonado sobre las solicitudes presentadas y trámites registrados, tales como: servicios contratados, portabilidad numérica, cambios de titularidad, y reposición de la *SIM Card*. Asimismo, precisar que, la empresa operadora debe informar si el motivo de la falta o inoperatividad del servicio o tarjeta SIM reportada por el usuario obedece a alguna solicitud o trámite registrado.	De los casos gestionados ante el OSIPTEL sobre fraude en la contratación y/o reposición de la *SIM Card* se advierte que las empresas operadoras no estarían informando de forma adecuada sobre el motivo de la falta o inoperatividad del servicio o tarjeta SIM reportada por el usuario, siendo que se aborda dicha problemática desde el punto de vista de averías en el servicio, pese a que en muchos casos corresponde a trámites realizados por terceros, suplantando la identidad del abonado. En ese sentido, se propone establecer la obligación expresa de las empresas operadoras de identificar las causas de tales eventos, e informar de forma adecuada a los usuarios respecto de los mismos, a fin de que éste pueda adoptar las medidas legales correspondientes. Se propone establecer la obligación expresa de la empresa operadora de informar al abonado sobre las solicitudes presentadas y trámites registrados, tales como: servicios contratados, portabilidad numérica, cambios de titularidad, y reposición de la *SIM Card*. Asimismo, precisar que, la empresa operadora debe informar si el motivo de la falta o inoperatividad del servicio o tarjeta SIM reportada por el usuario obedece a alguna solicitud o trámite registrado.

Artículo 75-B.- Suspensión del servicio por desconocimiento o cuestionamiento de la contratación o reposición de SIM Card. Se propone establecer que la suspensión del servicio por ante la presentación del reclamo por desconocimiento de la contratación del servicio, así como cuando el abonado comunica que desconoce la reposición de la *SIM Card*, se realiza de forma inmediata, al emplear el abonado el canal telefónico o presencial y en el plazo de un (1) día hábil, mediante el uso de un canal distinto. Asimismo, se precisa que, en el caso de contrataciones no solicitadas, la reactivación del servicio se realiza cuando el reclamo se declare infundado, mediante una resolución firme o que hubiere causado estado. Para el caso de desconocimiento de reposición de la *SIM Card*, el servicio se reactiva al efectuarse una nueva reposición de la *SIM Card*.	Conforme se indicó previamente, ante el desconocimiento de la contratación del servicio o reposición de la *SIM Card* por parte del abonado, corresponde la suspensión del servicio, en tanto no se tiene identificada a la persona que viene haciendo uso del mismo, y que habría accedido de forma ilícita y/o sin seguir el procedimiento establecido. En ese sentido, se requiere establecer el plazo en el que se realizaría dicha suspensión preventiva, así como la oportunidad en la que se realizaría la reactivación del servicio. Para tal efecto, se considera que de presentarse el desconocimiento de la contratación o reposición de la *SIM Card* por el canal telefónico o presencial corresponde que se realice de forma inmediata, en tanto existe una interacción directa con el asesor comercial de la empresa operadora, quien tiene acceso a los sistemas comerciales de la empresa y puede ingresar dicho pedido de suspensión del servicio. Cabe indicar que, actualmente se atienden solicitudes de forma inmediata para el caso de reporte de robo o pérdida de equipo terminal, por lo que se advierte que las empresas operadoras cuentan con el desarrollo que permite realizar la suspensión inmediata del servicio. Ahora bien, para el caso de otros canales como el de página web o aplicativo, en los cuales no existe una interacción directa con los asesores comerciales de la empresa operadora, se otorga un plazo de un (1) día hábil. Se propone establecer que la suspensión del servicio ante la presentación del reclamo por desconocimiento de la contratación

OSIPTEL DAPU H.GUSUKUMA

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU M.GONZALEZ

	del servicio, así como cuando el abonado comunica que desconoce la reposición de la *SIM Card*, se realiza de forma inmediata, al emplear el abonado el canal telefónico o presencial y en el plazo de un (1) día hábil, mediante el uso de un canal distinto. Asimismo, se precisa que, en el caso de contrataciones no solicitadas, la reactivación del servicio se realiza cuando el reclamo se declare infundado, mediante una resolución firme o que hubiere causado estado. Para el caso de desconocimiento de reposición de la *SIM Card*, el servicio se reactiva al efectuarse una nueva reposición de la *SIM Card*.
Artículo 121-B.- Información ante trámites cuestionados Se propone establecer la obligación expresa de la empresa operadora de que a solicitud del abonado que desconoce o cuestiona la contratación del servicio, la portabilidad numérica, el cambio de titularidad, y/o la reposición de la *SIM Card*, proporcione la información y documentación relacionada al trámite cuestionado. Se precisa que los plazos de entrega de dicha información y documentación.	En las suplantaciones de identidad en la contratación de servicios, portabilidad numérica, cambio de titularidad, y/o reposición de SIM Card, la persona que figura como titular del servicio requiere realizar acciones ante la Policía Nacional, el Ministerio Público, el Poder Judicial, entidades financieras, entre otras instituciones, a fin de desvincularse respecto del uso realizado del servicio o SIM Card que cuestiona, así como para que se sancione los hechos delictivos ocurridos como el referido a la suplantación de identidad y fraudes financieros. En ese sentido, se propone establecer la obligación expresa de la empresa operadora de que a solicitud del abonado que desconoce o cuestiona la contratación del servicio, la portabilidad numérica, el cambio de titularidad, y/o la reposición de SIM Card, proporcione la información y documentación relacionada al trámite cuestionado.

OSIPTEL DAPU H.GUSUKUMA

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU M.GONZALEZ

Con relación al régimen sancionador se propone modificar los artículos 2, 3 y 4 del “Anexo 5: Régimen de Infracciones y Sanciones” de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, conforme al siguiente detalle:

Propuesta	Fundamento
Se propone incluir como infracción leve el incumplimiento de los artículos 75-B y 121-B que se incorporan a las Condiciones de Uso. Como infracción grave el incumplimiento del artículo 6-C y como muy grave el noveno párrafo del artículo 11-A y el artículo 11-D	Considerando que se propone incluir tres artículos al TUO de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, corresponde establecer que su incumplimiento constituye una infracción administrativa, a fin de disuadir tales incumplimientos. Por tanto, se propone incluir como infracción leve el incumplimiento de los artículos 75-B y 121-B que se incorporan al TUO de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones. El incumplimiento del artículo 6-C se propone incluirlo como infracción grave en tanto se encuentra referido a falta de entrega de información al usuario, cuya tipificación actualmente se encuentra con el mismo nivel de gravedad (Vg. Artículo 6 y 6-B). Del mismo modo, en el caso del párrafo noveno del artículo 11-A se propone establecer su incumplimiento como una infracción muy grave en tanto hace referencia a los párrafos segundo y tercero de dicho artículo que actualmente se encuentran tipificados de esa manera. Finalmente, se modifica la tipificación del incumplimiento del artículo 11-D a infracción muy grave, teniendo en cuenta la relevancia de las obligaciones establecidas.

OSIPTEL DAPU H.GUSUKUMA

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU M.GONZALEZ

Sobre la vigencia de la normativa y demás disposiciones complementarias, se propone lo siguiente:

Propuesta	Fundamento
Se propone que las disposiciones referidas a: considerar solo poderes formales (artículo 2), requerir la exhibición del documento de identidad de forma adicional a la verificación biométrica para servicios móviles (artículo 11), establecer medidas de seguridad para la reposición de SIM Card (numerales 1, 2, 3 y 4 del artículo 67-B), entregar la información y documentación al abonado sobre el trámite cuestionado (artículo 121-B) y proporcionar la contraseña única (artículo 128) entren en vigencia en el plazo de veinte (20) días hábiles desde la publicación de la norma. Las demás disposiciones de la norma se proponen entren en vigencia en el plazo de tres (3) meses desde su publicación.	Teniendo en cuenta que, conforme a lo desarrollado en el presente Informe, se observa un incremento de los fraudes en la contratación del servicio y reposición de SIM Card, se propone que algunas disposiciones del proyecto normativo entren en vigencia en un plazo corto de veinte días hábiles y las demás disposiciones en el plazo de tres meses. Se propone que las disposiciones referidas a: considerar solo poderes formales (artículo 2), requerir la exhibición del documento de identidad de forma adicional a la verificación biométrica para servicios móviles (artículo 11), reglas sobre la captura de la huella dactilar y envío de locución y correo electrónico de forma adicional al mensaje de texto informando sobre altas nuevas (11-A), medidas de seguridad para la reposición de SIM Card (artículo 67-B), entregar la información y documentación al abonado sobre el trámite cuestionado (artículo 121-B) y proporcionar la contraseña única (artículo 128), entren en vigencia en el plazo de veinte (20) días hábiles desde la publicación de la norma. Las demás disposiciones de la norma se proponen entren en vigencia en el plazo de tres (3) meses desde su publicación.
Se propone que en el plazo de tres (3) meses de publicada la norma, la empresa operadora informe al OSIPTEL los supuestos de suspensión temporal y cese definitivo de operaciones del distribuidor autorizado debido a contrataciones no solicitadas, incluidos en los convenios suscritos con sus distribuidores.	Se propone otorgar a las empresas operadoras un plazo de tres meses para suscribir los acuerdos respectivos con sus distribuidores a fin de establecer supuestos de suspensión temporal y cese definitivo ante contrataciones no solicitadas, a fin de generar los incentivos suficientes para que dichos distribuidores cumplan con el procedimiento establecido en la normativa vigente.

OSIPTEL DAPU H.GUSUKUMA

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU M.GONZALEZ

Se propone derogar el numeral 3) del artículo segundo, así como los numerales 1, 2, 3, 4 y 5 del artículo tercero, y el artículo cuarto de la Resolución de Presidencia N° 042-2020-PD/OSIPTEL, mediante la cual se reguló la contratación del servicio y demás trámites durante el periodo de reactivación económica.	Durante el periodo de reactivación económica luego del aislamiento social obligatorio dictado por el Gobierno con la finalidad de evitar la propagación del COVID-19 el OSIPTEL emitió normativa que flexibilizó la contratación y realización de distintos trámites, dado el referido contexto de emergencia sanitaria. No obstante, siendo que actualmente, las actividades económicas se vienen desarrollando con normalidad, sin perjuicio de las medidas sanitarias respectivas, corresponde derogar las disposiciones emitidas en el año 2020, a fin de que no contravengan con la presente propuesta normativa.

La modificación planteada se adjunta en el Anexo I.

9.2. Proporcionalidad del proyecto normativo

Conforme a lo señalado en el presente informe, el proyecto normativo tiene los siguientes beneficios: *(i) evitar el mal uso de los datos personales del abonado por terceros, (ii) evitar los fraudes en las contrataciones y reposición de SIM Card, (iii) evitar la inadecuada o insuficiente información sobre el servicio a contratar, y (iv) facilitar las acciones de supervisión de OSIPTEL*.

- **Con relación a la finalidad pública de "Evitar el mal uso de los datos personales por terceros"**

Los usuarios no tienen cómo corroborar que la persona que le ofrece el servicio y le solicita sus datos personales es un distribuidor autorizado de la empresa operadora. En ese sentido, se requiere que se encuentren debidamente identificados los medios a través de los cuales la empresa operadora realiza la contratación del servicio.

La contratación del servicio debe realizarse por medios que permitan una trazabilidad de la transacción, por lo que si bien en la propuesta normativa se reconocen todas las formas que emplean actualmente las empresas operadoras, se excluye aquella referida a la comercialización del servicio en la vía pública genera por cuanto mayor inseguridad respecto del uso de los datos personales brindados, considerando que no se tiene los controles que se pueden implementar en un ambiente específico, como por ejemplo video cámaras de seguridad, uso de computadores con control de puertos de salida de información, entre otros.

Al respecto, cabe indicar que, en la vía pública los activadores, aun cuando sean autorizados por la empresa operadora, no son supervisados por algún trabajador de esta o del distribuidor, a diferencia de lo que ocurre en los puntos de venta o centros de atención. Así, el riesgo de la vulnerabilidad del uso de datos personales se mitiga realizando la contratación en un punto de venta ubicado en un ambiente específico que se encuentre controlado, donde los trabajadores de la empresa operadora están debidamente identificados y constantemente supervisados por algún encargado del centro de atención o punto de venta, y existen cámaras de seguridad que disuaden a los trabajadores de cometer algún acto ilícito con los datos personales de los usuarios que acuden a contratar un servicio. Ello debido a que, ante un acto fraudulento, se consultarían las cámaras de seguridad y fácilmente se identificaría sí tuvo lugar alguna práctica indebida, procedimiento que no puede llevarse a cabo si la contratación se realiza en la vía pública.

Del mismo modo, el riesgo del mal uso de datos personales se recude en escenarios como en el caso del canal *delivery*, en el cual es el usuario quien se contacta con la empresa, y esta tiene identificada al personal que realizará el *delivery*. Así como en el caso de la autoactivación, en el cual es el usuario quien tiene acceso directo al aplicativo informático de la empresa operadora y por lo tanto no brinda sus datos a personas respecto de las cuales no tiene la certeza de si representan o no a la empresa operadora.

- **Con relación a la finalidad pública de "Evitar los fraudes en las contrataciones y reposición de SIM Card"**

Con relación a dicha problemática, conforme se ha expuesto anteriormente, se han evidenciado diversos testimonios de usuarios, que manifiestan que las contrataciones cuestionadas fueron realizadas en vía ambulatoria.

Lo expuesto también tiene un correlato en las estadísticas expuestas en el presente informe, en las cuales se observa un incremento en las contrataciones no solicitadas, así como en los cuestionamientos de titularidad.

De otro lado, se observa el incremento de reposiciones de *SIM Card* no reconocidas por el abonado, que ha afectado la continuidad en la prestación del servicio y facilitado la comisión de fraudes financieros en perjuicio del abonado.

Ante dicha situación, resulta imprescindible la adopción de medidas que atiendan la problemática. Así las disposiciones propuestas al considerar un registro detallado de los distribuidores, puntos de venta y personal que participa en la contratación, así como requerir la exhibición del documento de identidad para los trámites, y programar la activación de la *SIM Card* después de informar al abonado, entre otras obligaciones, en su conjunto permiten brindar mayor seguridad al proceso de contratación y reposición de *SIM Card*.

- **Con relación a la finalidad pública de "Garantizar una adecuada información sobre el servicio a contratar"**

Conforme se mencionó previamente, la propuesta normativa se reconocen todas las formas que emplean actualmente las empresas operadoras, se excluye aquella referida a la comercialización del servicio en la vía pública por cuanto dicho escenario de venta ambulatoria no garantiza que las empresas operadoras cumplan con brindar a los abonados y usuarios la información necesaria para tomar una decisión de consumo debidamente informada. A diferencia de un punto de venta en el cual ante cualquier duda o problema respecto de la información brindada puede acudir ante el supervisor o jefe del punto de venta para su apoyo. Inclusive el propio local cuenta con información visual disponible para el abonado o usuario (por ejemplo, volantes, banners, paneles, vídeos, etc.)."

Sobre el particular, cuando la contratación del servicio móvil se da en la vía pública, a pesar de que el activador sepa que debe seguir un protocolo para brindar la información pertinente al usuario previamente a que finalice la venta, no hay manera de supervisar que ello efectivamente ocurra. No existen supervisores que vigilen dicho comportamiento *in situ* durante la concreción de la venta del servicio en la vía pública. A diferencia de lo que efectivamente ocurre en los puntos de venta ubicados en ambientes específicos, donde hay supervisores y es fácil comprobar que se está dando la información correcta y pertinente al usuario.

Asimismo, es preciso señalar que, aunque toda la información de los planes se encuentra en el contrato de abonado, en algunos casos disponible en el aplicativo, debe considerar que es el vendedor quien tiene el manejo del equipo a través del cual se realiza la contratación. En ese sentido, aunque las empresas señalen que los protocolos de contratación también lo siguen los activadores del servicio móvil que comercializan en la vía pública, no hay forma de corroborar si el activador informa debidamente al usuario sobre las condiciones y limitaciones del servicio. Incluso, con el objetivo de garantizar la venta, el activador podría brindar información errónea o inexacta al usuario, pues posee un esquema de incentivos que incrementa sus ingresos mientras más contrataciones logre.

Situación distinta ocurre en los casos del canal *delivery*, en el cual es el usuario quien se contacta con la empresa por distintos canales, momento en el cual recibe la información necesaria sobre el servicio a contratar. Así como en el caso de la autoactivación, en el cual es el usuario quien tiene acceso directo al aplicativo

informático de la empresa operadora y por lo tanto la disponibilidad de revisar con mayor detenimiento la información sobre el servicio proporcionada a través de dicho medio.

- **Con relación a la finalidad pública de "Facilitar las acciones de supervisión del OSIPTEL"**

El no contar con puntos de venta o medios a través de los cuales de comercializa el servicio debidamente identificados impide que este Organismo tenga conocimiento de los lugares o medios específicos en los cuales se llevan a cabo las contrataciones de los servicios públicos móviles, dificultando con ello una adecuada programación de las visitas de supervisión inopinadas (sin previo aviso) correspondientes.

En ese sentido, la propuesta normativa contempla diversas reglas tendientes a identificar adecuadamente los medios a través de los cuales la empresa operadora realiza la contratación del servicio, excluyendo aquella referida a la venta ambulatoria, por cuanto, de la experiencia de las acciones de supervisión realizadas por este Organismo en tales casos, los distribuidores o personal a cargo de la contratación del servicio se niegan a identificarse y suscribir las actas respectivas.

Asimismo, en tal escenario no se contaría con información precisa donde puedan acudir los supervisores, podría darse el caso de que estos no encuentren a los activadores para realizar la supervisión, ya que estos podrían estarse movilizando constantemente en el área designada por la empresa operadora, o incluso salirse del perímetro en el que debería realizar sus ventas, dificultando la supervisión, e incluso llegar a imposibilitarla.

De otro lado, cabe señalar que, la excepción de permitir las ferias itinerantes en centros poblados rurales en donde las empresas tengan cobertura estaba justificada por el objetivo del OSIPTEL de incrementar la penetración móvil en las zonas rurales. Al respecto, tal como se argumentó en su momento, los beneficios sociales en estos casos son notables porque están relacionados con el incremento de conectividad en zonas con bajo o nulo acceso al servicio móvil. Ello además que, en esta modalidad de venta no están presentes los problemas identificados por el OSIPTEL para el caso de la venta ambulatoria, toda vez que las ferias tienen una ubicación específica, es posible que haya supervisores que verifiquen el cumplimiento de los protocolos de seguridad para el uso de datos personales y de la entrega de información pertinente al usuario, y el OSIPTEL puede realizar sus supervisiones inopinadas al conocer la dirección exacta de la feria.

Asimismo, es preciso indicar que, la modalidad *delivery* reduciría ciertos riesgos en comparación con las ventas ambulatorias. Al respecto, la modalidad de *delivery* se ha venido incentivando debido a que es el abonado quien requiere el servicio y no es abordado en la vía pública. En tal sentido, el abonado cuenta con mayor información al momento de la contratación.

Por otra parte, previo a la exigencia de la verificación biométrica de huella dactilar, la comercialización, contratación y activación de las líneas móviles prepago (y las líneas móviles en general) se regían de acuerdo a lo previsto en el artículo 11 del TUO de las Condiciones de Uso (antes artículo 8º de las Condiciones de Uso), el cual –en línea con lo establecido en el Decreto Supremo Nº 023-2010-MTC- disponía lo siguiente:

*"**Artículo 11.- Registro de abonados de acuerdo a la modalidad de contratación del servicio***

La empresa operadora se encuentra obligada a llevar un registro debidamente actualizado de los abonados que hubieran contratado servicios bajo la modalidad prepago, control y/o postpago.

Cada registro deberá ser independiente, debiendo contener como mínimo: (i) Nombre y apellidos completos del abonado; (ii) Número y tipo de documento legal de identificación del abonado, debiendo incluirse únicamente el Documento Nacional de Identidad, Carné de Extranjería, Pasaporte o Registro Único de Contribuyentes, los mismos que deberán contener el número y/o la serie de dígitos que correspondan para cada tipo de documento; y, (iii) Número telefónico o de abonado, para el caso de los servicios de telefonía fija y servicios públicos móviles; o número de contrato o de identificación del abonado, en los demás casos.

La información señalada en los numerales (i) y (ii) antes indicados, deberá ser solicitada al abonado al momento de la contratación, debiendo exigirse la exhibición y copia del documento legal de identificación del abonado, con la finalidad que la empresa operadora, en dicha oportunidad, proceda a registrar los datos personales del abonado a través de los mecanismos que hubiera dispuesto para tal fin, debiendo la empresa operadora informar al OSIPTEL acerca de los referidos mecanismos, así como sobre la seguridad de los mismos.

La presentación de la copia del documento legal de identificación del abonado, podrá realizarse sobre papel o cualquier otro soporte que permita su almacenamiento y conservación por parte de la empresa operadora.

La empresa operadora, bajo responsabilidad, sólo podrá instalar y/o activar el servicio, una vez que la información proporcionada por el abonado sea incluida en el registro correspondiente. (…)"

Como se puede advertir, el segundo párrafo del referido artículo 11 del TUO de las Condiciones de Uso establecía, expresamente, que la activación del servicio se efectúe sólo luego de incluida la información proporcionada por el abonado de sus datos personales en el registro respectivo (en el presente caso en el Registro de Abonados Prepago); para lo cual, al momento de la contratación, la empresa debía solicitar la información de nombre y apellidos completos, número y tipo de documento legal de identificación del abonado, así como, exigir la exhibición y copia del documento legal de identificación del abonado. Por tanto, el requisito mínimo que debían presentar los usuarios para adquirir una línea móvil prepago era exhibir su documento de identidad y alcanzar una copia del mismo.

Al respecto, este Organismo verificó el incumplimiento de las obligaciones establecidas en el artículo 8 de las Condiciones de Uso (posterior artículo 11 del TUO de las Condiciones de Uso), por lo que **el 29 de abril de 2011** la entonces Gerencia de Fiscalización y Supervisión (GFS) actual Dirección de Fiscalización e Instrucción (DFI) dispuso el inicio de procedimientos administrativos sancionadores a cada una de las empresas móviles, América Móvil Perú S.A.C. (América Móvil), Telefónica Móviles S.A. (Telefónica Móviles) y Nextel del Perú S.A. (Nextel), imponiendo la Gerencia General con fecha 10 de octubre de 2011, multas de ciento cincuenta (150) unidades impositivas tributarias (UIT) por el incumplimiento de las obligaciones referidas al procedimiento de

contratación de líneas. Asimismo, sancionó con una multa de setenta y cinco (75) UIT a América Móvil y Telefónica Móviles, y con una amonestación a Nextel, por el incumplimiento de sus obligaciones referidas a la difusión sobre el procedimiento de contratación.

Luego de ello, el **21 de octubre del año 2011** se notificaron las Resoluciones de Gerencia General N° 499-2011-GG/OSIPTEL, N° 498-2011-GG/OSIPTEL y N° 500-2011- GG/OSIPTEL, mediante las cuales se impusieron medidas correctivas a fin que las empresas móviles adecúen su conducta a lo dispuesto en el artículo 8 del TUO de las Condiciones de Uso.

En **diciembre del año 2011**, ante la verificación del incumplimiento de dichas medidas correctivas se sancionó a América Móvil, Telefónica Móviles y Nextel, respectivamente, con una multa de ciento cincuenta y un (151) UIT19 y se dispuso la imposición de multas coercitivas, en caso se verifique que la conducta infractora se mantiene.

Como consecuencia de ello, **se impusieron tanto a Telefónica Móviles como a América Móvil un total de once (11) multas coercitivas a cada una de ellas, y a Nextel dos (02) multas coercitivas**, las cuales no superaron el monto de cincuenta (50) UIT, considerando que es el límite máximo permitido por el artículo 65 del Reglamento General de Infracciones y Sanciones (RGIS), aprobado por Resolución N° 002-99-CD/OSIPTEL, actualmente derogado.

En ese sentido, **entre el año 2011 a 2014 se impusieron 9 multas y 24 multas coercitivas a las empresas operadoras móviles, por no seguir el procedimiento de contratación establecido y su difusión.**

Pese a las medidas sancionadoras y de coerción, impuestas por el OSIPTEL, descritas en los párrafos precedentes, se observó que las empresas operadoras continuaban incumpliendo tales obligaciones.

Los factores que influyeron en que dicha conducta se mantenga, fueron el esquema de comercialización establecido por las empresas operadoras, en el cual la alta capilaridad de sus distribuidores y sub-distribuidores con los cuales la empresa operadora no llegaba a tener alguna vinculación, dificultaba el control del cumplimiento de la exigencia de la exhibición del documento de identidad, así como, que la conservación de la copia del documento identidad como medida de seguridad resultaba altamente vulnerable.

Por tanto, **existió una medida menos gravosa en la cual sólo se estableció la exigencia de exhibición y copia de DNI; sin embargo, dado el esquema de comercialización implementado por las empresas operadoras (alta capilaridad de distribuidores y subdistribuidores con los cuales la empresa no llegaba a tener una vinculación como por ejemplo bodegas, kioskos, ambulantes, etc) y el ahorro de costos en los controles respectivos, no resultó eficaz.**

En ese sentido, las reglas consideradas en la propuesta normativa apuntan a una comercialización formal de este servicio, lo que no puede alcanzarse si se permite que la contratación se realice en forma ambulatoria o en la vía pública, pues imposibilita el efectivo control por OSIPTEL y la Policía Nacional.

Otro de los objetivos del OSIPTEL y hacia donde se vienen orientando sus políticas es promover el uso del canal digital, por lo que se reconocen los nuevos mecanismos de contratación de autoactivación.

10. DIFUSIÓN Y PARTICIPACIÓN DE LOS AGENTES INVOLUCRADOS

Mediante las cartas C.3801-DAPU/2021, C.3802-DAPU/2021, C.3803-DAPU/2021 y C.3804-DAPU/2021 de fecha 31 de agosto de 2021, se recomendó a las empresas un procedimiento para brindar mayor seguridad en las contrataciones de servicio, así como reposiciones de *SIM Card*, siendo algunas de dichas disposiciones consideradas en la propuesta normativa.

Al respecto, mediante las siguientes comunicaciones las empresas operadoras presentaron sus comentarios al referido procedimiento:

- Carta N° 791-2021/DL recibida el 03.09.2021, remitida por Viettel Perú S.A.C.
- Carta N° DMR-CE/N°2167/21 recibida el 07.09.2021, remitida por América Móvil Perú S.A.C.
- Carta N° CGR-2305/2021 recibida el 07.09.2021, remitida por Entel Perú S.A.
- Carta N° TDP-2973-AR-GER-21 recibida el 09.09.2021, remitida por Telefónica del Perú S.A.A.

En atención a lo solicitado por la empresa Viettel Perú S.A.C., Telefónica del Perú S.A.A. con fecha 08.09.2021 y 09.09.2021, respectivamente, se llevó a cabo una reunión virtual a fin de evaluar las medidas recomendadas por este Organismo para brindar mayor seguridad en la contratación y reposición de *SIM Card*.

De otro lado, se debe indicar que la propuesta de norma preliminar fue alcanzada a las distintas Unidades Orgánicas del OSIPTEL; a efectos que brinden sus comentarios a la misma. Cabe indicar que se analizaron los comentarios recibidos, los cuales han sido incorporados en la presente propuesta de norma, la misma que será publicada para comentarios.

Asimismo, mediante carta C.3232-DAPU/2021, este Organismo comunicó al Banco de la Nación la problemática sobre fraudes en la contratación y/o reposición de SIM Card del servicio público móvil, motivados por fraudes financieros. En ese sentido, con fecha 03.09.2021 se llevó a cabo una reunión con funcionarios del OSIPTEL y personal gerencial del Banco de la Nación.

11. CONCLUSIONES

En atención a lo expuesto, se concluye lo siguiente:

11.1. En el primer semestre del año 2021, se presentaron cerca de 23 007 reclamos por contratación no solicitada, de los cuales 8765 resultaron fundados, es decir, hay 6.6 resoluciones fundadas por cada 10 000 contrataciones. No obstante, se debe señalar que este indicador de incidencia solo considera las contrataciones no solicitadas que se presentaron como reclamos, y no incluye los casos que no han sido denunciados o reportados. Al respecto, resulta importante considerar que, según la Encuesta de Satisfacción 2020, solo el 27% de los usuarios que experimenta un inconveniente formula su reclamo.

11.2. En el primer semestre del 2021, se reportaron al OSIPTEL 1220 denuncias de usuarios respecto a contrataciones no solicitadas en el servicio público móvil, el 53% de los casos está relacionado con altas nuevas, el 15% con la portabilidad no solicitada, 23% con migraciones de plan tarifario no autorizados y 8% en los que se hizo el cambio de titularidad. Asimismo, considerando solo los 1121 casos de altas nuevas, portabilidad no solicitadas y migraciones, las empresas

operadoras con mayor cantidad con este tipo de problema son Telefónica con el 44% del total, seguido de Entel, América Móvil y Viettel con el 27%, 20 y 8%, respectivamente.

Si bien los casos reportados al OSIPTEL son un subconjunto del total de usuarios que formularon un reclamo y de los usuarios que no denunciaron, se trata de casos que implican una mayor gravedad, debido a que han significado para los usuarios algún tipo de pérdida económica o se han visto involucrados en procesos judiciales. Se debe destacar los casos de las usuarias Guicela Taboada Campos y Eliana Ramos quienes fueron vinculadas con procesos judiciales; el caso del señor Gil de la Cruz, quien manifestó que la empresa Telefónica le ha realizado recargos por planes que no solicitó y el caso del señor Eulalio Máximo Torres Pariona, quien fue sentenciado a 14 años de pena privativa de libertad por cuanto se vio involucrado con la comisión de un delito de robo agravado, siendo que los asaltantes dejaron en su huida un celular que habría tenido contacto con una línea móvil que figurada bajo su titularidad.

11.3. De enero a agosto de 2021, se reportaron al OSIPTEL 394 casos de fraude financiero mediante la suplantación del abonado o representante en los trámites de reposición de SIM card o cambio de titularidad; de los cuales 120 casos tuvieron por objetivo robar los bonos de S/ 600, otorgados por el gobierno, mientras que el resto de fraudes (274 casos) se dirigieron a apoderarse de las cuentas bancarias de las víctimas. En este segundo tipo de casos, la pérdida promedio ha sido de S/ 10 065 en el caso de 23 usuarios. Adicionalmente, la empresa Viettel reportó 40 denuncias con una pérdida promedio de S/ 7113.

Por otra parte, es importante considerar que estos casos de fraude financiero generan una considerable afectación individual, como en el caso del señor Augusto Trelles Velásquez que perdió más de veinte mil soles, las profesoras Solange Palacios, Yesica Caituro y Diana Chero Pacheco que también fueron víctimas de este tipo de fraudes, entre otros. Se ha confirmado que detrás de todos estos delitos se encuentran bandas delincuenciales e incluso es posible que haya cómplices infiltrados dentro de las áreas de atención al usuario de las empresas operadoras.

11.4. Se han identificado cinco posibles causas de la problemática antes señalada: (a) inadecuadas prácticas en la contratación de líneas móviles; (b) bajos incentivos por parte de las empresas para adoptar soluciones efectivas; (c) información sensible en los equipos terminales móviles; y (d) limitado conocimiento de los usuarios sobre sus deberes y derechos y (e) vulnerabilidad de la verificación biométrica por existencia de bandas criminales organizadas.

En relación con las inadecuadas prácticas comerciales, se debe señalar que el principal factor es la venta chip y la realización de trámites en la vía pública. A partir de las diversas acciones de monitoreo y supervisión se ha podido identificar que los vendedores contratados por las empresas operadoras o por los distribuidores no cumplen con realizar adecuadamente la verificación de la identidad de los solicitantes, y en algunos casos inducen a error a los usuarios. Asimismo, que se han presentado varios reclamos en los que los usuarios señalan que, en la calle, un asesor de la empresa le había regalado el chip sin indicar que estaba contratando un plan postpago o que le habían hecho pasar la verificación biométrica y no le habían entregado la línea, con el objetivo de usar esa línea con otros fines.

11.5. Con la finalidad de dar solución a los problemas presentados, se analizaron dos alternativas de solución, mediante un análisis multicriterio (AMC), que consideró 4 atributos de comparación: facilidad de implementación, reducción de la afectación de los usuarios, manejo del riesgo y trazabilidad. Como resultado, se determinó que la alternativa 2 es la mejor opción para mitigar la ocurrencia de contrataciones no solicitadas y fraudes financieros. Esta alternativa contempla lo siguiente:

(i) Medidas para la identificación temprana de las solicitudes aprobadas sin el consentimiento del abonado:

- Informar al usuario acerca de las solicitudes presentadas a su nombre.
- Suspender el servicio cuando se desconozca la contratación.
- Facilitar el acceso a la información de la contratación o reposición no reconocida.

(ii) Medidas para la identificación de intentos de reposición fraudulenta:

- Implementar preguntas de validación de identidad.
- Envío de SMS, locución y correo electrónico hasta en 2 oportunidades.
- Exhibir el documento de identidad en el caso de un trámite con representante.
- La activación de la SIM card se realizará a las 4 horas de aprobada la solicitud.
- Enviar SMS y correo en el caso de intentos fallidos.

(iii) Reglas de seguridad en los canales de comercialización:

- Se puede contratar con distribuidores autorizados por la empresa y reportados al OSIPTEL, y en el punto de venta con dirección específica.
- Códigos de identificación al distribuidor y personal encargado.
- Antes de la contratación, el distribuidor debe pasar por la verificación biométrica o usar contraseña.
- Registro de distribuidores que permita la trazabilidad del trámite.
- La empresa debe establecer supuestos de suspensión o cese de distribuidores que realizan contrataciones no solicitadas.
- Las ferias itinerantes solo se permiten en centros poblados rurales sin oficina, centro de atención o punto de venta, o en otras ferias itinerantes autorizadas previamente por el OSIPTEL y donde la empresa disponga de cobertura.
- Para la auto-activación, el SIM card se entrega de manera personal en la dirección indicada con la exhibición del documento de identidad y con la captura de la imagen del solicitante.

- La empresa debe comunicar, el último día hábil de cada mes, el registro de los establecimientos que brindan auto-activación.
- La contratación del servicio público móvil se puede realizar mediante el canal telefónico usando la contraseña única.
- La empresa debe tener identificado y registrado el canal o medio a través del cual se contrató el servicio y el distribuidor o personal que participó en la contratación, así como el medio por el cual validó la identidad del abonado y se adquirió el SIM card.

(iv) Reglas de seguridad para los trámites con representantes

- Un representante ya no podrá ser acreditado con carta simple, copia de DNI y recibo de pago, dado que será obligatorio tener un poder legalizado por notario.
- El representante debe realizar la verificación biométrica para todo servicio y trámite.

(v) Reglas de seguridad para la verificación de la huella dactilar

- Se limita a un máximo de 5 intentos por transacción.
- Además del SMS, se debe enviar una locución y correo electrónico.

12. RECOMENDACIONES

Se recomienda elevar al Consejo Directivo del OSIPTEL el presente informe sustentatorio y la propuesta normativa respectiva, con la finalidad de que sea publicado para comentarios de los interesados.

Atentamente,

Firmado digitalmente por:PICCINI ANTON Tatiana Mercedes FAU 20216072155 soft

OSIPTEL DAPU H.GUSUKUMA

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU M.GONZALEZ

REFERENCIAS

ACMA (2020), Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standar 2020.

Coase, Ronald H. (1937) 'The Nature of the Firm', 4:16 *Econometrica* 386–405

FCC (2020), Notice of Proposed Rulemaking: Rules to Prevent SIM Swapping and Port-Out Fraud

Fisher, Irving (1912). The Nature of Capital and Income, Macmillan, New York.

GSMA (2019a). Mitigating common fraud risks Best practices for the mobile money industry, GSMA Association.

GSMA (2019b). Access to Mobile Services and Proof of Identity 2019: Assessing the impacto on digital and financial inclusion, GSMA Association.

INEI (junio 2021). *Informe Técnico N° 2: Estadísticas de Seguridad Ciudadana*, Lima.

ISO 31000:2009. *Risk management – Principles and guidelines*, Geneva.

ITU-FIGI (2019), Technical reporto on SS7 vulnerabilities and mitigation measures for digital services transactions

Knight Frank, H. (1921). Risk, uncertainty and profit. *книга*.

Lamont, J. (2020). CRTC, carriers refuse to share data about SIM hijacking and preventions efforts. Recuperado de: https://mobilesyrup.com/2020/10/24/crtc-telecom-refuse-share-data-sim-hijacking-prevention-efforts/

Lee, K., Kaiser, B., Mayer, J., & Narayanan, A. (2020). An Empirical Study of Wireless Carrier Authentication for SIM Swaps. In *Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020)* (pp. 61-79).

Neumann, John von y Morgenstern, Oskar (1944). Theory of Games and Economic Behavior, Princenton University Press, Princenton.

OECD. Publishing. (2010). *Risk and regulatory policy: Improving the governance of risk*. Organisation for Economic Co-operation and Development.

Oehler, A., Herberger, T., Wendt, S., & Höfer, A. (2015). Risk assessment and risk management in economics. In *Risk and EU law*. Edward Elgar Publishing.

UN. (2013). *Risk management in regulatory frameworks: towards a better management of risks*. UN

Savage, Leonard J. (1954). The Foundations of Statistics, Wiley, New York.

Simon. Herbert A. (1956), 'A Behavioral Model of Rational Choice', 69:1 *Quarterly Journal of Economics* 99–118; *id.*, 'Rational Choice and the Structure of Environments' (1956) 63:2 *Psychological Review* 129–138.

Squire Technologies (2020), Winning the war on Telecom Fraud, recuperado de https://squire-technologies.com/docs/Winning_The_War_On_Telcom_Fraud.pdf

Tamas K. (2021a), 11 Types of Communications Fraud: How to Detect & Prevent it., recuperado de: https://seon.io/resources/telecommunications-fraud-detection-and-prevention/?utm_term=&utm_campaign=%5BS%5D Blog - dynamic %5BLAT…

Tamas K. (2021b), 5 Fraund Trends We'll Be Keeping an Eye Pn in 2021, recupeado de: https://seon.io/resources/5-fraud-trends-well-be-keeping-an-eye-on-in-2021/

Williamson, Oliver E. (1985), *The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting*

ANEXO N° 1: DESCRIPCIÓN DE RIESGOS

Proceso donde se identifica el riesgo	Canal identificado	Activo comprometido	Amenaza	Vulnerabilidad	Consecuencias	Valoración del control actual por parte de las empresas
Cambio de Titularidad	Presencial Telefónico Ambulante	Línea de servicio	Pérdida de la titularidad de la línea	Falta de control en la tramitación con representante	La línea móvil puede ser utilizada con fines delictivos	Deficiente, dado que las empresas no facilitan la información sobre las suplantaciones, ni brindan apoyo a las víctimas. No se puede determinar si hay distribuidores o asesores cómplices o el grado de su negligencia. Los usuarios se enteran de manera tardía de las suplantaciones.
				Uso de huellas clonadas en la verificación biométrica		
Adquisición de línea	Presencial Telefónico Ambulante		Adquisición de una línea por parte de un desconocido	Falta de control en la tramitación con representante	La línea móvil puede ser utilizada con fines delictivos	
				Uso de huellas clonadas en la verificación biométrica	El usuario puede terminar con deudas por líneas móviles que no usa	
				Dificultad para verificar la identidad del asesor, sobre todo cuando la venta es ambulatoria	Pueden usar la línea móvil para hacer trámites a nombre del usuario	
Reposición de Chip	Presencial Telefónico Ambulante		Pérdida temporal del control de la línea del usuario	Falta de control en la tramitación con representante	La línea móvil puede ser utilizada con fines delictivos	
				Uso de huellas clonadas en la verificación biométrica	El estafador puede ingresar a sus cuentas bancarias y robar al usuario	

ANEXO N° 2: PROPUESTA NORMATIVA

Artículo Primero. - Modificar los artículos 2, 11, 11-A, 11-D, 67-B, 71, 118, 119 y 128 del Texto Único Ordenado de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, aprobado mediante Resolución de Consejo Directivo N° 138-2012-CD/OSIPTEL, conforme al siguiente texto:

"**Artículo 2.- Derecho de los abonados y usuarios**

Los abonados podrán ejercer todos los derechos que esta norma regula. Los usuarios pueden ejercer los derechos que establece la presente norma, salvo los derechos relativos a: (i) la modificación o extinción del contrato de abonado; (ii) la modificación de los sistemas o modalidades tarifarias; y, (iii) la contratación de servicios suplementarios, adicionales y demás prestaciones contempladas en la presente norma.

Para el ejercicio de los derechos que la presente norma regula, el abonado podrá actuar mediante representante. En estos casos, el representante deberá presentar la correspondiente solicitud, mediante documento escrito o a través de los medios informáticos o electrónicos que hubiera implementado la empresa operadora, debiendo adjuntar adicionalmente el poder respectivo.

Para el caso de representante de una persona natural, será suficiente el otorgamiento del poder con firma legalizada ante notario público.

Para el caso de representante de una persona jurídica, adicionalmente se requerirá copia simple de: (i) la vigencia del poder del representante, y (ii) el documento legal de identificación del representante (Documento Nacional de Identidad, Carné de Extranjería). Este representante, a su vez, podrá designar a un tercero utilizando la formalidad a la que se hace referencia en el párrafo anterior.

El representante no podrá ejercer los derechos que la presente norma regula mediante vía telefónica, salvo el representante de persona jurídica en el caso que la empresa operadora haya implementado la utilización de la contraseña a la que hace referencia el artículo 128 para validar la identidad del abonado o solicitante del servicio.

Los derechos contenidos en la presente norma no serán aplicables a aquellas personas que:

(i) Hubieran accedido a los servicios públicos de telecomunicaciones a través de medios fraudulentos u otros no permitidos por el ordenamiento legal; o,
(ii) Hubieran accedido a los equipos terminales a través de medios fraudulentos u otros no permitidos por ley."

"**Artículo 11.- Registro de abonados de acuerdo a la modalidad de contratación del servicio**

La empresa operadora debe verificar la identidad del solicitante de la contratación del servicio, para lo cual debe exigirse la exhibición del documento legal de identificación del abonado.

En el caso de personas jurídicas la verificación de identidad se realizará a través de su representante, sin perjuicio de la aplicación de lo dispuesto en el artículo 2.

La carga de la prueba de la verificación de identidad del solicitante es de la empresa operadora.

No es necesario que la empresa operadora exija la exhibición de documento legal de identificación, en los siguientes casos:

1. En la contratación de servicios de distribución de radiodifusión por cable bajo la modalidad prepago, servicios de larga distancia y servicios de interoperabilidad.

2. **En la contratación de servicios públicos móviles por mecanismos no presenciales de autoactivación señalados en el numeral 6 del artículo 11-D, cuando la validación de identidad se realice utilizando el sistema de verificación biométrica de huella dactilar mediante tecnología de detección de huella viva.**

Asimismo, la empresa operadora debe llevar un registro actualizado de los abonados que hubieran contratado servicios bajo la modalidad prepago, control y/o postpago.

Cada registro debe ser independiente, debiendo contener como mínimo:

N°	Contratante Persona Natural	Contratante Persona Jurídica
(i)	Nombre y apellidos completos del abonado	Razón social
(ii)	Nacionalidad del abonado	Registro Único de Contribuyentes (RUC)
(iii)	Número y tipo de documento legal de identificación del abonado, de acuerdo al siguiente detalle: • Nacionales: Documento Nacional de Identidad. • Extranjeros: Carné de Extranjería, Pasaporte o el documento legal de identidad válido requerido por la Superintendencia Nacional de Migraciones.	Nombre y apellidos completos, número y tipo de documento legal de identificación del representante legal, de acuerdo al siguiente detalle: • Nacionales: Documento Nacional de Identidad. • Extranjeros: Carné de Extranjería, Pasaporte o el documento legal de identidad válido requerido por la Superintendencia Nacional de Migraciones.
(iv)	• Servicios de telefonía fija y servicios públicos móviles: número telefónico • Demás servicios: número de contrato o de identificación del abonado.	
(v)	Fecha y hora de instalación y/o activación del servicio	
(vi)	Reporte de verificación biométrica (de aplicar)	

La empresa operadora, bajo responsabilidad, sólo puede instalar y/o activar el servicio, una vez que la información proporcionada por el abonado sea incluida en el registro correspondiente, previa verificación de identidad del solicitante."

"**Artículo 11-A.- Verificación de identidad del solicitante del servicio público móvil y para la contratación de servicios públicos móviles**

Salvo las excepciones previstas en el artículo 11-C y el numeral 1 del artículo 11, las empresas operadoras **del servicio público móvil** están obligadas a verificar la identidad del solicitante del servicio, mediante el uso del sistema de verificación biométrica de huella dactilar, el cual consiste en verificar la correspondencia de la impresión dactilar capturada con la información que obra en la base de datos biométrica del RENIEC.

Para tal efecto, se emplea la mejor huella registrada en el RENIEC y lectores biométricos que cumplan con las especificaciones técnicas requeridas por dicha entidad. **El número máximo de intentos de verificación biométrica por persona en el día es de cinco (5), por transacción, para lo cual la empresa operadora debe realizar la configuración correspondiente en sus sistemas y/o equipos**. **Previo a la captura de la huella dactilar, la empresa operadora debe verificar que la mano del solicitante del servicio o representante se encuentre libre de cualquier elemento externo que pueda adulterar o invalidar la verificación. Ante la negativa del solicitante del servicio o representante, la empresa operadora debe suspender el trámite, informando el motivo.**

La empresa operadora debe conservar y almacenar el reporte de la verificación cuyo resultado ha sido confirmado por el RENIEC, durante el plazo establecido en el tercer párrafo del artículo 9. El reporte de verificación es el resultado proporcionado por el RENIEC una vez efectuada la consulta, el cual contiene la siguiente información:

(i) Los nombres, apellidos y número del documento nacional de identidad del solicitante del servicio **o su representante**, respecto del cual se ha realizado la consulta.
(ii) La fecha y hora de la consulta ante el RENIEC.
(iii) El resultado de la consulta realizada al RENIEC.
(iv) ID de transacción de la consulta RENIEC.

El resultado de estas verificaciones debe guardar coincidencia con la información que obre en el RENIEC. De existir coincidencia, debe incluir dicha información en el Registro de Abonados y proceder a la activación del servicio.

La empresa operadora debe remitir inmediatamente **a la activación del servicio** un mensaje de texto y **una locución a cada una de las líneas móviles que el abonado tiene registrado con su documento legal de identificación en dicha empresa,** así como **un correo electrónico a la dirección electrónica registrada por el abonado.** El mensaje deberá contener como mínimo, información relativa: (a) el número del documento legal de identificación del abonado, (b) el número telefónico o de abonado del servicio contratado, (c) la modalidad de contratación del nuevo servicio, y (d) el derecho del abonado a reclamar o cuestionar la titularidad, en caso desconozca la contratación del servicio.

En los casos que el abonado sea una persona jurídica, la información a que se refiere el párrafo anterior podrá ser remitida utilizando cualquier otro medio alternativo propuesto por la empresa operadora, siempre que el abonado haya expresado su consentimiento para ello.

Adicionalmente, en caso el abonado sea persona natural y cuente con diez (10) servicios públicos móviles bajo su titularidad en una misma empresa operadora, la contratación de nuevos servicios públicos móviles, sea bajo la modalidad prepago, control o postpago, la empresa operadora debe:

1. Realizar la contratación en sus oficinas o centros de atención.
2. Solicitar una declaración jurada de la persona natural en la que indique, su compromiso de:
(i) No destinar el(los) servicio(s) a la reventa o comercialización.
(ii) Realizar el cambio de titularidad del servicio, cuando corresponda.

La carga de la prueba del cumplimiento de las reglas previstas en este artículo es de la empresa operadora.

Las disposiciones establecidas en el segundo y tercer párrafo aplican para todos los trámites y servicios en los cuales se realice la verificación biométrica de huella dactilar".

"**Artículo 11-D.- Contratación de servicios a través de los distintos canales**

La empresa operadora es responsable de todo el proceso de contratación del servicio que provea, que comprende la identificación y el registro de los abonados que contratan sus servicios, independientemente del canal o medio de atención o comercialización.

La contratación del servicio se realiza en los centros de atención, en la dirección específica del punto de venta previamente reportado al OSIPTEL, mediante el canal telefónico, de forma virtual o en la dirección indicada por el solicitante del servicio y excepcionalmente en ferias itinerantes, aplicando las siguientes disposiciones:

1. **La persona natural que interviene en cada contratación del servicio, sea el personal del centro de atención o punto de venta, el distribuidor autorizado o su personal u otro, valida su identidad mediante verificación biométrica de huella dactilar o con el uso de una contraseña, previo a la contratación.**

2. **Los puntos de venta pueden ser gestionado por la empresa operadora o distribuidor autorizado.**

3. **En el caso de distribuidores solo se puede contratar el servicio ante aquellos que se encuentren previamente autorizados por la empresa operadora y reportados al OSIPTEL y en el punto de venta con dirección específica registrada conforme al presente artículo.**

La empresa operadora otorga un código único que identifique al distribuidor autorizado, así como al punto de venta habilitado para realizar las contrataciones, y al personal que depende del distribuidor y participa directamente en la contratación del servicio.

La empresa operadora debe remitir al OSIPTEL el registro de distribuidores autorizados, **el cual contiene:**

a) **Nombres y apellidos o razón social del distribuidor, tipo y número de documento de identidad del distribuidor y** el código único del distribuidor.
b) **Código único de cada punto de venta del distribuidor, fecha de inicio de operaciones de cada punto de venta, dirección específica de cada punto de venta del distribuidor en los cuales éste se encuentra habilitado por la empresa operadora a realizar la contratación del servicio, con el detalle del distrito, provincia, departamento y ubicación georeferenciada.**
c) **Nombres, apellidos, tipo y número de documento de identidad del personal del distribuidor que interviene en la contratación, el código único que identifica a dicho personal.**

Dicho registro también incluye la información de aquellos centros de atención, y puntos de venta gestionados sin la intervención de un distribuidor autorizado. Para tal efecto, se omite la información registrada en el literal a), y se precisa que se trata de centros de atención, o puntos de venta gestionados directamente por la empresa operadora.

La empresa operadora debe comunicar al OSIPTEL cualquier modificación en el referido registro, el último día hábil de cada semana, al correo electrónico distribuidores_autorizados@osiptel.gob.pe. El OSIPTEL puede solicitar el registro de dicha información por otro medio o soporte electrónico.

La empresa operadora establece supuestos de suspensión temporal y cese definitivo de operaciones del distribuidor autorizado debido a contrataciones no solicitadas.

4. **En el caso de contrataciones en ferias itinerantes, estas se llevan a cabo solo en centros poblados rurales o en provincias en las cuales no cuenta con oficinas y/o centros de atención o puntos de venta, o en otras ferias itinerantes autorizadas previamente por el OSIPTEL. En ambos casos la empresa operadora debe contar con cobertura y la autorización municipal respectiva. La empresa operadora informa al OSIPTEL, con una anticipación de diez (10) días hábiles, las fechas y lugares donde se llevarán a cabo. Esta información debe ser reportada al correo electrónico distribuidores_autorizados@osiptel.gob.pe.**

5. **En el canal de comercialización del servicio mediante entrega a domicilio *(delivery),* la empresa operadora tiene identificado al personal que participa en la contratación, validación de identidad y/o realiza la entrega del SIM Card al solicitante del servicio. Para lo cual lleva un registro**

actualizado con el detalle que indica el literal c) del numeral 2. Para el uso de este canal, el solicitante debe requerir el servicio a través del canal telefónico, página web u otro canal virtual de la empresa operadora, brindando los datos señalados en los numerales (i), (ii) y (iii) del artículo 11, así como la dirección en la cual se solicita el *delivery* y otros datos de contacto. El SIM Card es entregado únicamente de manera personal por la empresa operadora en la dirección indicada por el solicitante del servicio público móvil, para lo cual la empresa operadora requiere la exhibición del documento de identidad del solicitante del servicio, debiendo conservar la captura de la imagen del mismo como constancia de su exhibición.

6. **En caso el SIM Card sea adquirido en establecimientos comerciales para posterior auto-activación, la empresa operadora debe tener un registro de tales establecimientos, con el nombre comercial y razón social del establecimiento comercial, la dirección específica de cada uno de ellos, con el detalle del distrito, provincia y departamento, así como el código designado del establecimiento comercial en el cual se adquiere el SIM Card. La activación del servicio público móvil mediante SIM Card adquirido en establecimientos comerciales se limita a una sola activación o portabilidad numérica en el mes por el abonado.**

   La empresa operadora debe comunicar dicha información al OSIPTEL o cualquier modificación en el referido registro, el último día hábil de cada mes, al correo electrónico distribuidores_autorizados@osiptel.gob.pe. El OSIPTEL puede comunicar el registro de dicha información por otro medio o soporte electrónico.

7. **La contratación de nuevos servicios por el canal telefónico de la empresa operadora no aplica para el servicio público móvil.**

La empresa operadora debe tener identificado y registrado el canal o medio a través del cual se contrató el servicio y el distribuidor o personal que participó en la contratación, así como el medio por el cual se validó la identidad del abonado y se adquirió el SIM Card, conforme al presente artículo.

La empresa operadora tiene la carga de la prueba de la validación de identidad exitosa de la persona natural que interviene en la contratación de cada uno de sus servicios.

"**Artículo 67-B.- Reposición de SIM Card y recuperación de número telefónico o de abonado del servicio público móvil**

La reposición de SIM Card se rige conforme a las siguientes disposiciones:

1. A solicitud del abonado, la empresa operadora de los servicios públicos móviles, está obligada a proporcionar un nuevo SIM Card asociado al número telefónico o de abonado cuya titularidad lo identifique como tal, cuando se haya reportado previamente la sustracción o pérdida del equipo terminal, o en los casos que el

SIM Card haya sido extraviado, presente fallas que ocasionen la inoperatividad del servicio, o se requiera un nuevo modelo de SIM Card.

2. **Esta solicitud debe ser presentada en forma personal por el abonado, en cualquiera de las oficinas o centros de atención de la empresa operadora y los puntos de venta o atención habilitados en virtud a lo dispuesto en el tercer y cuarto párrafo del artículo 43, previamente reportados al OSIPTEL.**

3. En todos los casos, la empresa operadora debe verificar la identidad del abonado únicamente mediante el sistema de verificación biométrica de huella dactilar y exhibición del documento nacional de identidad; o, en el caso de las excepciones previstas en el artículo 11-C, con el documento legal de identificación, en cuyo caso, la empresa operadora deberá conservar y almacenar una copia del mencionado documento. **Asimismo, como medida de seguridad complementaria, para validar la identidad del abonado, la empresa operadora debe aplicar el procedimiento previsto en los numerales i) y ii) de la sección 3 de los lineamientos aprobados por Resolución N° 002-2021-GG/OSIPTEL o la disposición que la modifique. Para tal efecto, la empresa debe registrar y conservar las constancias de las preguntas realizadas y las respuestas obtenidas de dicha validación.**

4. Cuando la referida solicitud sea presentada por representante, la empresa operadora debe exigir el otorgamiento de poder con firma legalizada ante notario público **y validar su identidad mediante verificación biométrica y exhibición de su documento de identidad**.

5. **Previo a la activación del nuevo SIM Card, la empresa operadora debe enviar un mensaje de texto y una locución a todos los servicios móviles bajo titularidad del abonado registrados en dicha empresa operadora, así como un correo electrónico a la dirección electrónica registrada por el abonado, al momento de recibir la solicitud de reposición de SIM Card y luego de transcurrido dos (2) horas desde el primer envío. Los mensajes deben informar sobre la solicitud de reposición de SIM Card, con detalle de la fecha y hora de la solicitud, lugar de presentación de la solicitud, y datos de contacto de la empresa operadora para que el abonado pueda informar si desconoce la solicitud y solicitar el bloqueo inmediato de la atención de dicha solicitud.**

6. **Luego de realizada la solicitud, del envío de los mensajes de texto, locuciones y correos electrónicos indicados en el párrafo precedente, y de la validación exitosa de la identidad del abonado, la empresa operadora debe proceder a la activación del mismo a las cuatro (4) horas de presentada la solicitud.**

7. **Asimismo, la empresa operadora debe enviar los referidos mensajes de texto, locuciones y correos electrónicos en los casos que la solicitud de reposición de SIM Card es denegada por intentos fallidos de verificación biométrica de huella dactilar o porque el poder presentado por el representante fue observado.**

OSIPTEL DAPU H.GUSUKUMA

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU M.GONZALEZ

8. La carga de la prueba respecto de la solicitud del abonado**, envío de los referidos mensajes de texto, locuciones y correos electrónicos, validación exitosa de la identidad del abonado, entrega del SIM Card al abonado y reactivación del servicio, corresponde a la empresa operadora**. El trámite de reposición del SIM Card se realizará de manera gratuita.

"**Artículo 71.- Supuestos de suspensión del servicio**
La empresa operadora únicamente podrá suspender el servicio:
(i) Por mandato judicial;
(ii) Cuando: (a) el recibo no es cancelado por el abonado en la fecha de vencimiento y ha transcurrido el período de gracia que la empresa operadora hubiere establecido, o (b) el abonado o usuario presenta un reclamo por facturación y no ha realizado el pago del monto que no se encuentra comprendido en el reclamo, en la fecha de vencimiento y ha transcurrido el período de gracia que la empresa operadora hubiere establecido. Para el servicio telefónico fijo, la empresa operadora sólo podrá suspender el servicio luego de transcurridos quince (15) días hábiles posteriores a la fecha de vencimiento que figura en el recibo correspondiente. Esta disposición también será aplicable a los servicios que se presten en forma empaquetada o en convergencia que comprendan al servicio de telefonía fija. Asimismo, para el servicio de arrendamiento de circuitos, la empresa operadora sólo podrá suspender el servicio por falta de pago siguiendo el procedimiento establecido en el artículo 91; en cualquier caso, la empresa operadora, deberá hacer efectiva la suspensión del servicio, transcurridos tres (3) meses de vencido el recibo impago.
(iii) Por declaración de insolvencia, conforme a la legislación de la materia;
(iv) Por uso indebido del servicio, de conformidad con lo dispuesto en el procedimiento aprobado por el OSIPTEL;
(v) Por la realización de llamadas malintencionadas a las centrales telefónicas de emergencias y urgencias, de conformidad con lo dispuesto en la normativa sobre la materia;
(vi) Por cualesquiera de las causales previstas en la presente norma y en las demás normas aprobadas por el OSIPTEL;
(vii) Por traslado del servicio realizado sin la autorización previa de la empresa operadora;
(viii) Por las causales establecidas en el Título XV; o,
(ix) Por las causales establecidas en el contrato de abonado, siempre que el OSIPTEL hubiera otorgado su conformidad al mismo.
(x) **Cuando el abonado desconoce o cuestiona la contratación del servicio o la reposición de SIM Card.**

En ningún caso, estas causales podrán estar referidas a supuestos que sean calificados por la empresa operadora como uso indebido del servicio.

La suspensión se mantendrá hasta que cesen las causas mencionadas, sin perjuicio de la facultad de la empresa operadora de resolver el contrato, de conformidad con lo dispuesto en la presente norma.

La empresa operadora no podrá realizar dicha suspensión del servicio en día feriado o no laborable ni en la víspera de cualquiera de ambos, salvo lo establecido

en los numerales (iv), (viii) y (x) del presente artículo y en el tercer párrafo del artículo 39.

En caso que el equipo terminal móvil ingrese al servicio técnico de la empresa operadora por un período mayor a un (1) día calendario, y siempre que el abonado lo haya solicitado expresamente, la empresa operadora deberá proceder a suspender el servicio; salvo que para efectos de comprobar el funcionamiento del equipo se requiera activar el servicio, en cuyo caso la empresa operadora, bajo su responsabilidad, activará el servicio sin que se genere costo alguno para el abonado.

La reactivación del servicio se efectuará de manera gratuita.

En este caso, la empresa operadora deberá entregar al abonado un documento escrito en el que conste la fecha y hora en que el abonado deberá recoger el equipo terminal, así como la indicación expresa acerca de que el servicio se reactivará de manera automática desde dicha fecha y hora".

"**Artículo 118.- Mecanismos de contratación**
Se considera como mecanismo de contratación a aquél documento que permita otorgar certeza de la solicitud o aceptación de los actos a los que se refiere el artículo precedente, siendo de manera taxativa los siguientes:

(i) Cualquier documento escrito;

(ii) Grabación de audio o video, la cual deberá comprender el íntegro de la comunicación entre el solicitante del servicio o el abonado, según corresponda, y la empresa operadora, desde que dicha comunicación se establece hasta su finalización.
En estos casos, la empresa operadora deberá requerir al abonado los datos personales que acrediten su identidad, para lo cual adicionalmente al número de documento legal de identificación del abonado (Documento Nacional de Identidad, Pasaporte, Carné de Extranjería, Registro Único de Contribuyentes o el documento legal de identidad válido requerido por la Superintendencia Nacional de Migraciones), deberá solicitar el lugar y fecha de nacimiento. Adicionalmente, la empresa operadora podrá solicitar el nombre del padre y/o madre, o alguna contraseña o clave secreta u otros datos que otorguen una mayor seguridad. La empresa operadora deberá entregar al abonado, de manera inmediata, un código o número correlativo de identificación del pedido realizado, debiendo mantener un registro de pedidos.
Este mecanismo no podrá ser utilizado para la contratación de altas nuevas, con excepción de: (a) aquellos casos en los que se valide la identidad del abonado a través de la contraseña única a la que hace referencia el artículo 128, y (b) los casos previstos en el artículo 11-F, siempre que el OSIPTEL hubiera aprobado el mecanismo de verificación de identidad respectivo.

(iii) Medios informáticos, que incluyan la utilización de contraseña o claves secretas que la empresa operadora le hubiere proporcionado previamente al abonado;

(iv) Marcación simple, para la contratación de prestaciones no continuadas de servicios, cuya utilización será empleada únicamente para realizar: (a) llamadas o remitir mensajería que sea tarificada individualmente, (b) afiliaciones a tarifas promocionales o establecidas que permitan la adquisición de paquetes de tráfico a través de la disposición del saldo de las recargas realizadas en los servicios bajo la modalidad prepago, (c) afiliaciones a

servicios adicionales que no impliquen el pago de una renta fija periódica, y (d) adquisición de eventos específicos, para el servicio de distribución de radiodifusión por cable.
En ningún caso, este mecanismo podrá ser utilizado para realizar migraciones de planes tarifarios o modificaciones en las condiciones del plan tarifario del abonado;

(v) Marcación doble (solicitud y confirmación), para la suscripción de servicios de contenido a ser provistos a través de mensajería o comunicaciones de voz, que impliquen prestaciones en forma continuada, de acuerdo a lo dispuesto en el artículo 118-A;

(vi) **Auto-activación, que implica que la validación de identidad del solicitante del servicio y su manifestación de voluntad se realiza mediante verificación biométrica de huella dactilar a través del aplicativo informático que la empresa operadora debe tener a disposición de todos los usuarios en la correspondiente tienda de aplicativos. La empresa operadora como mecanismo de seguridad realiza de manera aleatoria dos (2) de cualquiera de las siguientes preguntas de validación: a) nombre del padre, b) nombre de la madre, c) lugar de nacimiento, y/o d) fecha de nacimiento. Para una validación exitosa se requiere que se brinde el número del documento de identidad y la fecha correcta de su emisión, así como que ambas preguntas de validación sean contestadas de forma correcta. La empresa operadora proporciona al solicitante del servicio la información respectiva con las instrucciones que deberá seguir para el acceso y uso del referido aplicativo. Una vez llevado a cabo íntegra y exitosamente el procedimiento de validación de identidad y manifestación de la voluntad del solicitante a través del uso del aplicativo informático se entenderá perfeccionado el contrato del servicio, o presentada la solicitud y/o pedido del abonado.**

(vii) Otro mecanismo que haya sido aprobado previamente por el OSIPTEL.

Las empresas operadoras tienen la obligación de comunicar al OSIPTEL, de manera previa a su utilización, los mecanismos que implementen en aplicación del presente artículo, así como los mecanismos de seguridad que serán empleados para tales efectos.

Lo dispuesto en el presente artículo se aplica sin perjuicio que el abonado o usuario ejerza su derecho a reclamar y que dentro del procedimiento de reclamos se valoren otros medios probatorios. Para los casos de contratación previstos en los artículos 16 y 79 sólo será aplicable el mecanismo señalado en el numeral (i) del presente artículo".

"Artículo 119.- Migración a planes tarifarios y contratación de servicios suplementarios o adicionales

Para el caso de migración a planes tarifarios, contratación de servicios suplementarios o adicionales derivados del contrato de abonado u otras prestaciones contempladas en la presente norma, a través de los mecanismos de contratación señalados en los numerales (ii) y (iii) del artículo 118, no será exigible **la exhibición** del documento legal de identificación a que se refiere el artículo 11, así como la validación de identidad del abonado mediante el sistema de verificación

biométrica a que se refiere el artículo 11-A para el caso de los servicios públicos móviles, siempre que éste se encuentre debidamente identificado por ésta última**".**

"**Artículo 128.- Contraseña Única**

Mediante el uso de la contraseña única se sustituye la verificación biométrica de la identidad para la realización de trámites, **salvo para nuevas contrataciones de servicios principales, cambio de titularidad y reposición de SIM Card**.

Las empresas operadoras del servicio público móvil deben implementar la utilización de una contraseña por parte de sus abonados. En el caso de **migraciones o contrataciones de servicios adicionales o suplementarios** por vías distintas a la presencial, la empresa operadora deberá contar con la aprobación previa del OSIPTEL, de conformidad con lo dispuesto en artículo 118.

La empresa operadora **debe proporcionar a sus abonados dicha contraseña** al momento de la contratación del servicio o en cualquier otro en que su identidad sea validada a través del sistema de verificación biométrica de huella dactilar; o a través del correo electrónico que el abonado haya indicado en dicha oportunidad, **en cualquiera de las oficinas o centros de atención de la empresa operadora y los puntos de venta o atención habilitados en virtud a lo dispuesto en el tercer y cuarto párrafo del artículo 43, previamente reportados al OSIPTEL.**

La empresa operadora que entregue una contraseña a sus abonados, deberá exigir que el abonado modifique dicha contraseña antes de realizar el primer trámite que requiera su uso. Asimismo, deberá permitir que el abonado pueda cambiar dicha contraseña las veces que lo requiera.

Excepcionalmente, en el caso de nuevas contrataciones, la empresa operadora podrá permitir que el abonado obtenga su contraseña única a través del envío de un mensaje de texto al servicio contratado.

La entrega o generación de la contraseña a través de este mecanismo estará vigente por un periodo máximo de tres (3) días calendario. En caso el abonado no genere su contraseña única o no modifique la contraseña otorgada por la empresa operadora durante el referido plazo, solo se podrá obtener dicha contraseña mediante los mecanismos dispuestos en el tercer párrafo del presente artículo.

En ningún caso el sistema implementado por la empresa operadora para el cumplimiento de lo dispuesto en el presente artículo, permitirá que su personal de atención obtenga la contraseña del abonado. La referida contraseña será aplicable para todos los servicios públicos de telecomunicaciones prestados por cada empresa. Asimismo, la empresa operadora no podrá establecer diferenciaciones entre sus abonados respecto a los trámites y solicitudes que pueden realizar mediante el uso de esta contraseña.

Las empresas operadoras que prestan servicios distintos al servicio público móvil podrán implementar la utilización de esta contraseña. Las empresas operadoras tienen la obligación de comunicar al OSIPTEL, de manera previa a su utilización, los mecanismos que implementen en aplicación del presente artículo, así como los mecanismos de seguridad que serán empleados para tales efectos.

Para la contratación de nuevos servicios principales, cambio de titularidad y reposición de SIM Card de aquellos abonados que cuentan con contraseña única, de manera adicional a las validaciones de identidad previstas en los artículos 11, 11-A y 67-B, se requiere proporcione su contraseña única de forma exitosa"

Artículo Segundo.- Incluir los artículos 6-C, 75-B y 121-B al Texto Único Ordenado de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, aprobado mediante Resolución de Consejo Directivo N° 138-2012-CD/OSIPTEL, conforme al siguiente texto:

"**Artículo 6-C.- Información de solicitudes presentadas**

La empresa operadora debe informar al abonado sobre las solicitudes presentadas y trámites registrados, tales como: servicios contratados, portabilidad numérica, cambios de titularidad, y reposición de SIM Card.

Por medios no presenciales, la empresa operadora al brindar información sobre los servicios contratados, omite los últimos tres dígitos del servicio público móvil.

La empresa operadora debe informar si el motivo de la falta o inoperatividad del servicio o SIM Card reportada por el usuario obedece a alguna solicitud o trámite registrado".

"**Artículo 75-B.- Suspensión del servicio por desconocimiento o cuestionamiento de la contratación o reposición de SIM Card**

La empresa operadora suspende el servicio ante la presentación del reclamo por desconocimiento de la contratación del servicio; así como cuando el abonado comunica que desconoce la reposición de SIM Card. La suspensión se realiza de forma inmediata, al emplear el abonado el canal telefónico o presencial y en el plazo de un (1) día hábil, mediante el uso de un canal distinto.

En el caso de contrataciones no solicitadas, la reactivación del servicio se realiza cuando el reclamo se declare infundado, mediante una resolución firme o que hubiere causado estado, salvo que se haya solicitado la baja del servicio. Para el caso de desconocimiento de reposición de SIM Card, el servicio se reactiva al efectuarse una nueva reposición de SIM Card, conforme al procedimiento previsto en el artículo 67-B".

"**Artículo 121-B.- Información ante trámites cuestionados**

La empresa operadora del servicio público móvil debe proporcionar a solicitud del abonado que desconoce o cuestiona la contratación del servicio, la portabilidad numérica, el cambio de titularidad, y/o la reposición de SIM Card, lo siguiente:

1. **Detalle de fecha y hora de la solicitud o contratación, lugar de presentación de la solicitud o contratación.**
2. **Copia del mecanismo de contratación y/o solicitud correspondiente al trámite cuestionado.**

La información indicada en el numeral 1 se proporciona al momento de la atención del abonado. La entrega de la información indicada en el numeral 2 se realiza a pedido del abonado en el plazo máximo de cinco (5) días hábiles de presentada la solicitud de información. Los documentos proporcionados deben contar con sello o distintivo de la empresa a fin de que el abonado pueda emplearlos en la vía judicial".

Artículo Tercero. - Modifíquese los artículos 2, 3 y 4 del "Anexo 5: Régimen de Infracciones y Sanciones" del Texto Único Ordenado de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, aprobado mediante Resolución de Consejo Directivo N° 138-2012-CD/OSIPTEL, conforme al siguiente texto:

"**Artículo 2.- Infracciones leves**
Constituyen infracciones leves los incumplimientos, por parte de la empresa operadora, de cualesquiera de las disposiciones contenidas en los siguientes artículos: 2, 8, 8-A, 9, 10, 14, 15, 17, 18, 19, 20, 21, 21-A, 22, 27, 28, 29, 30, 31, 32, 33, 34, 34-A, 35, 37, 37-A, 38, 43, 43-A, 44, 45, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 59, 60, 62, 63, 64-A, 65, 67, 70, 71, 72, 73, 74, 75, 75-A, **75-B,** 77-A, 79, 80, 81, 82, 84, 87, 89, 91, 92, 95, 96, 97, 98, 101, 104, 106, 107, 109, 110, 111, 112, 113, 114, 115, 116, 118-A, 119, 120, 121, **121-B,** 122, 123, Quinta Disposición Final y Décimo Sexta Disposición Final."

"**Artículo 3.- Infracciones graves**
Constituyen infracciones graves los incumplimientos, por parte de la empresa operadora, de cualesquiera de las disposiciones contenidas en los siguientes artículos: 3 (segundo párrafo), 4 (primer y tercer párrafo), 6, 6-A, 6-B, **6-C,** 7, 9 (segundo párrafo), 10-A, 10-B, 10-C, 11-A (sétimo y octavo párrafo), 11-B (tercer párrafo), 12, 12-A (segundo, tercer y cuarto párrafo), 16, 16-A, 23, 23-A, 24, 36, 37-B, 39, 40, 40-A, 41, 42, 51-A, 66, 67-B, 76, 77, 78, 83, 88, 93, 99 (tercer párrafo), 100, 102, 118, 118-B, 121-A, 121-B, 124, 125, 126, 127, 128, 130, 131, 132, 133, 135, 136, 137, Sexta Disposición Final, Sétima Disposición Final y Décimo Primera Disposición Final. También constituye infracción grave el incumplimiento de la Resolución de Gerencia General a que se refiere el artículo 9, que ordena revocar o corregir cualquier modificación implementada por la empresa operadora."

"**Artículo 4.- Infracciones muy graves**
Constituyen infracciones muy graves los incumplimientos, por parte de la empresa operadora, de cualesquiera de las disposiciones contenidas en los siguientes artículos: 11, 11-A (primer, segundo, tercer, cuarto, quinto, sexto **y noveno** párrafo), 11-B, 11-C, **11-D** y 11-F.

Artículo Cuarto. - Incluir la siguiente definición al "Anexo 1: Glosario de Términos" del Texto Único Ordenado de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, aprobado mediante Resolución de Consejo Directivo N° 138-2012-CD/OSIPTEL, de acuerdo al siguiente texto:

ANEXO 1 GLOSARIO DE TÉRMINOS

Para efectos de las presentes Condiciones de Uso, se entenderá como:

(…)

PUNTO DE VENTA CON DIRECCIÓN ESPECÍFICA: Aquel establecimiento físico que se ubica en un lugar específico, y donde se realiza el comercio de acuerdo a las normas vigentes. No se considera como tal a la vía pública, plazas, parques u otros similares.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera. - Los artículos 2, 11, 11-A, 67-B, 119, 121-B y 128, así como los artículos 2, 3 y 4 del "Anexo 5: Régimen de Infracciones y Sanciones" entran en vigencia en el plazo de veinte (20) días hábiles desde la publicación de la presente resolución en el diario oficial "El Peruano".

Las demás disposiciones de la presente norma entran en vigencia en el plazo de tres (3) meses desde la publicación de la presente resolución en el diario oficial "El Peruano".

Segunda. - En el plazo de tres (3) meses de publicada la norma en el diario oficial "El Peruano", la empresa operadora informa al OSIPTEL los supuestos de suspensión temporal y cese definitivo de operaciones del distribuidor autorizado debido a contrataciones no solicitadas, incluidos en los convenios suscritos con sus distribuidores.

Tercero. - Derogar el numeral 3) del artículo segundo, así como los numerales 1, 2, 3, 4 y 5 del artículo tercero, y el artículo cuarto de la Resolución de Presidencia N° 042-2020-PD/OSIPTEL.

Cuarto. - Los mecanismos de contratación aprobados o con conformidad previo a la vigencia de la presente norma quedan sin efecto en los extremos que se opongan a estas disposiciones y corresponde que para su utilización incluyan las validaciones y requisitos establecidos en la presente norma.

Quinta.- La empresa operadora debe difundir a los abonados y usuarios, sobre los beneficios y uso de su aplicativo informático, implementado de acuerdo al artículo10-A del TUO de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones.

Para tal efecto, la empresa operadora debe transmitir un video informativo en sus oficinas o centros de atención, en caso cuente con un circuito cerrado de televisión o televisores empleados para difusión al público. Asimismo, el referido video informativo también debe encontrarse disponible en la página web de Internet y en las redes sociales de la empresa operadora. Del mismo modo, por dichos mecanismos la empresa operadora debe difundir piezas gráficas informativas.

El video informativo, el spot radial y las piezas gráficas con el contenido para la difusión son realizados por la empresa operadora. El sport radial sigue la pauta establecida por el OSIPTEL, en la cual se detalla el alcance, la frecuencia y horarios de difusión. El material para ser difundido debe ser comunicado a la Gerencia General del OSIPTEL a más tardar el 28 de febrero de 2022.

La fecha de inicio de la referida campaña de difusión será el 15 de marzo de 2022 y para el caso de radio, tendrá una duración mínima de tres meses. Respecto de los demás mecanismos de difusión es de forma permanente. El incumplimiento por parte de la empresa operadora a las obligaciones establecidas en esta disposición transitoria, constituye infracción grave.

OSIPTEL DAPU H.GUSUKUMA

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU M.GONZALEZ

ANEXO N° 3. EXPEDIENTES DE SUPERVISIÓN

EMPRESA	Expediente	Expediente asociado (Supervisión o Cautelar)	Infracciones detectadas	Tipo de infracción	Carta	Fecha de inicio de PAS	Fecha de emisión de IFI	Resolución Primera Instancia	Fecha de Resolución GG	Notificación	Multa en UIT	Resolución Reconsideración	Fecha de Resolución GG	Notificación	Resolución Segunda Instancia	Fecha de Resolución CD	Notificación
TELEFÓNICA	00125-2019-GG-GSF/PAS	00256-2019-GSF	Art. 6 del TUO de las Condiciones de Uso	Grave		16/12/2019	6/01/2020	00072-2020-GG/OSIPTEL	11/03/2020	13/03/2020	51	00106-2020-GG/OSIPTEL	27/05/2020	27/05/2020	00102-2020-CD/OSIPTEL	18/08/2020	-
			Art. 11-D del TUO de las Condiciones de Uso	Leve							18.1						
			Art. 27 del Reglamento de Supevisión	Leve							2.6						
CLARO	00124-2019-GG-GSF/PAS	00255-2019-GSF	Art. 6 del TUO de las Condiciones de Uso	Grave	02386-GSF/2019	16/12/2019	6/01/2020	00071-2020-GG/OSIPTEL	11/03/2020	13/03/2020	51	00200-2020-GG/OSIPTEL	28/08/2020	-	00188-2020-CD/OSIPTEL	4/12/2020	-
			Art. 11-D del TUO de las Condiciones de Uso	Leve							30.3						
			Art. 27 del Reglamento de Supevisión	Leve							2.6						
ENTEL	00122-2019-GG-GSF/PAS	00253-2019-GSF	Art. 6 del TUO de las Condiciones de Uso	Grave		16/12/2019	8/01/2020	00074-2020-GG/OSIPTEL	11/03/2020	13/03/2020	51	-	-	-	00089-2020-CD/OSIPTEL	30/07/2020	-
			Art. 11-D del TUO de las Condiciones de Uso	Leve							48.3						
			Art. 27 del Reglamento de Supevisión	Leve							4						
BITEL	00123-2019-GG-GSF/PAS	00254-2019-GSF	Art. 6 del TUO de las Condiciones de Uso	Grave		16/12/2019	6/01/2020	00073-2020-GG/OSIPTEL	11/03/2020	13/03/2020	70.7	-	-	-	00098-2020-CD/OSIPTEL	14/08/2020	-
			Art. 11-D del TUO de las Condiciones de Uso	Leve							50						
			Art. 27 del Reglamento de Supevisión	Leve							6.6						
TELEFÓNICA	00135-2019-GG-GSF/PAS	00008-2019-GG-GSF/CAUTELAR	Incumplimiento de Medida Cautelar	Muy grave		23/12/2019	22/01/2020	00139-2020-GG/OSIPTEL	7/07/2020	8/07/2020	151	00203-2020-GG/OSIPTEL	31/08/2020	31/08/2020	00169-2020-CD/OSIPTEL	9/11/2020	-
CLARO	00134-2019-GG-GSF/PAS	00007-2019-GG-GSF/CAUTELAR	Incumplimiento de Medida Cautelar	Muy grave	02429-GSF/2019	23/12/2019	17/01/2020	00141-2020-GG/OSIPTEL	7/07/2020	8/07/2020	151	00208-2020-GG/OSIPTEL	7/09/2020	-	00194-2020-CD/OSIPTEL	16/12/2020	-
ENTEL	00133-2019-GG-GSF/PAS	00005-2019-GG-GSF/CAUTELAR	Incumplimiento de Medida Cautelar	Muy grave		23/12/2019	21/01/2020	00140-2020-GG/OSIPTEL	7/07/2020	8/07/2020	151	-	-	-	00127-2020-CD/OSIPTEL	11/09/2020	-
BITEL	00132-2019-GG-GSF/PAS	00006-2019-GG-GSF/CAUTELAR	Incumplimiento de Medida Cautelar	Muy grave		23/12/2019	17/01/2020	00142-2020-GG/OSIPTEL	7/07/2020	8/07/2020	151	-	-	-	00126-2020-CD/OSIPTEL	11/09/2020	-

OSIPTEL DAPU H.GUSUKUMA

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU M.GONZALEZ

EMPRESA	Expediente	Expediente asociado (Supervisión o Cautelar)	Infracciones detectadas	Tipo de infracción	Carta	Fecha de inicio de PAS	Fecha de emisión de IFI	Resolución Primera Instancia	Fecha de Resolución GG	Notificación	Multa en UIT	Resolución Reconsideración	Fecha de Resolución GG	Notificación	Resolución Segunda Instancia	Fecha de Resolución CD	Notificación
TELEFÓNICA	00011-2020-GG-GSF/PAS	00011-2020-GSF	Art. 6 del TUO de las Condiciones de Uso	Grave		29/01/2020	6/03/2020	00198-2020-GG/OSIPTEL	26/08/2020	26/08/2020	51	00259-2020-GG/OSIPTEL	16/10/2020	16/10/2020	00003-2021-CD/OSIPTEL	4/01/2021	-
			Art. 11-A del TUO de las Condiciones de Uso	Muy grave							151						
			Art. 11-D del TUO de las Condiciones de Uso	Leve							27.6						
			Art. 27 del Reglamento de Supevisión	Leve							5.6						
CLARO	00010-2020-GG-GSF/PAS	00009-2020-GSF	Art. 6 del TUO de las Condiciones de Uso	Grave	00196-GSF/2020	29/01/2020	10/03/2020	00022-2021-GG/OSIPTEL	14/01/2021	-	51	00127-2021-GG/OSIPTEL	27/04/2021		00127-2021-CD/OSIPTEL	21/07/2021	
			Art. 11-D del TUO de las Condiciones de Uso	Leve							28.2						
			Art. 27 del Reglamento de Supevisión	Leve							1.4						
ENTEL	00008-2020-GG-GSF/PAS	00008-2020-GSF	Art. 6 del TUO de las Condiciones de Uso	Grave		29/01/2020	25/03/2020	00006-2021-GG/OSIPTEL	6/01/2021	-	51	-	-	-	00054-2021-CD/OSIPTEL	7/04/2021	-
			Art. 11-D del TUO de las Condiciones de Uso	Leve							50						
			Art. 27 del Reglamento de Supevisión	Leve							5.6						
BITEL	00009-2020-GG-GSF/PAS	00010-2020-GSF	Art. 6 del TUO de las Condiciones de Uso	Grave		29/01/2020	6/03/2020	00010-2021-GG/OSIPTEL	6/01/2021	-	51	-	-	-	00051-2021-CD/OSIPTEL	31/03/2021	-
			Art. 11-D del TUO de las Condiciones de Uso	Leve							40.9						
			Art. 27 del Reglamento de Supevisión	Leve							2.8						
TELEFÓNICA	00019-2020-GG-GSF/PAS	00001-2020-GG-GSF/CAUTELAR	Incumplimiento de Medida Cautelar	Muy grave		17/02/2020	16/05/2020	00325-2020-GG/OSIPTEL	21/12/2021	22/12/2020	151	00050-2021-GG/OSIPTEL	19/02/2021	19/02/2021	00092-2021-CD/OSIPTEL	8/06/2021	-
CLARO	00018-2020-GG-GSF/PAS	00004-2020-GG-GSF/CAUTELAR	Incumplimiento de Medida Cautelar	Muy grave	00355-GSF/2020	17/02/2020	6/04/2020	00036-2021-GG/OSIPTEL	1/02/2021		151	0269-2021-GG/OSIPTEL	30/07/2021	-	PENDIENTE		-
ENTEL	00020-2020-GG-GSF/PAS	00002-2020-GG-GSF/CAUTELAR	Incumplimiento de Medida Cautelar	Muy grave		17/02/2020	25/05/2020	00012-2021-GG/OSIPTEL	7/01/2021		151	-	-	-	00058-2021-CD/OSIPTEL	8/04/2021	-
BITEL	00017-2020-GG-GSF/PAS	00003-2020-GG-GSF/CAUTELAR	Incumplimiento de Medida Cautelar	Muy grave		17/02/2020	22/04/2020	00033-2021-GG/OSIPTEL	28/01/2021		151	-	-	-	PROCEDIMIENTO SUSPENDIDO	-	-

OSIPTEL DAPU H.GUSUKUMA

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU M.GONZALEZ

EMPRESA	Expediente	Expediente asociado (Supervisión o Cautelar)	Infracciones detectadas	Tipo de infracción	Carta	Fecha de inicio de PAS	Fecha de emisión de IFI	Resolución Primera Instancia	Fecha de Resolución GG	Notificación	Multa en UIT	Resolución Reconsideración	Fecha de Resolución GG	Notificación	Resolución Segunda Instancia	Fecha de Resolución CD	Notificación
TELEFÓNICA	00030-2020-GG-GSF/PAS	00030-2020-GSF	Art. 6 del TUO de las Condiciones de Uso	Grave		12/03/2020		00063-2021-GG/OSIPTEL	25/02/2021	26/02/2021	51	00141-2021-GG/OSIPTEL	6/05/2021	6/05/2021	00128-2021-CD/OSIPTEL	21/07/2021	-
			Art. 11-A del TUO de las Condiciones de Uso	Muy grave							151						
			Art. 11-D del TUO de las Condiciones de Uso	Leve							14.2						
			Art. 27 del Reglamento de Supevisión	Leve							1.4						
CLARO	00029-2020-GG-GSF/PAS	00029-2020-GSF	Art. 6 del TUO de las Condiciones de Uso	Grave	00499-GSF/2020	12/03/2020		00051-2021-GG/OSIPTEL	21/02/2021		51	00125-2021-GG/OSIPTEL	23/04/2021	-	00110-2021-CD/OSIPTEL	30/06/2021	-
			Art. 11-D del TUO de las Condiciones de Uso	Leve							22.9						
			Art. 27 del Reglamento de Supevisión	Leve							3						
ENTEL	00031-2020-GG-GSF/PAS	00031-2020-GSF	Art. 6 del TUO de las Condiciones de Uso	Grave		12/03/2020		00053-2021-GG/OSIPTEL	23/02/2021		51	00134-2021-GG/OSIPTEL	30/04/2021	-	00120-2021-CD/OSIPTEL	20/07/2021	-
			Art. 11-D del TUO de las Condiciones de Uso	Leve							50						
			Art. 27 del Reglamento de Supevisión	Leve							4.4						
BITEL	00032-2020-GG-GSF/PAS	00032-2020-GSF	Art. 6 del TUO de las Condiciones de Uso	Grave		12/03/2020		00062-2021-GG/OSIPTEL	25/02/2021		51	-	-	-	00082-2021-CD/OSIPTEL	22/05/2021	-
			Art. 11-D del TUO de las Condiciones de Uso	Leve							50						
			Art. 27 del Reglamento de Supevisión	Leve							5.8						
			Art. 11-A del TUO de las Condiciones de Uso	Muy grave							151						
TELEFÓNICA	00071-2020-GG-GSF/PAS	00007-2020-GG-GSF/CAUTELAR	Incumplimiento de Medida Cautelar	Muy grave		3/09/2020		00144-2021-GG/OSIPTEL	10/05/2021	10/05/2021	151	00208-2021-GG/OSIPTEL	17/06/2021	17/06/2021	00146-2021-CD/OSIPTEL	21/08/2021	-
CLARO	00069-2020-GG-GSF/PAS	00006-2020-GG-GSF/CAUTELAR	Incumplimiento de Medida Cautelar	Muy grave	01255-GSF/2020	3/09/2020		00179-2021-GG/OSIPTEL	1/06/2021	-	151	00264-2021-GG/OSIPTEL	26/07/2021	-	00195-2021-CD/OSIPTEL	20/10/2021	-
ENTEL	00068-2020-GG-GSF/PAS	00008-2020-GG-GSF/CAUTELAR	Incumplimiento de Medida Cautelar	Muy grave		2/09/2020		00173-2021-GG/OSIPTEL	27/05/2021	-	151	-	-	-	00153-2021-CD/OSIPTEL	24/08/2021	-
BITEL	00070-2020-GG-GSF/PAS	00009-2020-GG-GSF/CAUTELAR	Incumplimiento de Medida Cautelar	Muy grave		3/09/2020		PROCEDIMIENTO SUSPENDIDO	-	-	-	-	-	-	-	-	-

BICENTENARIO PERÚ 2021