FORMATO PARA PARTICIPAR EN LA CONSULTA PÚBLICA

Instrucciones para su llenado y participación:

I. Las opiniones, comentarios y propuestas deberán ser remitidas a la siguiente dirección de correo electrónico: seguridad.voz@ift.org.mx, en donde se deberá considerar que la capacidad límite para la recepción de archivos es de 25 Mb.
II. Proporcione su nombre completo (nombre y apellidos), razón o denominación social, o bien, el nombre completo (nombre y apellidos) de la persona que funja como representante legal. Para este último caso, deberá elegir entre las opciones el tipo de documento con el que acredita dicha representación, así como adjuntar –a la misma dirección de correo electrónico- copia electrónica legible del mismo.
III. Lea minuciosamente el **AVISO DE PRIVACIDAD** en materia del cuidado y resguardo de sus datos personales, así como sobre la publicidad que se dará a los comentarios, opiniones y aportaciones presentadas por usted en el presente proceso consultivo.
IV. Vierta sus comentarios conforme a la estructura de la Sección II del presente formato.
V. De contar con observaciones generales o alguna aportación adicional proporciónelos en el último recuadro.
VI. En caso de que sea de su interés, podrá adjuntar a su correo electrónico la documentación que estime conveniente.
VII. El periodo de Consulta Pública será del 9 de agosto al 5 de septiembre de 2024 (i.e. 20 días hábiles). Una vez concluido dicho periodo, se podrán continuar visualizando los comentarios vertidos, así como los documentos adjuntos en la siguiente dirección electrónica: http://www.ift.org.mx/industria/consultas-publicas
VIII. Para cualquier duda, comentario o inquietud sobre el presente proceso consultivo, el Instituto pone a su disposición el siguiente punto de contacto, Gabriel Huichán Muñoz, Director de Regulación Técnica de Servicios Mayoristas, correo electrónico: gabriel.huichan@ift.org.mx o bien, a través del número telefónico 55 5015 4000, extensión 2085.

I. Datos de la persona participante	
Nombre, razón o denominación social:	Pegaso PCS, S.A. de C.V. (Telefónica)
En su caso, nombre de la persona que funja como representante legal:	Natalia Guerra Caicedo
Documento para la acreditación de la representación: En caso de contar con una persona que funja como representante legal, adjuntar copia digitalizada del documento que acredite dicha representación, vía correo electrónico.	Poder Notarial

AVISO DE PRIVACIDAD INTEGRAL DE DATOS PERSONALES QUE EL INSTITUTO FEDERAL DE TELECOMUNICACIONES RECABA A TRAVÉS DE LA *UNIDAD DE POLÍTICA REGULATORIA*

En cumplimiento a lo dispuesto por los artículos 3, fracción II, 16, 17, 18, 21, 25, 26, 27 y 28 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en lo sucesivo, la "LGPDPPSO"); 9, fracción II, 15 y 26 al 45 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (en lo sucesivo los "Lineamientos Generales"); 11 de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales (en lo sucesivo los "Lineamientos de Portabilidad"), numeral XIV, punto 7, de la Política Interna de Gestión y Tratamiento de Datos Personales del Instituto Federal de Telecomunicaciones, se pone a disposición de las personas titulares de datos personales, el siguiente Aviso de Privacidad Integral:

I. Denominación del responsable
Instituto Federal de Telecomunicaciones (en lo sucesivo, el "IFT").

II. Domicilio del responsable
Avenida Insurgentes Sur #1143, Colonia Nochebuena, Demarcación Territorial Benito Juárez, Código Postal 03720, Ciudad de México.

III. Datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles
Los datos personales que el IFT recaba, a través de la *Unidad de Política Regulatoria*, son los siguientes:

- *Datos de identificación: Nombre completo de personas físicas, en su caso, nombre completo de representante legal.*
- *Datos de contacto: Dirección de correo electrónico.*
- *Datos laborales: Documentos que acrediten la personalidad del representante legal de personas físicas y morales.*

Se destaca que en términos del artículo 3, fracción X de la LGPDPPSO, ninguno de los anteriores corresponde a datos personales sensibles.

IV. Fundamento legal que faculta al responsable para llevar a cabo el tratamiento
El IFT, a través de la *Unidad de Política Regulatoria*, lleva a cabo el tratamiento de los datos personales mencionados en el apartado anterior, de conformidad con los artículos *15, fracciones XL y XLI, 51 de la Ley Federal de Telecomunicaciones y Radiodifusión , última modificación*

publicada en el Diario Oficial de la Federación el 20 de mayo de 2021,12, fracción XXII, segundo y tercer párrafos y 138 de la Ley Federal de Competencia Económica, última modificación publicada en el Diario Oficial de la Federación el 20 de mayo de 2021, así como el Lineamiento Octavo de los Lineamientos de Consulta Pública y Análisis de Impacto Regulatorio del Instituto Federal de Telecomunicaciones, publicados en el Diario Oficial de la Federación el 8 de noviembre de 2017, los artículos 19, 20 fracción XXII y 75 del Estatuto Orgánico del Instituto Federal de Telecomunicaciones, última modificación publicada en el Diario Oficial de la Federación el 18 de marzo de 2022; recabados en el ejercicio de sus funciones.

V. Finalidades del tratamiento

Los datos personales recabados por el IFT serán protegidos, incorporados y resguardados específicamente en los archivos de la *Unidad de Política Regulatoria*, y serán tratados conforme a las finalidades concretas, lícitas, explícitas y legítimas siguientes:

Datos personales	Finalidad del tratamiento
A. *Datos de identificación (nombre completo de personas físicas, en su caso, nombre completo de representante legal)*	*Divulgar íntegramente la documentación referente a los comentarios, opiniones y/o aportaciones que deriven de la participación de las personas físicas en los procesos de Consulta Pública a cargo del IFT.*
B. *Datos de contacto (dirección de correo electrónico)*	*Divulgar íntegramente la documentación referente a los comentarios, opiniones y/o aportaciones que deriven de la participación de las personas físicas en los procesos de Consulta Pública a cargo del IFT.* *Hacer llegar al IFT, mediante la dirección electrónica habilitada para ello, su participación en los procesos de Consulta Pública.*
C. *Datos laborales (documentos que acrediten la personalidad del representante legal de personas físicas y morales)*	*Acreditar la personalidad en caso de que los comentarios, opiniones y/o aportaciones, u otros elementos de los procesos consultivos sean presentados por los interesados a través de representante legal.*

VI. Información relativa a las transferencias de datos personales que requieran consentimiento

La *Unidad de Política Regulatoria* no llevará a cabo tratamiento de datos personales para finalidades distintas a las expresamente señaladas en este aviso de privacidad, ni realizará transferencias de datos personales a otros responsables, de carácter público o privado, salvo aquéllas que sean estrictamente necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados, o bien, cuando se actualice alguno de los supuestos previstos en los artículos 22 y 70 de la LGPDPPSO. Dichas transferencias no requerirán el consentimiento del titular para llevarse a cabo.

VII. Mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular

En concordancia con lo señalado en el apartado VI, del presente aviso de privacidad, se informa que los datos personales recabados no serán objeto de transferencias que requieran el consentimiento del titular. No obstante, en caso de que el titular tenga alguna duda respecto al tratamiento de sus datos personales, así como a los mecanismos para ejercer sus derechos, puede acudir a la Unidad de Transparencia del IFT, ubicada en Avenida Insurgentes Sur #1143 (Edificio Sede), Planta Baja, Colonia Nochebuena, Demarcación Territorial Benito Juárez, Código Postal 03720, Ciudad de México, o bien, enviar un correo electrónico a la siguiente dirección unidad.transparencia@ift.org.mx, e incluso, comunicarse al teléfono 55 5015 4000, extensiones 4688, 2321 y 2205.

VIII. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO (derechos de acceso, rectificación, cancelación y oposición al tratamiento de los datos personales)

Las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Unidad de Transparencia del IFT, a través de escrito libre, formatos, medios electrónicos o cualquier otro medio que establezca el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en lo sucesivo el "INAI").

El procedimiento se regirá por lo dispuesto en los artículos 48 a 56 de la LGPDPPSO, así como en los numerales 73 al 107 de los Lineamientos Generales, así como lo señalado en el Procedimiento Interno para garantizar el ejercicio de los Derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad de Datos Personales ejercidos ante el Instituto Federal de Telecomunicaciones[1], de conformidad con lo siguiente:

a) Los requisitos que debe contener la solicitud para el ejercicio de los derechos ARCO.

- Nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones;
- Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante;
- De ser posible, el área responsable que trata los datos personales y ante la cual se presenta la solicitud;
- La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO;
- La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular, y
- Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

[1] Disponible para consulta en: https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/3_M_ARCO/Criterio_3_1_1.zip

b) Los medios a través de los cuales el titular podrá presentar las solicitudes para el ejercicio de los derechos ARCO.

Los medios se encuentran establecidos en el párrafo octavo del artículo 52 de la LGPDPPSO, que señala lo siguiente: Las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Unidad de Transparencia del responsable, que el titular considere competente, a través de escrito libre, formatos, medios electrónicos o cualquier otro medio que al efecto establezca el INAI.

c) Los formularios, sistemas y otros medios simplificados que, en su caso, el INAI hubiere establecido para facilitar al titular el ejercicio de sus derechos ARCO.

Los formularios que ha desarrollado el INAI para el ejercicio de los derechos ARCO, se encuentran disponibles en su portal de Internet https://home.inai.org.mx/, en la sección "Protección de Datos Personales" /"Ingresa tu solicitud o denuncia" / "Formatos" / "En el sector público" /"Formato de Solicitud de derechos ARCO para el Sector Público"".

d) Los medios habilitados para dar respuesta a las solicitudes para el ejercicio de los derechos ARCO.

De conformidad con lo establecido en el artículo 90 de los Lineamientos Generales, la respuesta adoptada por el responsable podrá ser notificada al titular en su Unidad de Transparencia o en las oficinas que tenga habilitadas para tal efecto, previa acreditación de su identidad y, en su caso, de la identidad y personalidad de su representante de manera presencial, o por la Plataforma Nacional de Transparencia o correo certificado en cuyo caso no procederá la notificación a través de representante para estos dos últimos medios.

e) La modalidad o medios de reproducción de los datos personales.

Según lo dispuesto en el artículo 92 de los Lineamientos Generales, la modalidad o medios de reproducción de los datos personales será a través de consulta directa, en el sitio donde se encuentren, o mediante la expedición de copias simples, copias certificadas, medios magnéticos, ópticos, sonoros, visuales u holográficos, o cualquier otra tecnología que determine el titular.

f) Los plazos establecidos dentro del procedimiento —los cuales no deberán contravenir lo previsto en los artículos 51, 52, 53 y 54 de la LGPDPPSO— son los siguientes:

El responsable deberá establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO, cuyo plazo de respuesta no deberá exceder de veinte días contados a partir del día siguiente a la recepción de la solicitud.

El plazo referido en el párrafo anterior podrá ser ampliado por una sola vez hasta por diez días cuando así lo justifiquen las circunstancias, y siempre y cuando se le notifique al titular dentro del plazo de respuesta.

En caso de resultar procedente el ejercicio de los derechos ARCO, el responsable deberá hacerlo efectivo en un plazo que no podrá exceder de quince días contados a partir del día siguiente en que se haya notificado la respuesta al titular.

En caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos a que se refiere el párrafo cuarto del artículo 52 de la LGPDPPSO, y el responsable no cuente con elementos para subsanarla, se prevendrá al titular de los datos dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio de los derechos ARCO, por una sola ocasión, para que subsane las omisiones dentro de un plazo de diez días contados a partir del día siguiente al de la notificación. Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de ejercicio de los derechos ARCO.

La prevención tendrá el efecto de interrumpir el plazo que tiene el INAI para resolver la solicitud de ejercicio de los derechos ARCO.

Cuando el responsable no sea competente para atender la solicitud para el ejercicio de los derechos ARCO, deberá hacer del conocimiento del titular dicha situación dentro de los tres días siguientes a la presentación de la solicitud, y en caso de poderlo determinar, orientarlo hacia el responsable competente.

Cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un trámite o procedimiento específico para solicitar el ejercicio de los derechos ARCO, el responsable deberá informar al titular sobre la existencia del mismo, en un plazo no mayor a cinco días siguientes a la presentación de la solicitud para el ejercicio de los derechos ARCO, a efecto de que este último decida si ejerce sus derechos a través del trámite específico, o bien, por medio del procedimiento que el responsable haya institucionalizado para la atención de solicitudes para el ejercicio de los derechos ARCO conforme a las disposiciones establecidas en los artículos 48 a 56 de la LGPDPPSO.

En el caso en concreto, se informa que no existe un procedimiento específico para solicitar el ejercicio de los derechos ARCO en relación con los datos personales que son recabados con motivo del cumplimiento de las finalidades informadas en el presente aviso de privacidad.

g) El derecho que tiene el titular de presentar un recurso de revisión ante el INAI en caso de estar inconforme con la respuesta.

El referido derecho se encuentra establecido en los artículos 103 al 116 de la LGPDPPSO, los cuales disponen que el titular, por sí mismo o a través de su representante, podrán interponer un recurso de revisión ante el INAI o la Unidad de Transparencia del responsable que haya conocido de la solicitud para el ejercicio de los derechos ARCO, dentro de un plazo que no podrá exceder de quince días contados a partir del siguiente a la fecha de la notificación de la respuesta.

En caso de que el titular tenga alguna duda respecto al procedimiento para el ejercicio de los derechos ARCO, puede acudir a la Unidad de Transparencia del IFT, ubicada en Avenida Insurgentes Sur #1143 (Edificio Sede), Planta Baja, Colonia Nochebuena, Demarcación Territorial Benito Juárez, Código Postal 03720, Ciudad de México, enviar un correo electrónico a la siguiente dirección unidad.transparencia@ift.org.mx o comunicarse al teléfono 55 5015 4000, extensiones 4688, 2321 y 2205.

IX. Mecanismos, medios y procedimientos para ejercer el derecho de portabilidad de datos personales ante el IFT.

La persona titular, o su representante legal, podrá ejercer el derecho a la portabilidad de los datos personales en posesión del IFT. Al respecto, se informa que el derecho a la portabilidad de datos personales es una prerrogativa que permite a la persona titular, obtener una copia de los datos personales que ha proporcionado directamente al IFT, en un formato estructurado y comúnmente utilizado, para reutilizarlos con fines propios y en diferentes servicios.

Este derecho también implica que los datos personales puedan ser transmitidos a otros organismos, dependencias o entidades de carácter público (responsables), sin necesidad de ser entregados a la persona titular.

Los formatos con los que cuenta el IFT para garantizar el ejercicio del derecho a la portabilidad de datos personales, son los siguientes:

a) Excel (*.xlsx)
b) Texto (*.txt)
c) Archivo de texto (*.csv), y

d) Lenguaje de marcas de hipertexto (*.html)

En este sentido, los tipos o categorías de datos personales recabados e informados en el presente aviso de privacidad, que técnicamente son portables en los formatos antes señalados, son los siguientes:

- *Datos de identificación: Nombre completo de personas físicas, en su caso, nombre completo de representante legal.*
- *Datos de contacto: Dirección de correo electrónico.*

El derecho a la portabilidad de datos personales podrá ser ejercido ante el IFT, a través de escrito libre, o bien, mediante el **formato** diseñado para tal efecto, el cual se encuentra disponible en el vínculo electrónico siguiente: https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/4_Portabilidad/Criterio_4_1_2.zip.

La solicitud de portabilidad de datos personales podrá dirigirse a la Unidad de Transparencia, mediante el correo electrónico unidad.transparencia@ift.org.mx, o bien, entregarse de manera presencial en el módulo de la Unidad de Transparencia, situado en la Planta Baja del Edificio Sede, ubicado en la Avenida Insurgentes Sur #1143, Colonia Nochebuena, Demarcación territorial Benito Juárez, Código Postal 03720, en la Ciudad de México.
Para conocer mayor información acerca de cómo ejercer el derecho a la portabilidad de datos personales, el IFT pone a disposición del público la "Guía para ejercer el derecho a la portabilidad de los datos personales en posesión del Instituto Federal de Telecomunicaciones", la cual se encuentra disponible en el vínculo electrónico: https://www.ift.org.mx/sites/default/files/OPNT/LGPDPPSO/4_Portabilidad/Criterio_4_1_2.zip.

X. El domicilio de la Unidad de Transparencia del IFT.
La Unidad de Transparencia del IFT se encuentra ubicada en Avenida Insurgentes Sur #1143 (Edificio Sede), Colonia Nochebuena, Demarcación Territorial Benito Juárez, Código Postal 03720, Ciudad de México, y cuenta con un módulo de atención al público en la planta baja del edificio, con un horario laboral de 9:00 a 18:30 horas, de lunes a jueves, y viernes de 9:00 a 15:00 horas, número telefónico 55 5015 4000, extensiones 4688, 2321 y 2205.

XI. Los medios a través de los cuales el responsable comunicará a las personas titulares los cambios al aviso de privacidad.
Todo cambio al Aviso de Privacidad será comunicado a los titulares de datos personales en la sección de "Avisos de privacidad del Instituto Federal de Telecomunicaciones", del Apartado Virtual de Protección de Datos Personales del IFT, disponible en la dirección electrónica: https://www.ift.org.mx/proteccion_de_datos_personales/avisos_de_privacidad

Última actualización: (30/06/2023)

II. Comentarios, opiniones y aportaciones específicos de la persona participante sobre el asunto en Consulta Pública

Artículo o apartado	Comentario, opiniones o aportaciones
Tercero, Definiciones	***Sobre la definición de Llamada abandonada:*** La definición no es clara. ¿Cómo saber si una llamada terminada por el abonado que recibe es abandonada? Es factible saber quién es el primero que cuelga; no obstante, se necesita una regla clara para definir/identificar si es abandonada o no. ***Sobre las definiciones de Operador de Puerto Internacional e Identidad de la línea llamante (CLI):*** No es un dato que necesariamente siempre esté en CDR (factibilidad para su extracción). ¿Qué otro tipo de información se requiere del Carrier internacional? La implementación de esta medida podría enfrentar desafíos técnicos, especialmente en llamadas que transitan por múltiples redes internacionales. Asimismo, ver comentarios a los lineamientos Sexto y Noveno, relativos al tráfico internacional. ***Sobre la definición de tráfico sospechoso:***

	Se solicita a ese Instituto aclare y/o delimite el alcance, los parámetros y umbrales aplicables. La propuesta no diferencia claramente entre actividades sospechosas respecto al volumen de tráfico de la manipulación del CLI (casuísticas que deben tratarse de manera distinta y cuyas medidas de mitigación tienen naturaleza diversa), para garantizar una implementación más efectiva.
Cuarto	***Sobre la obligación para los Proveedores de Servicios de Voz (PSV) de autenticar la Identidad de la Línea Llamante para prevenir el spoofing (suplantación de identidad):*** Si bien deja a consideración del PSV el mecanismo de autenticación, es de la mayor relevancia que ese Instituto señale con claridad cuál es el operador que debe implementar la autenticación. Consideramos que es más adecuado que sea el operador que origina el que verifique la veracidad del CLI (dado que cuenta con más información para hacerlo) y es el que tiene a cargo la entrega de la información del abonado llamante.
Sexto y Noveno, en lo relativo al tráfico internacional	**Sobre i) la obligación para los PSV de bloquear las llamadas cuyo formato de numeración no sea conforme al estándar E.164 (ITU); ii) la obligación para los operadores de puertos internacionales de bloquear las llamadas cuyo formato de numeración no sea conforme al estándar E.164 (ITU):** Si bien se reconoce que las medidas impuestas son consistentes y reflejan prácticas internacionales para permitir la identificación de las llamadas internacionales de forma clara -lo cual es importantísimo para la prevención del fraude-, la implementación de dichas medidas enfrentará desafíos técnicos en llamadas que transitan por múltiples redes internacionales y que harían dichas disposiciones de imposible cumplimiento, por ejemplo, respecto a los servicios móviles, el operador no puede identificar saber si el usuario está en el extranjero o no; únicamente que tiene la facultad de poder hacer uso del servicio de roaming y si la comunicación no viene en el formato internacional que establece el estándar de ITU también deberá ser bloqueada, y no necesariamente se trata de comunicaciones posiblemente fraudulentas o irregulares. Por ejemplo, hay operadores que entregan la identificación de CLI en formatos distintos y no siempre están identificados en las banderas de TON+NPI. Es decir, hay llamadas con +52+NN sin tener bandera de internacional, entonces es erróneo el valor recibido o llega NN con bandera Internacional, entonces también es erróneo y no significa que sea una llamada errónea.

	Por ello, se solicita a ese Instituto que analice y considere establecer mecanismos de cooperación con sus homólogos internacionales a efecto de emitir consideraciones que coadyuven en la prevención del fraude en los servicios de telecomunicaciones donde se involucra la participación de carriers internacionales. Asimismo, se solicita que la implementación del estándar se limite a las comunicaciones originadas en territorio nacional.
Décimo	***Sobre las disposiciones preventivas y las condiciones contractuales para evitar llamadas no solicitadas por los usuarios:*** 1. El presente lineamiento sugiere el establecimiento de condiciones para control, registro y almacenamiento de información de campañas de marketing y publicidad. No obstante, lo anterior contraviene los acuerdos entre las partes en condiciones de carácter meramente comercial al prever intervención regulatoria; asimismo, genera carga regulatoria adicional, de la cual no se identifica la utilidad. 2. Por otra parte, no es claro si el mecanismo de exclusión es único para el usuario de Servicios de voz No Residenciales que está llamando; asimismo, señalamos que 24 horas se trata de un plazo de implementación muy corto y de imposible cumplimiento. En ese sentido, sugerimos no crear listas de exclusión adicionales sino apegarse al uso de los mecanismos ya existentes para evitar que los usuarios reciban llamadas no solicitadas, específicamente, REPEP, así como considerar el tiempo para aplicación/incorporación de los cambios que éste ya considera (30 días). Asimismo, solicitamos a ese Instituto que permita a los operadores que cuenten con la solicitud y consentimiento expreso de sus usuarios para ser inscritos por este a su nombre en la lista de exclusión existente. 3. Llamadas abandonadas. No es claro cómo medir el % de llamada abandonada y nivel por cliente (PBX). Se requiere regla clara.
Décimo Tercero a Décimo Noveno	***Sobre el proceso de rastreo:*** Se incrementa la carga regulatoria, técnica, administrativa y económica por la inversión requerida para dar cumplimiento, dado que implica desarrollar sistemas, procesos e instaurar equipos de trabajo dedicados al monitoreo, registro, almacenamiento de información, reporteo, implementación, entre otros. Adicionalmente, este proceso representa retos respecto al acceso y

	disponibilidad de la información cuando intervienen varios operador y alguno de estos es internacional. En dado caso, es recomendable establecer mecanismos de coordinación entre las diversas partes previo a cualquier implementación, para garantizar la inviolabilidad de las comunicaciones. En ese sentido, se solicita atentamente la eliminación de dichos numerales dado que no se justifica y fundamenta, y se realicen mesas de trabajo para identificar mecanismos más idóneos para atender la problemática.
Transitorio Primero	***Sobre la entrada en vigor del acuerdo:*** Toda vez que los operadores deben disponer del tiempo suficiente para realizar las inversiones, actualizaciones y adaptaciones necesarias a nivel técnico para la implementación de los presentes lineamientos, se solicita a ese Instituto que el plazo de entrada en vigor de los lineamientos sea de al menos 365 días, a efecto de contar con el tiempo suficiente para realizar las adecuaciones que sean pertinentes.
Nota: añadir cuantas filas considere necesarias.	

III. Comentarios, opiniones y aportaciones generales de la persona participante sobre el asunto en Consulta Pública

1. Sobre el uso de stir/shaken en México

Introducción

El protocolo STIR/SHAKEN ha sido adoptado por países como Estados Unidos y Canadá con el objetivo de combatir las llamadas fraudulentas y el "spoofing" de ID de llamadas. Esta tecnología busca autenticar y verificar la procedencia de las llamadas, ayudando a los consumidores a identificar llamadas de fuentes confiables. Sin embargo, no todos los países han optado por su implementación. En particular, el Reino Unido ha decidido no adoptar esta tecnología. A pesar de las aparentes ventajas, los desafíos significativos que enfrentan los países que han implementado STIR/SHAKEN sugieren que México debería reconsiderar su adopción.

Experiencia de Estados Unidos y Canadá

En Estados Unidos, la implementación de STIR/SHAKEN fue un paso ambicioso hacia la reducción de las llamadas no deseadas. A pesar de su implementación obligatoria, los resultados han demostrado que STIR/SHAKEN no ha sido tan efectivo como se esperaba. Las cifras revelan que, tras su mandato, el número de robollamadas no solo no disminuyó, sino que alcanzó un récord

de 5.5 mil millones de llamadas en octubre de 2022[2]. Aunque los operadores de telecomunicaciones se han esforzado para integrar STIR/SHAKEN, estas cifras muestran que las llamadas fraudulentas siguen siendo un problema grave y persistente.

Los altos costos de implementación también representan un obstáculo importante. Se estima que la implementación de STIR/SHAKEN en una red de telecomunicaciones puede costar a las compañías millones de dólares. De acuerdo con Priezkalns (2022)[3], las compañías de telecomunicaciones en Estados Unidos han destinado en conjunto aproximadamente 500 millones de dólares para implementar el sistema STIR/SHAKEN. Asimismo, se menciona que, para una sola empresa, los costos pueden llegar a decenas de millones de dólares. Por ejemplo, algunos proveedores tienen que afrontar gastos iniciales que pueden superar los 10 millones de dólares. Este gasto significativo puede no ser justificado en relación con los resultados obtenidos, especialmente si las cifras de llamadas fraudulentas no disminuyen de manera significativa.

Además, existen desafíos técnicos que afectan la efectividad de STIR/SHAKEN. Las redes más antiguas y los sistemas de telecomunicaciones que no se han modernizado completamente presentan problemas de compatibilidad. Esto implica que, a pesar de la autenticación de una llamada en la red de origen, la señal puede perderse o no ser reconocida en redes que no soportan STIR/SHAKEN, limitando su efectividad[4].

La decisión del Reino Unido

El Reino Unido optó por no implementar STIR/SHAKEN, citando preocupaciones sobre su efectividad y costo[5]. En su lugar, el Reino Unido ha explorado alternativas que no solo son más rentables, sino que también abordan de manera más integral la problemática de las llamadas fraudulentas. Al no adoptar STIR/SHAKEN, el Reino Unido ha evitado los desafíos técnicos y financieros asociados, centrando sus esfuerzos en medidas menos costosas y más adaptables.

Problemas en la efectividad de STIR/SHAKEN

Uno de los problemas clave con STIR/SHAKEN es la necesidad de cooperación internacional. Las llamadas fraudulentas a menudo se originan en el extranjero, lo que complica la autenticación y rastreo de estas llamadas si los países de origen no adoptan tecnologías similares. Además, las soluciones basadas únicamente en STIR/SHAKEN pueden ser insuficientes sin un enfoque global coherente y coordinado. Esta falta de uniformidad en la adopción mundial limita

[2] Wang, S., Delavar, M., Azad, M. A., Nabizadeh, F., Smith, S., & Hao, F. (2023). Spoofing Against Spoofing: Toward Caller ID Verification in Heterogeneous Telecommunication Systems. *ACM Transactions on Privacy and Security*, *27*(1), 1–25. https://doi.org/10.1145/3625546
[3] Priezkalns, E. (2022). The Million-Pound British Alternative to the Billion-Dollar STIR/SHAKEN Program. Commsrisk. https://commsrisk.com/the-million-pound-british-alternative-to-the-billion-dollar-stir-shaken-program/
[4] Priezkalns, E. (2023, June 12). US receives 5.1 billion robocalls in May; The excuses for failure keep getting worse. Commsrisk. https://commsrisk.com/the-million-pound-british-alternative-to-the-billion-dollar-stir-shaken-program/
[5] Priezkalns, E. (2024, February 2). UK rejects STIR/SHAKEN; US plan to control global caller ID now dead. Commsrisk. https://commsrisk.com/uk-rejects-stir-shaken-us-plan-to-control-global-caller-id-now-dead/

significativamente la capacidad de STIR/SHAKEN para reducir las llamadas fraudulentas de manera efectiva[6].

Otra cuestión es la adaptación tecnológica.

Muchos sistemas de telefonía en el mundo todavía dependen de tecnologías más antiguas, como el Protocolo de Inicio de Sesión (SIP) en redes de VoIP y otras tecnologías heredadas. El sistema STIR/SHAKEN, diseñado para autenticar llamadas y evitar el spoofing de identificador de llamadas, requiere una infraestructura de telecomunicaciones moderna y actualizada para funcionar de manera efectiva. Esta necesidad de modernización se convierte en un obstáculo considerable en muchos países donde la infraestructura de red no ha sido completamente actualizada o donde se siguen utilizando sistemas basados en tecnologías más antiguas como SS7.

Uno de los principales problemas con STIR/SHAKEN es su dependencia de una infraestructura de Clave Pública (PKI), que es costosa de implementar y mantener. Además, este sistema fue diseñado originalmente para redes IP, lo que significa que las redes que aún operan con tecnologías de señalización más antiguas quedan excluidas de su protección. Aunque hay propuestas para adaptar STIR/SHAKEN a redes no basadas en IP, como SS7, estas soluciones no son claras y conllevan desafíos adicionales en términos de implementación efectiva y seguridad de la información.

La falta de interoperabilidad entre las tecnologías modernas y las antiguas, junto con la necesidad de un consenso y cooperación internacional para que STIR/SHAKEN funcione de manera global, complica aún más su implementación. Los sistemas de telecomunicaciones que no están alineados con las tecnologías más recientes podrían enfrentar dificultades significativas para integrar STIR/SHAKEN sin realizar costosas actualizaciones en su infraestructura de red, lo que retrasa la adopción universal de este estándar [7] [8].

Costos y retorno de inversión

El alto costo de la implementación de STIR/SHAKEN no solo incluye la inversión inicial en infraestructura y tecnología, sino también los costos continuos de mantenimiento, actualización y supervisión del sistema. En un entorno de mercado donde las ganancias pueden ser ajustadas, las empresas de telecomunicaciones en México podrían no estar dispuestas a asumir estos costos sin evidencia clara de un retorno significativo de la inversión en términos de reducción de llamadas fraudulentas y mejora en la experiencia del usuario.

Alternativas más rentables y efectivas

[6] Priezkalns, E. (2024, March 8). Global STIR/SHAKEN is dead; What comes next? Commsrisk. https://commsrisk.com/global-stir-shaken-is-dead-what-comes-next/

[7] Priezkalns, E. (2024, March 8). Global STIR/SHAKEN is dead; What comes next? Commsrisk. https://commsrisk.com/global-stir-shaken-is-dead-what-comes-next/

[8] Priezkalns, E. (2023, June 12). US receives 5.1 billion robocalls in May; The excuses for failure keep getting worse. Commsrisk. https://commsrisk.com/the-million-pound-british-alternative-to-the-billion-dollar-stir-shaken-program/

En lugar de adoptar STIR/SHAKEN, México podría considerar alternativas menos costosas y potencialmente más efectivas para combatir el fraude por suplantación de identidad en llamadas telefónicas. Una opción es la implementación de sistemas de análisis de tráfico y patrones de llamadas, que pueden identificar y bloquear de manera proactiva las llamadas sospechosas basándose en el comportamiento en tiempo real. Esta técnica no requiere la infraestructura compleja de autenticación que necesita STIR/SHAKEN, lo que resulta en una reducción significativa de costos operativos[9].

Otra alternativa viable es promover la colaboración entre operadores de telecomunicaciones, tanto nacionales como internacionales, para compartir información sobre patrones de llamadas fraudulentas y coordinar esfuerzos para bloquear estos números de origen. Este enfoque colaborativo permitiría una respuesta más ágil y flexible ante nuevas tácticas de fraude. Además, la integración de sistemas como la Verificación de Identificación de Llamadas (CIV), que no dependen de una infraestructura PKI (infraestructura de clave pública), podría ser una solución efectiva para verificar la autenticidad de las llamadas en redes heterogéneas, incluyendo tanto sistemas IP como no-IP[10].

Además de estas estrategias técnicas, la educación del consumidor es crucial en la reducción de la efectividad de las llamadas fraudulentas. Las campañas de sensibilización pueden informar a los usuarios sobre las tácticas comunes de fraude y cómo protegerse, empoderando a los consumidores para que sean más vigilantes y estén mejor preparados para identificar llamadas sospechosas. Al combinar la tecnología con la educación del usuario, se crea una barrera adicional contra el fraude.[11]

Otra opción es la planteada por Du et al (2023)[12], un estudio reciente sobre el sistema UCBlocker propuesto en el 32nd USENIX Security Symposium sugieren que el uso de credenciales anónimas podría ser una alternativa innovadora para bloquear llamadas no deseadas. Este enfoque permite la autenticación del llamante sin revelar su identidad completa, utilizando políticas basadas en atributos específicos del llamante. UCBlocker minimiza los cambios en las redes telefónicas existentes y reduce la latencia en la autenticación de llamadas, proporcionando una solución robusta y escalable que podría ser considerada por México como parte de su estrategia contra el fraude telefónico.

Finalmente, para maximizar la efectividad de estas medidas, es esencial una implementación a nivel de red. Por ejemplo, la integración de soluciones como CIV directamente en la infraestructura de telecomunicaciones permitiría autenticar las llamadas de forma más eficiente, reduciendo la dependencia de verificaciones manuales y mejorando la capacidad de respuesta

[9] Wang, S., Delavar, M., Azad, M. A., Nabizadeh, F., Smith, S., & Hao, F. (2023). Spoofing Against Spoofing: Toward Caller ID Verification in Heterogeneous Telecommunication Systems. *ACM*

[10] Wang, S., Delavar, M., Azad, M. A., Nabizadeh, F., Smith, S., & Hao, F. (2023). Spoofing Against Spoofing: Toward Caller ID Verification in Heterogeneous Telecommunication Systems. *ACM*

[11] Wang, S., Delavar, M., Azad, M. A., Nabizadeh, F., Smith, S., & Hao, F. (2023). Spoofing Against Spoofing: Toward Caller ID Verification in Heterogeneous Telecommunication Systems. *ACM*

[12] Du, C., Yu, H., Xiao, Y., Hou, Y. T., Keromytis, A. D., & Lou, W. (2024). UCBlocker: Unwanted call blocking using anonymous authentication. In *Proceedings of the 33rd USENIX Security Symposium*. USENIX Association. Retrieved from https://www.usenix.org/conference/usenixsecurity24/presentation/du

ante intentos de fraude. Esta integración no solo mejoraría la seguridad de las llamadas, sino que también optimizaría los recursos, haciendo que las soluciones sean sostenibles y escalables en el largo plazo[13].

Conclusión

Aunque STIR/SHAKEN puede parecer una solución técnica avanzada para combatir las llamadas fraudulentas, los desafíos y limitaciones que presenta en términos de costo, compatibilidad y necesidad de cooperación internacional sugieren que México debería ser cauteloso en su adopción. Al considerar la experiencia de otros países como Estados Unidos, que ha enfrentado problemas significativos a pesar de la implementación de STIR/SHAKEN, y el Reino Unido, que ha optado por no implementarlo, México tiene la oportunidad de explorar alternativas más rentables y efectivas. **Desde Telefónica, recomendamos adoptar un enfoque basado en educación del consumidor,** análisis anonimizado de tráfico, y colaboración internacional. Este enfoque puede proporcionar una solución más flexible y eficiente para abordar el problema de las llamadas fraudulentas sin incurrir en los altos costos y desafíos técnicos asociados con STIR/SHAKEN.

2. Sobre la inclusión del servicio de SMS y la determinación de reglas análogas.

Las comunicaciones no deseadas o autorizadas/consentidas por el usuario, o con un potencial origen o contenido fraudulento generan molestia a estos y disminuyen su confianza para utilizar servicios de telecomunicaciones de manera segura, al incrementar su exposición, riesgo y vulnerabilidad a ser objeto de robo de información, de fraude o extorsión, o de recibir información con carácter malicioso, entre otros; lo que sin lugar a duda, repercute en la experiencia del usuario para utilizar la conectividad como herramienta para el acceso a otros servicios como el comercio o la banca electrónicos. Adicionalmente, no debiera obviarse que esta problemática repercute únicamente a los servicios de voz, sino también a la mensajería (situación que es de conocimiento de ese Instituto); precisamente por ello se requiere que el Instituto establezca reglas estrictas y claras para reducir las vulnerabilidades a las que se enfrentan los usuarios de servicios de telecomunicaciones para reducirlas en la medida de lo posible.

Tanto en el caso de la voz como de la mensajería, se genera i) un alto consumo de recursos que puede afectar las capacidades de la red, afectando el servicio público que se presta a los usuarios en general, impactando en los índices de calidad; ii) saturación o degradación del servicio. Asimismo, se incrementan las quejas de los usuarios por afectaciones derivadas de comunicaciones no deseadas o que tienen carácter fraudulento y/u origen desconocido.

Desde la perspectiva de usuario, desafortunadamente, son limitados los mecanismos con los que cuentan los usuarios para evitar recibir comunicaciones de voz y mensajería no deseadas o con carácter fraudulento; sobre todo en la mensajería en la que los usuarios no cuentan con una

[13] Wang, S., Delavar, M., Azad, M. A., Nabizadeh, F., Smith, S., & Hao, F. (2023). Spoofing Against Spoofing: Toward Caller ID Verification in Heterogeneous Telecommunication Systems. *ACM*

oportunidad para recibir o no los mismos, por lo que insistimos en que se requieren medidas adicionales claras y estrictas para prevenir afectaciones a los usuarios. Se recomienda realizar campañas con fines educativos para que los usuarios cuenten con herramientas para detectar comunicaciones no deseadas y/o con fines fraudulentos, así como para contar con herramientas para prevenir vulnerabilidades frente a estas comunicaciones. Debe considerarse un catálogo de prácticas mensajería. Puede tomarse como base para la determinación de prácticas no deseadas aquellas señaladas en los convenios de Interconexión celebradas entre los operadores de telecomunicaciones; de manera enunciativa, más no limitativa, spam y flooding, con definiciones claras y parámetros específicos. También, se requiere establecer mecanismos de cooperación para la detección, análisis y atención de comunicaciones no deseadas o fraudulentas y sus efectos, por tener efectos transversales hacia empresas y usuarios, entre todos los actores involucrados en la cadena de valor. Asimismo, se requiere que el Instituto establezca reglas estrictas y claras para reducir las vulnerabilidades a las que se enfrentan los usuarios de servicios de telecomunicaciones frente a comunicaciones no deseadas o posiblemente fraudulentas para reducirlas en la medida de lo posible, así como validar el uso de herramientas anti-spamming por el proveedor de destino, cuando las conductas se circunscriban a las prácticas identificadas en la normatividad y en los acuerdos celebrados.
Nota: añadir cuantas filas considere necesarias.