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 conforme a la estructura de la Sección III del presente formato.
VI. En caso de que sea de su interés, podrá adjuntar a su correo electrónico la documentación que estime conveniente.
VII. El período de consulta pública será del 14 de diciembre de 2023 al 26 de enero 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 y número telefónico 55 5015 4000, extensión 2085.

I. Datos de la persona participante	
Nombre, razón o denominación social:	Cablevisión, S.A. de C.V., Operbes, S.A. de C.V., Cablemás Telecomunicaciones, S.A. de C.V., México Red de Telecomunicaciones, S. de R.L. de C.V., Televisión Internacional, S.A. de C.V., Cablevisión Red, S.A. de C.V., y TV Cable de Oriente, S.A. de C.V.
En su caso, nombre de la persona que funja como representante legal:	Víctor Tomás López Baltierra
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.

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

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

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: (XX/06/2023)

II. Cuestionario de la Consulta Pública de Integración

Nota 1: El documento "**Estudio sobre la Seguridad de las Comunicaciones de Voz a través de Redes Públicas de Telecomunicaciones**", es un documento de referencia que ayuda en la comprensión de los cuestionamientos listados en la siguiente tabla. Por sí mismo, dicho documento de referencia no se encuentra en Consulta Pública.

Nota 2: Se recomienda responder a todas las preguntas contenidas en la siguiente tabla, acompañado de los argumentos, planteamientos, justificaciones y elementos de análisis que se considere necesario para sustentar la opinión, incluyendo documentos de soporte que se deseen adjuntar.

No. de pregunta	Pregunta	Comentarios, opiniones o aportaciones
1	¿Cuál considera que es el impacto de prácticas no deseadas en los servicios de telefonía tales como llamadas no solicitadas, no autorizadas o de suplantación de identidad (spoofing), entre otras, en la experiencia y satisfacción de los usuarios?	Las prácticas no deseadas generan afectaciones en la experiencia del usuario principalmente por qué; i) ponen en riesgo su seguridad (afectan directamente la seguridad de la información), lo que genera inconformidad y desconfianza en los clientes, incluso generando cargos no reconocidos y ii) la saturación de red que generan impacta en la disponibilidad para cursar el tráfico del usuario, restringen la prestación de los servicios y disminuyen la calidad con que se presta. Por otro lado, para el operador constituyen un incremento de costos y puede impactar en la reputación de la empresa ya que la reclamación de los clientes es directamente con el prestador de servicios de telecomunicaciones, aunado a que, el cliente percibe que no se le protege.
2	¿Cuál considera que es el impacto de prácticas no deseadas en los servicios de telefonía tales como llamadas no solicitadas, no autorizadas o de suplantación de identidad (spoofing), entre otras, en los servicios de telecomunicaciones y en la operación de redes públicas de telecomunicaciones?	Las llamadas con estos escenarios propician un consumo excesivo de recursos de red y baja disponibilidad para cursar el tráfico de los usuarios finales. Lo anterior, puede impactar en la experiencia del cliente sobre los servicios prestados. Además, la atención a estas prácticas implica recursos para los prestadores de servicios de telecomunicaciones, quienes deben utilizar herramientas costosas para evitarlas.
3	¿Qué prácticas no deseadas en los servicios de voz considera que debieran ser consideradas en el desarrollo del "*Anteproyecto de Lineamientos para garantizar la seguridad de las comunicaciones de voz a través de redes públicas de telecomunicaciones*"?	Consideramos que las prácticas no deseadas más recurrentes y que deben ser atendidas en el anteproyecto de Lineamientos son la suplantación de identidad (spoofing), SPAM y el IRSF (International Revenue Share Fraud), debido a que son temas que han ido creciendo considerablemente y tienen un impacto directo sobre el cliente y los prestadores de servicios de telecomunicaciones.

No. de pregunta	Pregunta	Comentarios, opiniones o aportaciones
4	¿Actualmente implementa medidas o proporciona herramientas a sus usuarios para evitar o gestionar llamadas no deseadas?	Actualmente se utilizan políticas de seguridad como User Agent en las troncales de Voz. Sin embargo, es importante recordar que no es posible bloquear el tráfico que llega de otras redes en forma selectiva, ya que dicho bloqueo sólo puede realizarse por orden de una autoridad competente, lo anterior de conformidad con la regulación vigente.
5	¿Cuáles considera que son los principales desafíos técnicos y operativos que se enfrenta para la detección y prevención de llamadas no deseadas y/o de suplantación de identidad (spoofing)?	Consideramos que el principal desafío es el uso de herramientas que utilicen detección y bloqueo dinámico, así como identificación del origen de la llamada, ya sea la IP origen (que puede cambiar dinámicamente) o el número de "A" (que se cambia aleatoriamente).
6	¿Qué tecnologías y métodos identifica para detectar y bloquear llamadas no deseadas y/o llamadas de suplantación de identidad telefónica (spoofing)?	El uso de políticas de seguridad como son: - Validación del número de A en llamadas nacionales e internacionales. - Restringir la longitud del número de origen. - Formato y bloqueo del número de origen (por ejemplo: 1112223334, 8888888888).
7	¿Qué prácticas identifica para el manejo y atención de las quejas de los usuarios relacionadas con llamadas no deseadas o de suplantación de identidad (spoofing) y qué procedimientos de respuesta a este tipo de incidentes identifica o considera que deben ser establecidos?	Se podrían establecer lineamientos de configuración entre operadores y clientes con el fin de proteger la identidad de los clientes, para minimizar los impactos y en los casos concretados se realizarían análisis post-mortem para establecer medidas de mejora.
8	¿Realiza trabajos de coordinación con otras entidades o redes para abordar el problema de llamadas no deseadas y de suplantación de identidad (spoofing)?, ¿qué tipo de colaboración entre operadores considera necesaria para combatir efectivamente este tipo de prácticas?	Actualmente se aplican algunas políticas de seguridad como User Agent y CAC en conjunto con distintos operadores. Aunado a lo anterior, se realizan actividades para evitar las llamadas no deseadas a los suscriptores.
9	¿Qué soluciones podrían introducir los prestadores de servicios para proteger a los usuarios de las llamadas no deseadas y las llamadas de suplantación de identidad (spoofing)?	Consideramos que la solución STIR/SHAKEN para validación del número de origen y base de datos de SPAM o lista negra de los números de origen, podría ser útil para la industria, sin embargo, habría que revisar los retos técnicos y económicos de implementación de esta solución.

No. de pregunta	Pregunta	Comentarios, opiniones o aportaciones
10	¿Cuál considera que sería el impacto de la adopción de medidas para la autenticación de identidad de origen en la reducción de llamadas no deseadas?, ¿Identifica algún enfoque o estrategia alternativa mejor?	Consideramos que el impacto sería principalmente económico/operativo, debido a que la adquisición e implementación de herramientas (CAPEX u OPEX) para mitigar estas conductas generaría altos costos a la industria. Por lo que, ese Instituto debe considerar realizar una estrategia donde existan bases de datos comunes para consultar números no deseados, que sean controladas y administradas por el ente regulador (vía un tercero), con la finalidad de apalancar costos.
11	¿Cuál es su opinión sobre la implementación de STIR/SHAKEN para el combate de llamadas no deseadas y/o de suplantación de identidad (spoofing)?	Podría ser un modelo viable considerando que se ha implementado por otros operadores en distintos países, sin embargo, habría que revisar la factibilidad de implementación en México.
12	¿Qué retos técnicos, operativos y económicos considera de importancia para la implementación de soluciones de autenticación de llamadas, como STIR/SHAKEN?	Consideramos que para la implementación de un estándar como STIR/SHAKEN deben considerarse los siguientes aspectos: - La implementación debe ser de extremo a extremo. - Habrá más elementos entre el origen y destino de una llamada. - El MTU de las interconexiones, se verá incrementado >1500 bytes, lo que implicará reconfiguraciones en todos los puntos de interconexión o PDI entre operadores. - Implicará pruebas de interconexión e interoperabilidad entre los operadores. - Riesgo de bloqueo de llamadas que sí sean deseadas y posible pérdida de tráfico. - Riesgo de incremento del PDD. - Nuevas políticas para el manejo de fallas. - Costos CAPEX u OPEX asociados a la implementación.

No. de pregunta	Pregunta	Comentarios, opiniones o aportaciones
13	¿Cuál es su opinión sobre la implementación de otras soluciones como *blockchain*, AB Handshake, bloqueo y filtrado de llamadas, listas de "*No Llamar*", entre otras, para el combate de llamadas no deseadas y/o de spoofing?	Consideramos que ninguno de los mecanismos ofrecería una mejora realmente satisfactoria a la problemática actual, sin embargo, se hacen los siguientes comentarios: - Respecto a las tecnologías Blockchain y AB Handshake, no son soluciones maduras e implican una complejidad operativa a considerar respectivamente. - En relación con la solución de inteligencia artificial, se solicitaría profundizar más en los elementos de implementación para estar en condiciones de emitir una opinión al respecto. - Ahora bien, las listas de "No llamar" son medidas que pudieran adoptarse y que podrían tener un beneficio para los usuarios, sin embargo, habría que revisar los retos técnicos y económicos de implementación de esta solución.
14	¿Hay algún otro enfoque técnico o regulatorio que considere deba ser tomado en cuenta para el combate de llamadas no deseadas y/o de suplantación de identidad (spoofing)?	Se debería precisar el número de dígitos del formato de CLI que deberá ser permitido, sobre todo en llamadas internacionales entrantes. Asimismo, deberían definirse las políticas de seguridad entre operadores.

III. Comentarios, opiniones, aportaciones generales u otros elementos de análisis formulados por el participante

Nota 3: En la presente sección se podrán realizar comentarios, opiniones, aportaciones generales u otros elementos de análisis.

Nota 4: El interesado deberá añadir las filas que considere necesarias para formular los comentarios, opiniones, aportaciones u otros elementos de análisis que considere pertinentes.

Número de página del estudio/documento de referencia	Comentario(s), opinión(es), aportación(es) u otros elementos de análisis
Página 22/63, de la sección: II. Panorama General y Políticas Implementadas en Reino Unido	En relación con las políticas implementadas en Reino Unido, consideramos que algunas iniciativas podrían analizarse para ser implementadas en México, ya que es importante definir el número de "A" en llamadas originadas en el extranjero, con el fin de poder aplicar políticas de seguridad en el origen sin bloquear llamadas válidas. Por lo anterior, es posible que las siguientes iniciativas se analicen para determinar la factibilidad de ser implementadas en México: *"• Precisa que el formato del CLI debe ser de 10 u 11 dígitos.* *• Utilizar la información disponible sobre números que no deben ser utilizados en el CLI como la lista de no originación.*

Número de página del estudio/documento de referencia	Comentario(s), opinión(es), aportación(es) u otros elementos de análisis
	• Bloquear las llamadas originadas en el extranjero y que no tienen un CLI valido. *• Bloquear las llamadas originadas en el extranjero y que falsifican un CLI del Reino Unido.* *• Prohibir el uso de números no geográficos como CLI."*
Página 24/63, de la sección: III. Panorama General y Políticas Implementadas en Canadá. Página 29/63, de la sección: IV. Panorama General y Políticas Implementadas en la India	Sería importante contar con una lista de números a los cuáles el usuario de su consentimiento para recibir llamadas y poder controlar cuando no se requieren recibir ciertas llamadas.
Página 26/63, de la sección: III. Panorama General y Políticas Implementadas en Canadá.	Consideramos importante que ese Instituto comparta de forma más detallada este caso de éxito "Bell Canada" señalado en esta sección, con la finalidad de analizar costo-beneficio de implementación en los operadores nacionales. *"Además, han surgido iniciativas conjuntas entre la CRTC y la industria, como el caso de Bell Canada, operador que implementó un sistema de bloqueo de llamadas basado en inteligencia artificial el cual analiza el tráfico de telecomunicaciones y detecta anomalías que sugieren una posible actividad fraudulenta a nivel de red. La CRTC aprobó su implementación como resultado directo de un período de prueba exitoso, durante el cual se bloquearon más de mil millones de llamadas fraudulentas (CRTC, 2023)."*
Página 29/63, de la sección: IV. Panorama General y Políticas Implementadas en la India	Consideramos que debe prestarse especial atención a la identificación del usuario, con la finalidad de detectar cualquier comportamiento no deseado que pueda impactar las redes de servicios de telefonía. *"Por otra parte, como parte de la regulación para erradicar las llamadas fraudulentas y a los emisores de spam, la TRAI está implementando un sistema unificado denominado KYC (del inglés, "Know Your Customer"), diseñado para prevenir el uso indebido de servicios de telecomunicaciones y asegurar la identificación adecuada de los usuarios de dichos servicios.* *A través del KYC, los operadores de telecomunicaciones están obligados a verificar la identidad y la dirección de sus usuarios mediante documentos oficiales. Al garantizar que cada cuenta esté vinculada a una identidad verificable, el sistema KYC ayuda a prevenir el fraude, como la suplantación de identidad y el uso ilegal de servicios de telecomunicaciones"*
Página 31/63 de la sección: V. Enfoque de la Unión Internacional de Telecomunicaciones	Respecto al modelo STIR/SHAKEN habría que poder autentificar la línea y tener certeza de que se conoce quién es el dueño de la numeración. Por otro lado, en el futuro cercano sería interesante evaluar la implementación de SEISMIC basado en SOLID y que indica como característica importante que no depende de que la señalización sea soportada de extremo a extremo y funciona con TDM /SIP. Habrá que considerar los costos asociados a este modelo que es complementario a STIR/SHAKEN.