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:	ASLO TECNOLOGIA Y COMUNICACIONES
En su caso, nombre de la persona que funja como representante legal:	OSCAR RODRIGO LAZCANO LIRA
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.	Acta Constitutiva

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.

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"".

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

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?	A nivel abonado es evidente desde hace al menos 10 años la pérdida total de confianza en el identificador de llamadas y el altísimo riesgo de fraude, estafa y/o de extorsión telefónica al contestar números desconocidos. La suplantación telefónica ha ocasionado que usuarios pierdan su patrimonio por contestar una sola llamada de riesgo. La laxitud de las redes telefónicas públicas ha sido abusada tanto por el defraudador, como por negocios legítimos que se aprovechan de las facilidades de enmascaramiento y reciclaje de números (DIDs) para generar spam con fines de cobranza o televentas. Y al mismo tiempo, los operadores telefónicos han sido omisos y permiten estás prácticas para satisfacer la necesidad de Centros de Contacto con campañas agresivas de venta o cobranza, a los cuales ellos mismos les circulan cientos de DIDs para burlar los intentos de evadir estas llamadas por parte de los usuarios finales. En pocas palabras, es verdaderamente un círculo vicioso en dónde el gran perdedor es el usuario final. El negocio legitimo del operador y del centro de contacto genera un spam interminable, lo que finalmente permite al defraudador aprovechar esa condición para pasar más fácilmente desapercibido. Los intentos de PROFECO y de CONDUSEF, con el REUS y el REPEP, han ayudado poco o nada.

No. de pregunta	Pregunta	Comentarios, opiniones o aportaciones
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?	Me parece que para los TELCOs es un problema administrativo MENOR. En términos operativos y tecnológicos no les representa un problema. Administrativamente, para atender la demanda de algunos bancos, han tenido que aplicar algunas políticas de ruteo especiales para evitar que algunos ANI's que son solo "inbound" (ej. 800) cursen por su red, pero son casos contados. Considero que el bypass dejo de ser un problema mayor para los TELCOs hace varios años, que sería un aspecto de negocio en dónde el uso incorrecto de ANI's nacionales en tráfico internacional pudiera ser de impacto. Por otro lado, la proliferación de SIM boxes para generar tráfico celular con fines de spam, me parece que, sí pudiera representar un problema de capacidad en ciertas zonas, pero que, la implementación de STIR/SHAKEN o cualquier otro esquema de verificación fuera de banda (out-of-band) no va a resolver, pues el problema es de una naturaleza distinta. Finalmente, el cambio de hábito y la migración del usuario final desde la llamada telefónica hacia los canales de comunicación "Over-the-top" (ej. WhatsApp), me parece que ha subsanado de forma indirecta el otrora problema de capacidad en el Core telefónico del Carrier, a causa del tráfico "no-solicitado".

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*"?	1. La asignación sin control, recurrente e ilimitada de DIDs a Centros de Contacto y/u otro tipo de empresas que lo soliciten. 2. La ausencia de controles de ruteo por ANI, que ocasionan que, llamadas con número de A asignados a clientes empresariales o líneas de negocio, circulen por las redes libremente, o bien, circulen por las interconexiones domésticas o internacionales sin control. 3. La ausencia de sistemas de analíticos cuya inexistencia o desaprovechamiento evita detectar proactiva y automáticamente, patrones de tráfico inequívocos de SPAM o ABUSO telefónico con acciones de bloqueo y puesta en cuarentena de forma automática. 4. La ausencia de un esquema de sanciones que termine con la suspensión parcial o total de los DIDs asignados por omisión o evasión de las reglas de control. 5. La ausencia de un esquema de sanciones ágil, efectivo y expedito que termine con la suspensión parcial o total de líneas celulares con patrones de uso maliciosos. 6. La ausencia de un esquema de denuncia que permita procesar de forma ágil y expedita el bloqueo de números reportados como de fraude, abuso o uso malicioso en las redes públicas. 7. La ausencia de mecanismos de verificación de origen de llamadas telefónicas que permiten la suplantación de números de A sin control, sin identificación, sin rastreo y sin acciones temporales o definitivas para su erradicación. 8. La laxitud de los procedimientos "KYC" o "Know Your Customer" para la entrega de servicios empresariales o de alta capacidad. 9. La laxitud de los procedimientos de identificación de usuario final para la adquisición de servicios de prepago. 10. La laxitud de los procedimientos de venta que permiten la comercialización y la activación sin control, sin límite, y sin identificación de tarjetas SIM de prepago.

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?	Afirmativo. Las ofrecemos al mercado TELCO, empresarial, Micro, PyME y gran empresa, y también al usuario final particular. (usuario de smartphone).

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)?	Los sistemas de prevención de llamadas no deseadas y/o de suplantación de identidad verdaderamente efectivos en las redes empresariales funcionan en las redes IP (SIP). Las arquitecturas telefónicas basadas en TDM requieren tener un punto de interconexión IP para poder tomar ventaja del software y/o servicios especializados en el mercado, que combinan el análisis en tiempo real, con el comportamiento histórico, y listas negras para ofrecer acciones de bloqueo, suspensión y redirección de llamadas en tiempo real. En ese sentido, las soluciones que basan su funcionamiento en Call Detail Records (CDRs) son lentas, imprecisas, costosas por requerir hardware para su ejecución, y sujetas a errores humanos, o dependientes de información que las hacen inefectivas. Del lado residencial, las soluciones son nulas o de muy baja penetración, y al igual que las soluciones móviles “no empresariales”, ofrecen bloqueos por listas negras con absolutamente nulo rigor en su construcción, por lo que el bloqueo es impreciso, intrusivo para las empresas legítimas e intrusivo para el usuario final pues consumen el historial de llamadas a través del otorgamiento de permisos poco claros en el smartphone. En ese sentido y de acuerdo al funcionamiento del ecosistema actual, puedo entonces enlistar: 1. Existencia de conmutadores tradicionales en un número aún muy importante de negocios. 2. Inexistencia de soluciones residenciales de calidad o interoperables con servicios FTTH. 3. Existencia de apps móviles gratuitas y de pago que lejos de cumplir con su promesa de valor, adquieren información del usuario final ofreciendo un alto nivel de imprecisión en el bloqueo, en detrimento de negocios legítimos. Desde el punto de vista del TELCO, considero que hay estás limitaciones importantes: 1. La gran capacidad TDM (SS7) aún en operación que impiden aprovechar las ventajas de las soluciones para redes SIP. 2. El alto volumen de tráfico que pudiera encarecer la implementación de soluciones para problemas que técnicamente no son un problema

No. de pregunta	Pregunta	Comentarios, opiniones o aportaciones
		prioritario pues no existe la motivación comercial, ni la obligación regulatoria de ofrecer soluciones.
6	¿Qué tecnologías y métodos identifica para detectar y bloquear llamadas no deseadas y/o llamadas de suplantación de identidad telefónica (spoofing)?	1. Analíticos de tráfico telefónico en tiempo real para la detección y el bloqueo de robocalls. 2. Firmado digital y verificación de origen de llamada, fuera de banda. 3. Políticas especiales de ruteo antiabuso de ANI en el Core TELCO. 4. Adopción del estándar STIR/SHAKEN. 5. Endurecimiento de los lineamientos “KYC” y prohibiciones para la entrega indiscriminada de DIDs por Carriers Tier1, Tier2 y Tier3, así como comercializadoras de servicios de telecomunicaciones. 6. Endurecimiento de las reglas y las sanciones para la obtención de SIMs prepago. 7. Recomendaciones o lineamientos oficiales (tal vez no obligatorios) para el mercado empresarial.

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?	Segmentando a los usuarios en: 1. Empresa privada de sector estratégico 2. Empresa pública de sector estratégico 3. Empresa privada 4. Micro y PyME 5. Usuario residencial 6. Usuario móvil Procedimientos que serán necesarios: **Reporte de suplantación**: El "usuario" reporta que su número telefónico está siendo utilizado por terceros para "X" objetivo. **Reporte de categorización incorrecta como SPAM:** El "usuario" reporta que su número telefónico está siendo incorrectamente identificado como SPAM en las terminales de identificador de llamada. **Reporte de recepción de SPAM**: El "usuario" reporta que está recibiendo llamadas de SPAM en sus líneas contratadas. **Solicitud de bloqueo de SPAM**: El "usuario" demanda que se ponga un alto a las llamadas de SPAM que está recibiendo en sus líneas. **Reporte de intento de fraude, estafa, engaño o extorsión**: El "usuario" reporta que ha recibido una o varias llamadas amenazantes en particular de uno o varios números. **Reporte de Saturación por robocalls**: El usuario reporta que sus líneas están colapsadas temporal, parcialmente o totalmente, a causa de la recepción de tormentas de llamadas desde uno, o varios números. **Reporte por saturación maliciosa:** El usuario reporta un ataque de denegación de servicio telefónico (TDoS) y solicita acciones de emergencia para bloquear el tráfico no solicitado y permitir la recepción de llamadas normales. **Colaboración y canales de comunicación** con: • CONDUSEF • PROFECO • SSP Federal y estatal (Policía cibernética)

No. de pregunta	Pregunta	Comentarios, opiniones o aportaciones
		• Fiscalías estatales o general.
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?	Afirmativo. Somos miembros de la Communications Fraud Control Association (CFCA) (www.cfca.org) y colaboramos con otros fabricantes líderes en la industria de la prevención de fraude en las telecomunicaciones, además de brindar consultoría y servicios expertos a Carriers Tier 2 y Tier 3 para el cumplimiento del TRACED Act en USA. (STIR/SHAKEN) Considero que la colaboración entre todos los operadores concesionados y las comercializadoras de servicios debe ser integrada en un Hub tecnológico y de información que posea autoridad para que, con todo el rigor técnico y administrativo, concentre la gestión de los procedimientos que se adopten para dicha colaboración, ya sea para el intercambio de información, la atención de los distintos escenarios descritos en la pregunta 7, así como para la ejecución de los roles de control y autoridad definidos tanto por STIR/SHAKEN como por otros mecanismos de verificación de llamadas “out-of-band”, y otros frameworks de cumplimiento anti-robocall y anti-spoofing. Existen mejores prácticas para la mitigación de las robocalls que no necesitan, ni interfieren con un potencial esfuerzo para implementar STIR/SHAKEN, y que, por el contrario, complementan y enriquecen de forma “inmediata” una potencial efectividad del estándar en el mediano y largo plazo. El intercambio de información entre operadores a través del mencionado Hub autorizado es una opción viable, administrative y tecnológicamente hablando pues el Hub ofrece servicios de información en tiempo real, y en alta capacidad, para la aplicación de dichos controles.

No. de pregunta	Pregunta	Comentarios, opiniones o aportaciones
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)?	1. Mejores prácticas para la mitigación de robocalls. Se adoptan de forma individual, y permite también la colaboración entre operadores. 2. Sistemas de verificación "fuera-de-banda" como servicio, para clientes empresariales de sectores estratégicos que son actualmente severamente afectados por el SPAM y por la suplantación telefónica. 3. Sistemas "como servicio" de gestión de identidad telefónica empresarial para centrales telefónicas (PBXs) y terminales móviles (smartphones, IoT, etc) 4. Repositorios rigurosos de listas negras para la consulta como servicio por parte de otros operadores y de empresas en general. 5. Servicios de filtrado de llamadas (scrubbing) en tiempo real. 6. Un estándar de verificación in-band, como STIR/SHAKEN (a *muy largo plazo, ambicioso y virtualmente medianamente efectivo en contra del mayor dolor del usuario final:* ***robo de datos y de identidad***) 7. Un estándar de verificación de llamadas out-of-band nacional, alineado con las leyes de protección de datos personales en posesión de particulares y a los estándares de seguridad de información, continuidad de negocio, sistemas anticorrupción, etc. 8. Adopción de tecnologías de "contenido enriquecido" para agregar datos adicionales a la llamada con el fin de generar confianza en el usuario final. (*te hablo para…)* 9. Habilitación desde fábrica de terminales móviles para ofrecer **un servicio NACIONAL** riguroso, controlado y experto de bloqueo de spam directamente en el smartphone o teléfono móvil.

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?	La generación de spam (llamadas no deseadas) y la suplantación telefónica están ligadas, pero no son interdependientes ni mutuamente excluyentes. La verificación de origen tampoco es dependiente ni mutuamente excluyente de los controles anti-robocall. Ambas conductas de abuso tienen orígenes diferentes, y si bien la adopción de medidas para la autenticación de identidad va a desincentivar el spam que se tolera bajo el amparo del negocio legítimo, pero poco ético, como es el caso de la cobranza o las televentas, no va a resolver propiamente ni directa ni indirectamente en su totalidad, el problema del fraude y estafa por ingeniería social (comúnmente llamado fraude guiado), mientras persistan los factores que habilitan al defraudador telefónico para actuar impunemente. En este sentido, adoptar medidas para la autenticación de identidad de origen puede coadyuvar a: 1. Evitar la suplantación de los números comerciales de sectores estratégicos que sin duda afectan los datos personales y la identidad de las personas (ej. bancos, aseguradoras, gobierno) (*este es 1 solo caso de uso del fraude telefónico*) 2. Elevar el nivel de rigor con el que se "identifican" ciertas llamadas como SPAM en el equipo terminal (smartphone). Se debe considerar que esta experiencia YA existe hoy, pero se hace por empresas INTERNACIONALES bajo ninguna regulación, ni observación de ninguna autoridad nacional, sin respeto por los datos personales de los usuarios, y con total carencia de rigor y compromiso por la exactitud. Nadie exige cuentas, ni audita la precisión con las que Google, y otras aplicaciones extranjeras "condenan" a la numeración nacional para ser spam ante los demás. 3. Evitar tramitar y completar llamadas que desde el Core no cumplan con el nivel de "atestación" requerido por los operadores, según está definido por STIR/SHAKEN. Este mecanismo limita el tráfico de baja calidad típicamente introducido por los agregadores de tráfico, con su respectivo impacto en el "*revenue*" o ingreso del operador, lo que podría generar resistencias para su adopción. ¿Algo mejor? Podemos partir de lo que no requiere cambios estructurales, ni adopción de estándar por todos los operadores, para mitigar el problema para el

No. de pregunta	Pregunta	Comentarios, opiniones o aportaciones
		usuario final en el corto plazo, mientras se prepara para una introducción del estándar que se perfila para ser eventualmente la regla a nivel internacional (en 10 o 15 años)

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)?	STIR/SHAKEN es el resultado de un trabajo arduo por parte de expertos en telefonía y encriptación y ha sido construido con el rigor necesario para ser considerado un estándar. Es posiblemente la única opción en la industria que se considere un estándar sobre el que puede pesar un mandato de cumplimiento, a diferencia de los SERVICIOS que, por definición, no se puede – posiblemente – obligar a adquirir, solo recomendar. STIR/SHAKEN está lejos de ser perfecto a juzgar por sus resultados en la unión americana. Si bien el ecosistema de operadores en USA es muy diferente al mexicano en número y complejidad, los resultados a la fecha, posteriores a la adopción de los grandes Carriers y a la expiración de las fechas para el cumplimiento de los "Gateway providers" y de los operadores más pequeños es: 1. Hubo una reducción **marginal** en el nivel de spam en general. 2. Se incremento de forma importante (*aunque posiblemente de forma temporal*) las quejas de usuarios legítimos respecto a que sus llamadas se marcaron indebidamente como spam. 3. Los operadores tecnológicos más grandes adoptaron tecnología e infraestructura para cumplir, sin embargo, existe tráfico internacional y de ciertos tipos de clientes agregadores que se firma "artificialmente" con el mayor nivel de atestación, como un acto de "asumir" responsabilidad sobre la llamada, aunque el nivel no corresponda a la legitima verificación del origen. 4. Los operadores más pequeños declararon cumplir exponiéndose a auditorias y/u observaciones que demuestren lo contrario. 5. El tráfico de numeración 800 o "sin costo de originación" es en su mayoría el que goza de un nivel mayor de atestación confiable entre los operadores. 6. El tráfico VoIP en general esta alrededor del 50% en su firma con el mayor nivel de atestación. 7. El fraude y la estafa por ingeniería social no ha demostrado una reducción, y el estándar no es propiamente la solución para esquemas nuevos de fraude basados en IA o desde tráfico internacional.

No. de pregunta	Pregunta	Comentarios, opiniones o aportaciones
		8. El estándar no cubre la gran deuda técnica que representa la capacidad TDM existente. 9. El camino aún es largo para lograr la inclusión de todos los puntos TDM y los nuevos modelos de colaboración (“X”aaS” que surgen mes a mes)

12	¿Qué retos técnicos, operativos y económicos considera de importancia para la implementación de soluciones de autenticación de llamadas, como STIR/SHAKEN?	Retos técnicos: • Elevar la iniciativa a nivel ley. • La exclusión automática de la capacidad TDM. • La actualización de infraestructura IP para soportar el estándar. • La selección de empresas con las capacidades para llevar a cabo los roles de autoridad del estándar, como la emisión de certificados, etc. • La potencial migración muy lenta a servicios IP. • El establecimiento de los canales de comunicación y la interoperabilidad en la interconexión entre operadores. Operativos: • La atención de quejas y solicitudes de aclaración por la imprecisión en las etapas tempranas de la implementación. • La capacitación o suficiencia de personal capacitado en las filas de los operadores. • Los aspectos inherentes de toda migración o renovación tecnológica como puntos de falla inexplorados, falta de capacidad de procesamiento o transmisión, problemas de calidad en el ruteo de llamadas, etc. Económicos • La inversión por parte del operador en la actualización de sus sistemas Core IP. • La inversión del operador para la transición de su capacidad TDM a IP. • La inversión del operador en la adopción de esquemas “fuera-de-banda” para incluir su capacidad TDM. • El impacto en el ingreso (“revenue”) por la disminución en la tramitación de las llamadas de spam de corta y larga duración que por definición se busca erradicar, y que actualmente aporta al ingreso de varios operadores. Lo anterior, sin contar con las resistencias que podrían surgir para solicitar ampliación de plazos que comprometan el alcance oportuno de los beneficios, o que

No. de pregunta	Pregunta	Comentarios, opiniones o aportaciones
		argumenten otro tipo de violaciones o excesos en función de una interpretación a modo de las leyes o de los reglamentos vigentes.
L	¿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?	Como he mencionado anteriormente en la descripción de las mejores prácticas para mitigar los robocalls, estas soluciones son sin duda complementarias y efectivas si se llevan a cabo por empresas profesionales con alto rigor en el procesamiento de sus políticas, y con las características de seguridad y protección de información que las condiciones actuales exigen. **Las aplicaciones en las "*app stores*" que no están respaldadas por servicios Carrier-grade, no son una opción a considerar al nivel de esta discusión de anteproyecto de lineamientos**. *AB Handshake* es un **servicio privado** basado en algunas de sus partes en la colaboración internacional, en sus otras funcionalidades antifraude (para diferentes tipos) y en su modelo de licenciamiento SaaS. Sus resultados en el mercado internacional demuestran que técnicamente su propuesta es técnicamente viable, pero siempre dependiente de la adopción global en las regiones de interés. Al ser un servicio privado, considero que la concesión como tal de un servicio con fines de obligatoriedad, forzosamente requeriría de una apertura neutral por parte del regulador, a cualquier otro proveedor de servicios nacional e internacional capaz de ofrecer un esquema "out-of-band" de capacidades similares. Finalmente, al ser estos, servicios privados, bastaría con establecer una recomendación neutral con fines de adopción de algún sistema de verificación de llamadas "fuera-de-banda" que demuestre cumplimiento con las funcionalidades requeridas, así como criterios de interoperabilidad y de viabilidad económica, de tal suerte que el operador goce de opciones para adherirse a la recomendación. Me parece que la opción de blockchain es prometedora, pero en etapas muy tempranas. Finalmente, considero que la tecnología blockchain estará presente dentro de la infraestructura de los proveedores de servicios de seguridad telefónica, y no debería propiamente verse como una opción con fines de adopción estandarizada, sino como una herramienta tecnológica que eventualmente estará a disposición de un operador como un método más, con las ventajas y retos naturales y propias del blockchain.

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)?	Considero que el análisis de las opciones hecho por el IFT en el documento amablemente puesto a disposición cubre las opciones más viables respecto a las opciones tecnológicas disponibles en el mercado. He procurado ser conciso en mis respuestas para justificar lo siguiente: 1. Existen metodologías y mejores prácticas de relativa fácil adopción que acotarían el problema de los robocalls y de la suplantación telefónica con mayor efectividad y en un plazo menor, sin la necesidad de la adopción de un estándar. Por lo que yo recomiendo amplia y enérgicamente explorar este como paso 1. 2. Las metodologías y mejores prácticas del punto anterior son prácticamente obligatorias y coexistentes a la potencial adopción de STIR/SHAKEN o cualquier otro esquema de verificación de origen in-band o out-of-band. 3. Considero que el sector empresarial "no-TELCO" debe ser concientizado enérgicamente para que adopte medidas que coadyuven a la mitigación del problema, empezando por identificar, restringir y sancionar a los generadores de spam. 4. La colaboración estrecha, efectiva y sin sesgos del IFT, la CNBV, la AMB, CONDUSEF, PROFECO, Secretarias de seguridad pública de los tres niveles de gobierno, así como las fiscalías general y estatales, así como otros organismos que representan a otros sectores industriales estratégicos, es una obligación para que el problema que verdaderamente afecta al usuario final (robo de datos y de identidad) sea atacado desde todos los frentes, y el esfuerzo a nivel telecomunicaciones no sea rápidamente invalidado por la evolución acelerada del criminal o abusador digital. 5. Es indispensable reconocer lo siguiente: *spam = molestia para el usuario*. *Suplantación = a riesgo inminente de perder patrimonio e identidad*. El enfoque de soluciones no debería entender el problema como uno solo. Son dos problemas de implicaciones y orígenes muy diferentes, con un factor común: la laxitud de las redes públicas de telefonía, exacerbados por un profundo desconocimiento y desinterés de la población en general, y un abuso sistematizado de ciertas verticales de negocio. 6. El problema es multifactorial pero su mitigación se logra si usamos tecnología contra el abuso tecnológico, y concientización contra el abuso

No. de pregunta	Pregunta	Comentarios, opiniones o aportaciones
		humano, en un ecosistema de colaboración, reglas claras, y cumplimiento de la ley en todos sus niveles.

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