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: info.upr@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 período de Consulta Pública será del Del 8 de enero al 5 de febrero de 2025 (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: Ricardo Martínez Salazar, Director de Desarrollo y Prospectiva Técnica Regulatoria, correo electrónico: ricardo.martinez@ift.org.mx o bien, a través del número telefónico 55 5015 4000, extensión 4161.

I. Datos de la persona participante	
Nombre, razón o denominación social:	Andrea Garcia Tapia
En su caso, nombre de la persona que funja como representante legal:	
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.	Elija un elemento.

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.

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

- 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"".

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: (06/01/2025)

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

Artículo o apartado	Comentario, opiniones o aportaciones

Nota: añadir cuantas filas considere necesarias.

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

Nota: añadir cuantas filas considere necesarias.

PROPUESTA DE ACCIONES PARA LA ATENCIÓN DE EMERGENCIAS

Antecedentes:

En el marco de la consulta pública del "Anteproyecto de Lineamientos de actuación de los concesionarios y autorizados ante la ocurrencia de situaciones de Emergencia o Desastre" se presentan recomendaciones para el manejo de datos provenientes del sector de telecomunicaciones en caso de desastres o emergencias.

Objetivo:

En el contexto del rápido avance en las tecnologías de telecomunicación, en particular su uso para comprender comportamientos y movilidad humana, es pertinente revisitar los Planes Nacionales de Telecomunicaciones de Emergencia (PNTEs) para darles un enfoque que potencie el uso de datos de telecomunicación en la respuesta a emergencias. El Protocolo de Actuación en consulta pública puede incluir el manejo de los datos de las concesionarias para dar una mejor atención a desastres.

Contexto:

Los PNTEs describen los protocolos para el mantenimiento y uso de *recursos de telecomunicación*. Estos protocolos se conciben a través de la creación del Comité Sectorial de Gestión del Riesgo en Telecomunicaciones, cuya función es garantizar la cooperación entre los diferentes actores del sector de telecomunicaciones. Actualmente, los protocolos propuestos únicamente lidian con *recursos en función de infraestructura de telecomunicaciones*, creando la necesidad de incluir protocolos para el intercambio y el uso de *recursos informáticos*, es decir, de los datos generados por el sector de telecomunicaciones. Estos datos incluyen, pero no están limitados, a registros de detalles de llamadas (CDR) y datos de posición móvil (MPD).

A continuación se presenta una lista de actividades críticas identificadas por CrisisReady. Estas actividades incluyen actividades ya incluidas en los PNTEs y unas adicionales específicas al intercambio de datos de telecomunicación en emergencias:

1. Elaboración de un mapa del país identificando las zonas de mayor vulnerabilidad. La información aquí mencionada debe validarse, trabajarse y compartirse con las autoridades responsables de la protección civil.

2. Realizar un levantamiento de las redes tanto públicas como privadas, sobre todo en zonas vulnerables.
3. Identificar operadores por zona de cobertura y de servicio (tanto de redes públicas como privadas).
4. Identificar posibles fuentes de datos de telecomunicación, incluyendo su estructura y metadata por zona de cobertura y de servicio (tanto de redes públicas como privadas).
5. Contar con información sobre la capacidad de reserva de los operadores.
6. Desarrollar un plan de priorización de llamadas para uso de las autoridades competentes.
7. Coordinar acercamientos con instituciones clave para el manejo de emergencias.
8. Revisar el marco jurídico nacional con el objetivo de poder implementar un Plan Nacional de Emergencias.
9. Revisar el marco jurídico nacional con el objetivo de poder regular el uso de datos de telecomunicaciones para el manejo de emergencias.
10. Formalizar los nombres o cargos de las personas que pueden fungir como puntos de contacto dentro de las instituciones que integran los diversos esquemas de coordinación en casos de emergencia.
11. Analizar las posibles sinergias y eventuales acuerdos binacionales o multilaterales que potencien las capacidades de los países para atender las emergencias.
12. Impulsar la creación de un protocolo de importación y reexportación de equipos de telecomunicaciones para casos de emergencia, apoyado en acuerdos binacionales o regionales.
13. Conformar un Comité de Emergencia. Es fundamental agregar, además de los integrantes propuestos, por lo menos dos integrantes dedicados a la administración de datos y el diseño y mantenimiento de los flujos de datos. Uno de estos integrantes estará encargado de la administración de datos por parte de las agencias de respuesta a emergencias y el otro deberá tener el rol equivalente para los operadores de servicios de telecomunicación. Ver sección *Comité de Emergencia en Telecomunicaciones*.
14. Realizar un inventario de los datos de telecomunicaciones disponibles, así como los estándares de recolección, la estructura y metadatos de los mismos, y cualquier otra especificación técnica necesaria para entender los datos y los requerimientos computacionales para procesarlos.

15. Desarrollar protocolos que garanticen la privacidad en cuanto al uso de datos de telecomunicación.
16. Generar estandarización de métricas a utilizar y definir qué actor va a procesar los datos.
17. Impulsar la creación del rol profesional de Administrador de Datos tanto en el IFT como en las agencias nacionales de respuesta a emergencias. Ver sección *Perfil de administrador de datos*.
18. Impulsar la creación de acuerdos de intercambio de datos entre los proveedores de servicios de telecomunicación y las agencias de respuesta. Ver sección *Acuerdos de intercambio de datos* .

Comité de Emergencia en Telecomunicaciones

En complementación a la estructura propuesta para el Comité de Emergencia en Telecomunicaciones de los PNTEs existentes, se recomienda complementar con lo siguiente para robustecer el intercambio de datos de telecomunicación.

1. Incorporar un administrador de datos al comité cuya función sea supervisar y promover el intercambio de datos con el fin de potenciar el uso para informar la respuesta a emergencias. Este rol idealmente es llevado por un profesional afiliado con el IFT. Ver sección de *Perfil de administrador de datos*.

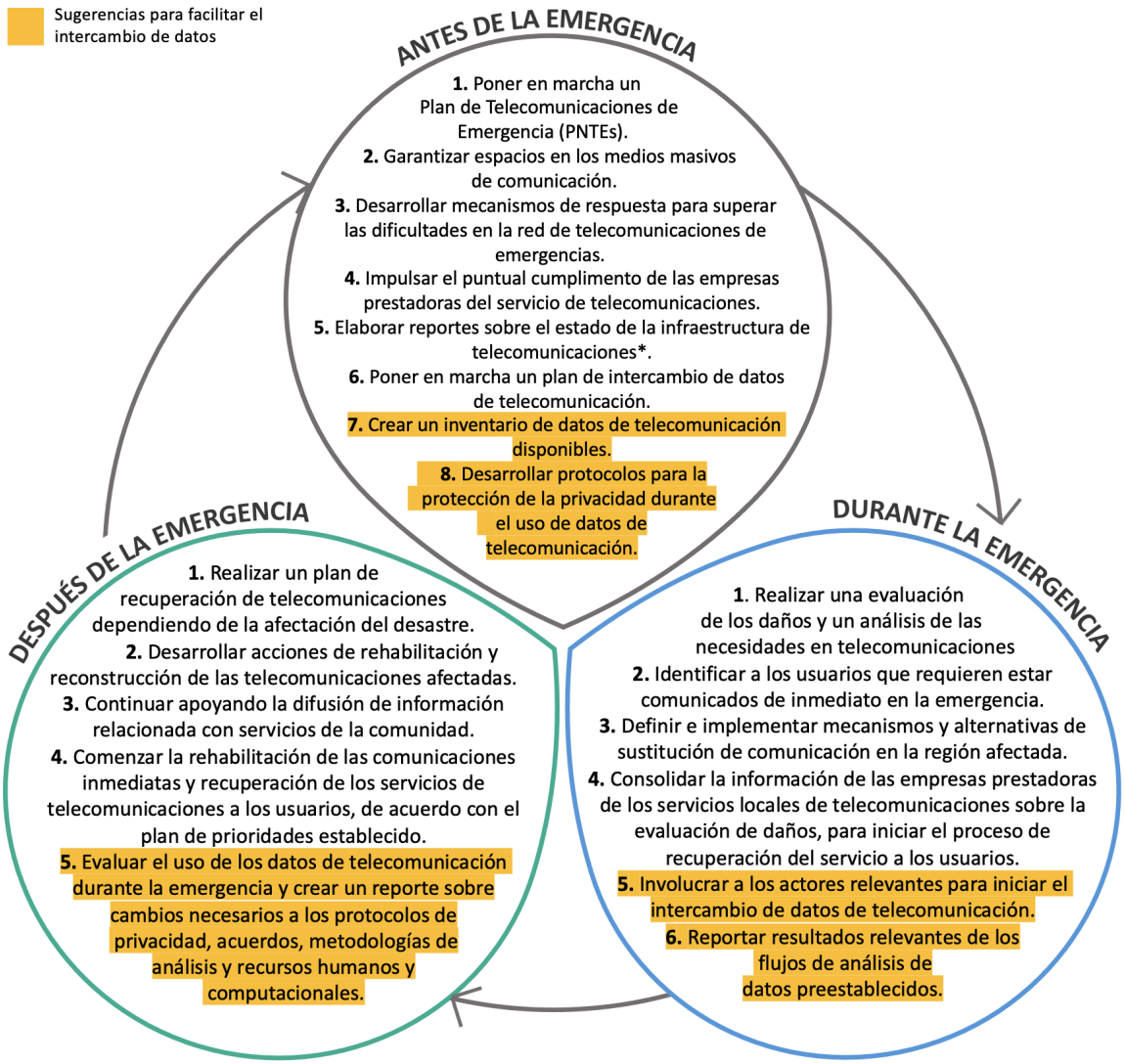


Figura 1. Responsabilidades del Comité de Emergencias en Telecomunicaciones. Contenido extraído de los actuales PNTEs, y complementado con el enfoque de intercambio de datos.

Perfil de administrador de datos

El perfil de administrador de datos, más que el rol tradicional de administrar datos internos, se entiende como un rol de alto nivel que busca aprovechar fuentes de datos para crear valor de interés público. Su tarea principal es generar colaboraciones entre diferentes actores para crear flujos de datos sostenibles, transparentes y eficaces, por lo cual *deben tener amplio conocimiento de gobernanza de datos*[1].

[1] El concepto se traduce del inglés “data steward” que tiene connotación no solo de “administrador de datos”, sino también de “guardián de los datos”. Para más información, consultar: https://thegovlab.org/static/files/publications/wanted-data-stewards.pdf

Roles del administrador de datos:

1. Buscar e involucrar socios viables para catalizar la creación de colaboraciones que generen hallazgos de interés público. En este caso, colaboraciones que optimicen el manejo de emergencias.
2. Involucrar a los beneficiarios durante el ciclo de vida de los datos. En este caso, los beneficiarios serán las agencias nacionales de respuesta a emergencias. El administrador de datos debe asegurarse que cualquier hallazgo generado tenga una implementación viable dentro de la misión específica de estas agencias.
3. Coordinar a los actores internos para establecer los protocolos y flujos de datos necesarios. Esto incluye sistematizar aprobaciones legales y técnicas.
4. Monitorear y evaluar el valor, potencial y riesgo de diferentes fuentes de datos. Es fundamental que el administrador tenga conciencia de cualquier implicación ética tanto de los datos mismos como de las metodologías usadas para procesarlos.
5. Diseminar y comunicar los hallazgos encontrados. Frecuentemente, el administrador de datos será responsable de la comunicación entre usuarios, beneficiarios, socios, y demás actores.
6. Anclar cualquier iniciativa de colaboración en las misiones, visiones y necesidades de las organizaciones involucradas. Esto con el propósito de prevenir que las iniciativas colapsen por estar desalineadas con los intereses específicos de las partes.

Acuerdos de intercambio de datos

El marco de cooperación que se defina para el intercambio de datos determinará a los responsables de cargar el costo de las operaciones, la usabilidad de los datos, la transparencia en los flujos de análisis y la disposición misma de los actores.[2] Marcos de cooperación que ubican a actores no gubernamentales para mediar la interacción entre proveedores de datos y usuarios gubernamentales son más robustos en cara a mantener estándares de privacidad y protección de datos.[3] En el diagrama usamos al CEPREDENAC Centro de Coordinación para la Prevención de los Desastres en América Central y República Dominicana, pero se puede reemplazar por otro centro de investigación u organismo internacional.

[2] Ver: https://unstats.un.org/wiki/display/MPDDS

[3] Ver: CrisisReady's novel framework for transdisciplinary translation: Case-studies in wildfire and hurricane response

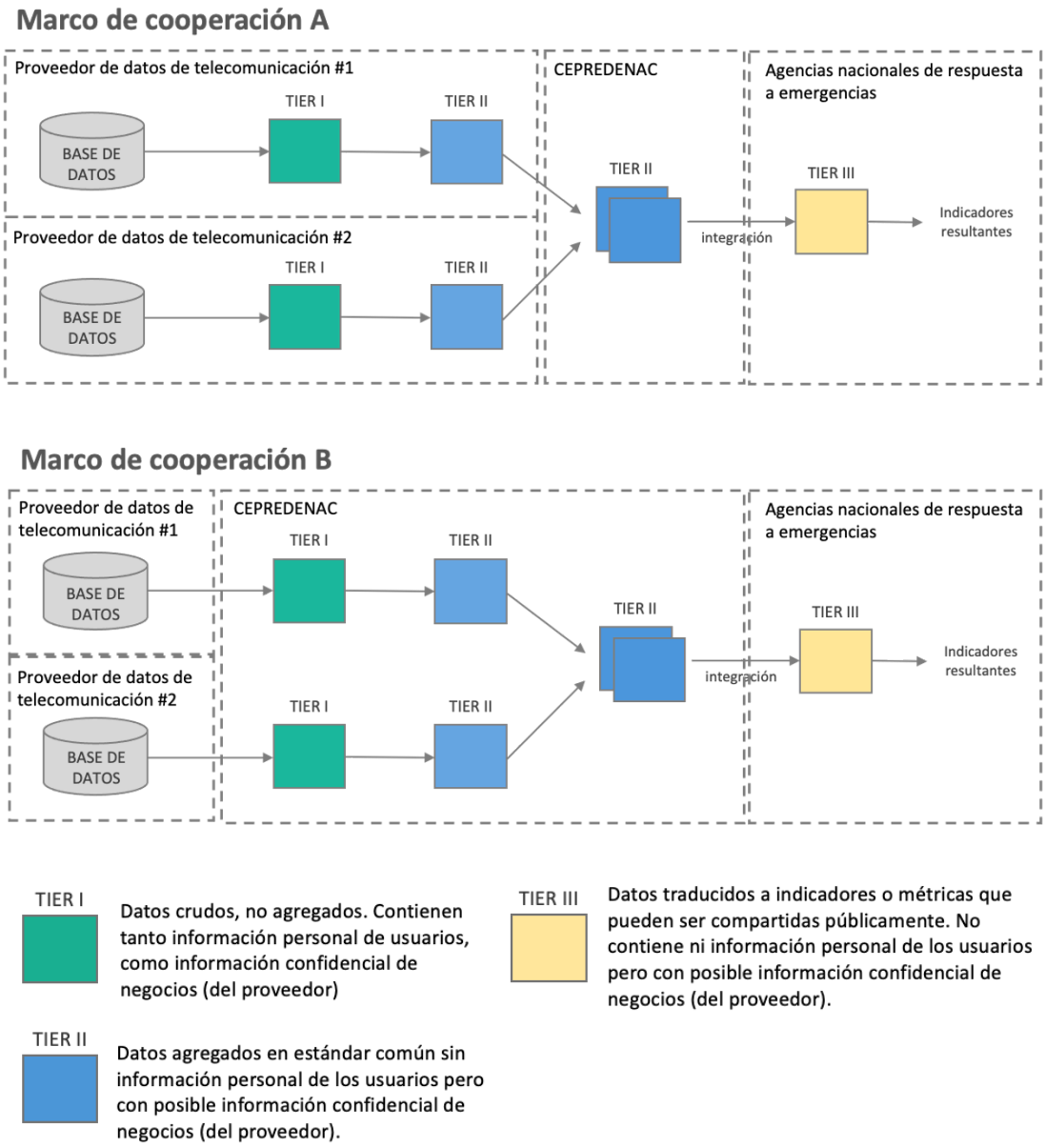


Figura 2. Posibles marcos de cooperación entre proveedores de datos de telecomunicación y usuarios gubernamentales. Un tipo híbrido consistiría en mantener los datos en las instalaciones del proveedor de datos, pero dando acceso constante a científicos o administradores de datos CEPREDENAC. Adaptado del Manual de uso de datos móviles en estadísticas oficiales[4].

[4] Ver: https://unstats.un.org/bigdata/task-teams/mobile-phone/MPD%20Handbook%2020191004.pdf

Lo siguiente es una lista de recomendaciones sobre lo mínimo necesario para poder entablar una cooperación de intercambio de datos de telecomunicación en momentos de crisis.

1. Es necesario escoger un marco de cooperación que se adhiera al marco legal existente en materia de privacidad.
2. Es necesario acordar términos administrativos y legales que lidien con:
    a. Protocolos de privacidad y protección de confidencialidad de negocio (de los proveedores).
    b. Estándares de estructura de los datos, así como protocolos de transferencia de estos.
    c. Las responsabilidades específicas de cada parte, en términos de costos, procesamiento de datos, y propiedad intelectual de metodologías de análisis y resultados.
    d. Metodologías aceptables para el procesamiento de los datos.
3. Es necesario desarrollar capacidad instalada en cuestión de recursos humanos y computacionales para el almacenamiento y procesamiento de los datos.
4. Es necesario contar con por lo menos un administrador de datos que facilite la colaboración entre diferentes actores y administre y supervise el ciclo de vida de los datos.
5. Es necesario establecer protocolos que garanticen la transparencia sobre las fuentes de los datos y métodos de agregación, para poder evaluar sesgos y representatividad.

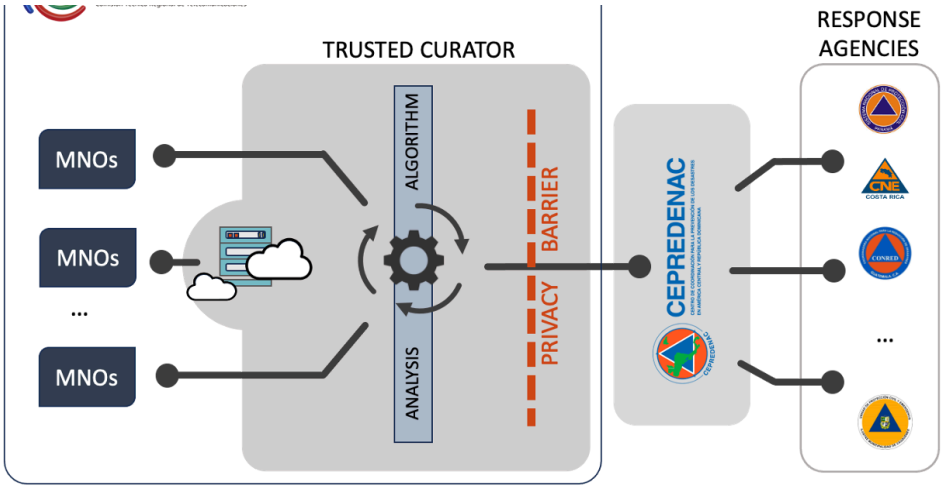
Actores and Roles:

- **Proveedores de Datos:** Operadores de Redes Móviles comprometidos a compartir de manera segura sus datos de telecomunicaciones.
- **Reguladores Nacionales:** Supervisarán los acuerdos de intercambio a nivel local y su cumplimiento.
- **IFT:** Encargada de promover la inclusión de los acuerdos de intercambio de datos en los planes nacionales de respuesta y mitigación de desastres.
- **CEPREDENAC o CENAPRED:** Compartirá la gobernanza sobre el análisis e informes generados por el marco durante una respuesta a desastres.
- **CrisisReady:** Encargada de las tareas algorítmicas y analíticas dentro del marco, creando los scripts y procedimientos necesarios para ayudar en la toma de decisiones durante una respuesta a desastres. Además, garantizará la privacidad del usuario, asegurando que los resultados cumplan con las normas de privacidad.
- **AWS:** Tendrá la gobernanza técnica sobre el marco en su conjunto y sus partes.

- **Agencias Locales de Respuesta de Emergencia:** serán el usuario final del marco, recibiendo información analítica a través de CENAPRED para respaldar las respuestas a desastres.

Gobernanza de datos

Los operadores de red cargan datos en un servidor seguro en la nube, donde algoritmos de procesamiento acordados permitirán procesarán dichos datos para extraer métricas de movilidad relevantes. Los datos en sí no se compartirán. Más bien, el marco estará federado de tal manera que permita que los análisis se ejecuten sobre conjuntos de datos protegidos, que hayan sido autorizados para uso durante emergencias. Estos algoritmos deben cumplir con estándares de privacidad diferencial por sí mismos o incorporar un muro de privacidad adicional que garantice la privacidad diferencial. Las métricas calculadas serán accedidas por CENAPRED, quien las compartirá a su discreción con agencias nacionales de respuesta. IFT, junto con otros reguladores federales, dará supervisión para asegurar que se respeten los marcos legales locales.



Caso de uso

Un caso de uso clave es el uso de tendencias de movilidad a partir de datos de telecomunicaciones para comprender fluctuaciones en la población durante una emergencia. Esto permite monitorear la respuesta y la asignación de recursos. Los proveedores de datos, bajo condiciones acordadas, subirán sus datos al sistema. Posteriormente, una serie de modelos generarán información casi en tiempo real mostrando tendencias de movilidad y cambios de densidad poblacional cerca de áreas de interés. Esta información se compartirá a través de paneles o informes y se transmitirán a agencias locales de respuesta a través de CENAPRED. Una vez concluida la emergencia, los datos de movilidad no procesados se eliminarán.

Consideraciones de privacidad

Dada la naturaleza sensible de los datos, tanto por razones de privacidad como de inteligencia empresarial, la infraestructura propuesta debe adherirse a las mejores prácticas.

a. **Curador de confianza (Trusted curator)**
   Un curador de confianza es un intermediario entre los proveedores de datos y los usuarios de datos. Su función es mantener los datos a salvo de adversarios. La barrera de privacidad, que garantizará la privacidad diferencial, se aplica a todo, lo que significa que la información nunca está disponible para nadie más que los proveedores y el curador de confianza. El curador de confianza suele ser un servidor seguro (en la nube) donde se cargan los datos para procesarlos más tarde.

b. **Privacidad diferencial**
   La privacidad diferencial es una definición matemáticamente rigurosa de la privacidad, donde las estadísticas de la población general están disponibles, mientras que la información a nivel individual permanece oculta. Se dice que un algoritmo es diferencialmente privado si, al observar la salida del algoritmo, es imposible decir si se utilizó un registro específico como entrada. Esto puede convertirse en un desafío una vez que se combinan varias fuentes de información o cuando hay registros particularmente identificables.