INFORME DE EJECUCIÓN DEL PROCESO DE CONSULTAS PÚBLICAS DE LA PROPUESTA DE "REFORMA A LA NORMA TÉCNICA QUE REGULA LAS CONDICIONES GENERALES DE LOS CONTRATOS DE ADHESIÓN, DEL CONTRATO NEGOCIADO CON CLIENTES, Y DEL EMPADRONAMIENTO DE ABONADOS Y CLIENTES"

INFORME TÉCNICO No. IT-CRDS-GR-2025-0039

11 de julio de 2025

1. PROYECTO DE REGULACIÓN

PROPUESTA DE "REFORMA A LA NORMA TÉCNICA QUE REGULA LAS CONDICIONES GENERALES DE LOS CONTRATOS DE ADHESIÓN, DEL CONTRATO NEGOCIADO CON CLIENTES, Y DEL EMPADRONAMIENTO DE ABONADOS Y CLIENTES".

2. ANTECEDENTES

2.1. Mediante memorando Nro. ARCOTEL-CREG-2025-0298-M de 05 de junio de 2025, la Dirección Ejecutiva de la ARCOTEL puso a consideración y aprobación del Director Ejecutivo de ARCOTEL el Informe Técnico No. IT-CRDS-GR-2025-0032 de 05 de junio de 2025, el proyecto de resolución "REFORMA A LA NORMA TÉCNICA QUE REGULA LAS CONDICIONES GENERALES DE LOS CONTRATOS DE ADHESIÓN, DEL CONTRATO NEGOCIADO CON CLIENTES, Y DEL EMPADRONAMIENTO DE ABONADOS Y CLIENTES", el Informe jurídico No. ARCOTEL-CJDA-2025-0019 de 29 de mayo de 2025, aprobado por la Coordinación General Jurídica para su consideración, y de considerarlo pertinente, disponga el inicio del proceso de consulta pública respectivo, en aplicación a lo dispuesto en el Reglamento de Consultas Públicas emitido con Resolución Nro. 003-03-ARCOTEL-2015 de 15 de mayo de 2015.

2.2. La Dirección Ejecutiva de la ARCOTEL, mediante sumilla inserta en el memorando Nro. ARCOTEL-CREG-2025-0298-M 05 de junio de 2025, autorizó y dispuso a la Coordinación Técnica de Regulación, ejecutar el procedimiento de consultas públicas, para la emisión de la resolución de "REFORMA A LA NORMA TÉCNICA QUE REGULA LAS CONDICIONES GENERALES DE LOS CONTRATOS DE ADHESIÓN, DEL CONTRATO NEGOCIADO CON CLIENTES, Y DEL EMPADRONAMIENTO DE ABONADOS Y CLIENTES", con sujeción a la Disposición General Primera de la Ley Orgánica de Telecomunicaciones, que regula el procedimiento de consultas públicas.

2.3. Mediante memorando Nro. ARCOTEL-CREG-2025-0303-M de 09 de junio de 2025, la Coordinación Técnica de Regulación, en atención a la sumilla inserta en el memorando Nro. ARCOTEL-CREG-2025-0298-M, solicitó a la Responsable de la Unidad de Comunicación Social, realizar el día 09 de junio de 2025, la publicación de la convocatoria a la audiencia pública del proyecto de "REFORMA A LA NORMA TÉCNICA QUE REGULA LAS CONDICIONES GENERALES DE LOS CONTRATOS DE ADHESIÓN, DEL CONTRATO NEGOCIADO CON CLIENTES, Y DEL EMPADRONAMIENTO DE ABONADOS Y CLIENTES", el respectivo informe técnico, y el formulario para las observaciones. Se publicó hasta el 19 de junio de 2025, siendo ésta la fecha límite para la recepción de opiniones, recomendaciones y/o comentarios de la ciudadanía en general.

2.4. Mediante memorando Nro. ARCOTEL-DECS-2025-0100-M de 12 de junio de 2025, la Unidad de Comunicación Social informó que:

"Con base en lo solicitado en el memorando ARCOTEL-CREG-2025-0303-M, cumplo con indicar que se realizó publicación de la convocatoria a la audiencia pública del proyecto normativo de "REFORMA A LA NORMA TÉCNICA QUE REGULA LAS CONDICIONES GENERALES DE LOS CONTRATOS DE ADHESIÓN, DEL CONTRATO NEGOCIADO CON CLIENTES, Y DEL EMPADRONAMIENTO DE ABONADOS Y CLIENTES", cumplo con informar que se realizó la publicación el 09 de junio de 2025, en el sitio web institucional y puede ser revisado en el siguiente link:

http://sisap.arcotel.gob.ec/preguntas/95/reforma-a-la-norma-tecnica-que-regula-las-condiciones-generales-de-los-contratos-de-adhesion-del-contrato-negociado-con-clientes-y-del-empadronamiento-de-abonados-y-clientes

Informe:
https://www.arcotel.gob.ec/wp-content/uploads/2025/06/it-crds-gr-2025-0032_proyecto_informe_ver_1-signed-signed-signed04053700017492410 71.pdf

Proyecto de resolución:
https://www.arcotel.gob.ec/wp-content/uploads/2025/06/proyecto_resoluciOn_reforma_ver_1.doc

Formulario de observaciones:
https://www.arcotel.gob.ec/wp-content/uploads/2025/06/formulario-observaciones-propuesta-normativa07518710017492410 71.xls

2.5. Las observaciones y comentarios al proyecto de reforma, recibidas durante el tiempo estipulado 19 de junio de 2025, fueron las siguientes:

- ***DINARP,*** *mediante oficio DINARP-DINARP-2025-0380-OF recibido mediante el Sistema de Gestión Documental (Quipux) el 18 de junio de 2025.*
- ***ASETEL,*** *con oficio Nro. 089-AS-2025 recibido mediante correo electrónico el 19 de junio de 2025.*
- ***OTECEL,*** *con oficio VPR-32765-2025 recibido mediante correo electrónico el 19 de junio de 2025.*
- ***CNT EP,*** *con oficio Nro. CNTEP-GNARI-RG-2025-0361-O recibido mediante correo electrónico y mediante el Sistema de Gestión Documental (Quipux), el 19 de junio de 2025.*
- ***MEGADATOS,*** *con oficio Nro. MD-2025-077 recibido mediante correo electrónico el 19 de junio de 2025.*
- ***CONECEL,*** *con oficio DR- 0436-2025 recibido mediante correo electrónico el 19 de junio de 2025.*
- ***PUNTONET,*** *con oficio Nro. PUNTONET-2025-SAI-INF-015 recibido mediante el Sistema de Gestión Documental (Quipux) el 19 de junio de 2025.*

2.6. Con memorando Nro. ARCOTEL-CREG-2025-0339-M de 23 de junio de 2025, la Coordinación Técnica de Regulación solicitó a la Responsable de la Unidad de Comunicación Social, realice la publicación de las observaciones realizadas por parte de los prestadores y asociaciones del sector del proyecto de "REFORMA A LA NORMA TÉCNICA QUE REGULA LAS CONDICIONES GENERALES DE

LOS CONTRATOS DE ADHESIÓN, DEL CONTRATO NEGOCIADO CON CLIENTES, Y DEL EMPADRONAMIENTO DE ABONADOS Y CLIENTES".

2.7. Mediante memorando Nro. ARCOTEL-DECS-2025-0111-M de 23 de junio de 2025, el Responsable de la Unidad de Comunicación Social informó que se publicaron las observaciones y comentarios recibidos en página Web de consultas públicas de la ARCOTEL:

http://sisap.arcotel.gob.ec/preguntas/95/reforma-a-la-norma-tecnica-que-regula-las-condiciones-generales-de-los-contratos-de-adhesion-del-contrato-negociado-con-clientes-y-del-empadronamiento-de-abonados-y-clientes

https://www.arcotel.gob.ec/wp-content/uploads/2025/06/dinarp-dinarp-2025-0380-of0826245001750693968.pdf

https://www.arcotel.gob.ec/wp-content/uploads/2025/06/dinarp_-_formulario-observaciones-propuesta-normativa013103800175069396 9.xls

https://www.arcotel.gob.ec/wp-content/uploads/2025/06/asetel_-_089-as-2025_06_19_observaciones_norma_contratos.pdf

https://www.arcotel.gob.ec/wp-content/uploads/2025/06/asetel_-_2025_06_19_matriz_comentarios_asetel.xls

https://www.arcotel.gob.ec/wp-content/uploads/2025/06/otecel_-_2025_06_19_observaciones_reformas_norma_de_contratos.pdf

https://www.arcotel.gob.ec/wp-content/uploads/2025/06/otecel_-_formulario-observaciones-propuesta-normativa_otecel.xls

https://www.arcotel.gob.ec/wp-content/uploads/2025/06/cntep_-_gnari-rg-2025-0361-o.pdf

https://www.arcotel.gob.ec/wp-content/uploads/2025/06/cntep_-_copia_de_18_jun_observaciones_cnt_-arcotel_final.xls

https://www.arcotel.gob.ec/wp-content/uploads/2025/06/megadatos_-_md-2025-077_observaciones_al_proyecto_de_actualizacion_a_la_norma_tecnica-signed.pdf

https://www.arcotel.gob.ec/wp-content/uploads/2025/06/megadatos_-_formulario-observaciones-propuesta-normativa_megadatos.xls

https://www.arcotel.gob.ec/wp-content/uploads/2025/06/conecel_-_2025_06_19_oficio_dr-0436-2025_-_observaciones.pdf

https://www.arcotel.gob.ec/wp-content/uploads/2025/06/puntonet_-_formulario-observaciones_de_puntonet_s.a.xls

2.8. El 25 de junio de 2025, a partir de las 10h00 se efectuó la audiencia pública presencial, conforme a la convocatoria realizada.

3. APORTES RECIBIDOS EN EL PROCESO DE CONSULTAS PÚBLICAS

En la publicación realizada el 9 de junio de 2023, en aplicación del Reglamento de consultas públicas (Resolución No. 003-03-ARCOTEL-2015), se otorgó el término de ocho días, es decir hasta el 19 de junio de 2023, para que se remitan las observaciones, opiniones y comentarios a la propuesta regulatoria, por medio de correo electrónico o por escrito en la Agencia de Regulación y Control de las Telecomunicaciones.

De acuerdo con la información recibida al correo electrónico institucional consulta.publica@arcotel.gob.ec y en el sistema de Gestión Documental Quipux, se determina que se recibieron de siete entidades opiniones, recomendaciones y comentarios, de acuerdo al siguiente detalle:

- ***DINARP,*** *mediante oficio DINARP-DINARP-2025-0380-OF recibido mediante el Sistema de Gestión Documental (Quipux) el 18 de junio de 2025.*
- ***ASETEL,*** *con oficio Nro. 089-AS-2025 recibido mediante correo electrónico el 19 de junio de 2025.*
- ***OTECEL,*** *con oficio VPR-32765-2025 recibido mediante correo electrónico el 19 de junio de 2025.*
- ***CNT EP,*** *con oficio Nro. CNTEP-GNARI-RG-2025-0361-O recibido mediante correo electrónico y mediante el Sistema de Gestión Documental (Quipux), el 19 de junio de 2025.*
- ***MEGADATOS,*** *con oficio Nro. MD-2025-077 recibido mediante correo electrónico el 19 de junio de 2025.*
- ***CONECEL,*** *con oficio DR- 0436-2025 recibido mediante correo electrónico el 19 de junio de 2025.*
- ***PUNTONET,*** *con oficio Nro. PUNTONET-2025-SAI-INF-015 recibido mediante el Sistema de Gestión Documental (Quipux) el 19 de junio de 2025.*

4. REALIZACIÓN DE LA AUDIENCIA PÚBLICA PRESENCIAL

La audiencia pública se realizó desde las 10H00 hasta las 12H35 del 25 de junio de 2025, de manera presencial en el Auditorio ubicado en la Av. Amazonas N40-71 y Gaspar Villarroel, en la ciudad de Quito.

Asistieron las siguientes personas:

N°	ENTIDAD	REPRESENTANTE
1	ASETEL	Patricia Falconí
2	ASOCIACIÓN ECUATORIANA DE PROTECCIÓN DE DATOS - AEPD	Lorena Naranjo Godoy
3	CONECEL	Simón Zevallos
4	CONECEL	María Belén Cárdenas
5	CNT EP	Giovana Méndez
6	CNT EP	Catalina Gonzalez

7	CNT EP	Natalia Martínez
8	DINARDAP	Jean Cifuentes
9	MEGADATOS S.A	Romel Espinosa
10	MEGADATOS S.A	Edison Patricio Sánchez Mendez
11	OTECEL MOVISTAR	Estaefanía Majo
12	OTECEL MOVISTAR	Fernando Palacios
13	OTECEL MOVISTAR	Beatriz Tato Gonzalez
14	PUNTONET S.A.	Daniel Paillacho
15	PUNTONET S.A.	Olivier Monjaret
16	SUPERINTENDENCIA DE PROTECCIÓN DE DATOS PERSONALES -SPDP	Camila Valdez González
17	SUPERINTENDENCIA DE PROTECCIÓN DE DATOS PERSONALES -SPDP	David Sánchez Matovelle
18	SUPERINTENDENCIA DE PROTECCIÓN DE DATOS PERSONALES -SPDP	René Orbe

En la audiencia pública del 25 de junio de 2025, se receptaron, adicionalmente a las observaciones presentadas hasta el 19 de junio de 2025, observaciones de la Superintendencia de Protección de Datos Personales de manera verbal y mediante oficio Nro. SPDP-SPD-2025-341-O.

5. ANÁLISIS DE LOS APORTES RECIBIDOS EN EL PERÍODO DE LA CONSULTA PÚBLICA

A continuación, se realiza un análisis de las observaciones de manera general recibidas del proyecto de “REFORMA A LA NORMA TÉCNICA QUE REGULA LAS CONDICIONES GENERALES DE LOS CONTRATOS DE ADHESIÓN, DEL CONTRATO NEGOCIADO CON CLIENTES, Y DEL EMPADRONAMIENTO DE ABONADOS Y CLIENTES”, los cuales no tienen carácter de vinculantes para la ARCOTEL, y en función de su pertinencia, se realizarán los ajustes en el proyecto de resolución. Adicionalmente, es necesario señalar que el análisis por articulado, se presenta en el documento denominado “Cuadro de análisis por formulario-observaciones-propuesta-normativa-consolidada.xls”, adjunto al presente documento.

5.1. OBSERVACIONES GENERALES

En referencia a las observaciones recibidas a través del correo consulta.pública@arcotel.gob.ec o ingresadas a la ARCOTEL, y las expresadas y/o reiteradas en la audiencia pública del 25 de junio de 2025, al proyecto de “REFORMA A LA NORMA TÉCNICA QUE REGULA LAS CONDICIONES GENERALES DE LOS CONTRATOS DE ADHESIÓN, DEL CONTRATO NEGOCIADO CON CLIENTES, Y DEL EMPADRONAMIENTO DE ABONADOS Y CLIENTES” a continuación se realiza el análisis respectivo a las consideraciones generales emitidas:

1. **ARMONIZACIÓN CON LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP):**

OBSERVACIÓN:

Es fundamental que cualquier propuesta de reforma o nueva normativa técnica (como la de ARCOTEL) evite duplicar o contradecir lo ya establecido en la Ley Orgánica de Protección de Datos Personales (LOPDP).

Actualmente, los prestadores de servicios ya están obligados a garantizar la privacidad y protección de los datos personales, permitiendo a los usuarios autorizar o rechazar su tratamiento conforme a la LOPDP. Introducir nuevas disposiciones que se superpongan con esta ley integral generaría incertidumbre, afectaría su correcta aplicación y obstaculizaría la labor de los entes de control (Superintendencia de Protección de Datos Personales - SPDP y ARCOTEL).

La reforma propuesta debe alinearse con la sentencia de la Corte Constitucional y mantener su enfoque específico en telecomunicaciones, respetando la autonomía de los reguladores.

Se enfatiza la importancia de una armonización completa de la nueva norma técnica de ARCOTEL con la LOPDP. Esto implica alinear la propuesta con los principios, derechos, obligaciones y mecanismos de tutela ya definidos en la ley, prestando especial atención a:

- El consentimiento del usuario para el tratamiento de sus datos.
- La finalidad del tratamiento de dichos datos.
- Los periodos de conservación de la información.
- El rol del encargado del tratamiento de datos.

Este enfoque asegura la coherencia legal y la protección efectiva de los datos personales de los ciudadanos.

RESPUESTA:

Conforme lo establece la Ley Orgánica de Protección de Datos Personales (LOPDP):

La entidad competente para el control del cumplimiento de la LOPDP es la Autoridad de Protección de Datos Personales (APDP), si bien ARCOTEL tiene competencias en telecomunicaciones y puede estar involucrada en aspectos específicos de datos en su sector, la LOPDP establece una autoridad principal para velar por el cumplimiento general de la ley, que es la Superintendencia de Protección de Datos Personales (SPDP), o la Autoridad de Protección de Datos Personales, encargada de la supervisión y control.

De manera general, la LOPDP contempla y regula los siguientes aspectos fundamentales:

- **Principios para el tratamiento de datos personales:** Establece las bases éticas y legales bajo las cuales se deben manejar los datos, como la legalidad, lealtad, transparencia, minimización de datos, limitación de la finalidad, exactitud, limitación del plazo de conservación, integridad, confidencialidad, y responsabilidad proactiva.
- **Derechos de los titulares de datos:** Reconoce y garantiza una serie de derechos a los ciudadanos sobre su información personal, incluyendo el derecho a la información, acceso, rectificación y actualización, eliminación, oposición, portabilidad, suspensión del tratamiento y a no ser objeto de decisiones basadas únicamente en valoraciones automatizadas.
- **Obligaciones de los responsables y encargados del tratamiento:** Define las responsabilidades de quienes manejan datos personales, incluyendo la implementación de medidas de seguridad técnicas y organizativas adecuadas para proteger los datos, la necesidad de obtener consentimiento, la notificación de vulneraciones de seguridad, entre otras.
- **Mecanismos de tutela y supervisión:** Establece los procedimientos para que los ciudadanos puedan ejercer sus derechos y para que la autoridad de control (SPDP) pueda investigar, sancionar y asegurar el cumplimiento de la ley.

Enfatizando lo dispuesto en la LOPDP, no es necesario escribir otras disposiciones en otras normas sectoriales, como en el ámbito de las telecomunicaciones, que dupliquen la LOPDP. Los prestadores de servicios y cualquier entidad que trate datos personales deben ceñirse a lo ya dispuesto en la LOPDP, ya que esta es la ley integral y marco que regula la materia. La reforma, en su caso, debe buscar la armonización y el enfoque específico sin desvirtuar lo ya establecido por la LOPDP y la autonomía de los reguladores sectoriales dentro de ese marco.

Así:

- El uso, tratamiento y protección de los datos personales debe regirse estrictamente por lo establecido en la Ley Orgánica de Protección de Datos Personales de Ecuador, su Reglamento General y las directrices emitidas por la Autoridad de Protección de Datos.

- Toda la información personal que se recopile, procese o almacene debe manejarse con total transparencia, seguridad y respeto a los derechos de los titulares de los datos. Se debe garantizar que los datos serán utilizados únicamente para los fines contractuales para la prestación del servicio y adicionalmente para los que el usuario ha dado su consentimiento explícito, e informado, y siempre en cumplimiento con el marco legal vigente.

2. RECOPILACIÓN Y CONSERVACIÓN DE DATOS BIOMÉTRICOS

OBSERVACIÓN:

La propuesta no debería imponer a los prestadores de servicios de telecomunicaciones la obligación directa de recopilar o almacenar datos biométricos. La Norma Técnica para la Prestación de los Servicios de Información y Servicios Relacionados de las Entidades de

Certificación Acreditadas y Terceros Vinculados ya regula este proceso. Los prestadores pueden contratar a estas Entidades de Certificación Acreditadas (terceros especializados y regulados por ARCOTEL) para realizar verificaciones biométricas, sin necesidad de manejar directamente esta información sensible.

RESPUESTA:

Analizando el escenario planteado a la luz de la Ley Orgánica de Protección de Datos Personales (LOPDP), la responsabilidad del manejo y protección de los datos personales recae de la siguiente manera:

1. El Responsable del Tratamiento: El Prestador de Servicios de Telecomunicaciones

Según la LOPDP, la responsabilidad principal y última del manejo y la protección de los datos personales recae siempre en el "Responsable del Tratamiento".

En el caso expuesto, el prestador de servicios de telecomunicaciones es inequívocamente el Responsable del Tratamiento. Porque es esta entidad quien:

- **Define la finalidad y los medios del tratamiento de los datos.** Es decir, es el prestador de servicios quien decide para qué se van a usar los datos (ej., para la contratación de un servicio, para la facturación, para la verificación de identidad) y cómo se van a tratar.

- **Obtiene el consentimiento del usuario**. Los usuarios dan su consentimiento al prestador de servicios para la entrega y tratamiento de su información.

- **Tiene la relación directa con el titular de los datos.** El usuario es su cliente y, por lo tanto, es el prestador de servicios quien debe garantizar el ejercicio de los derechos del titular (acceso, rectificación, eliminación, etc.).

- La LOPDP establece que el Responsable del Tratamiento tiene la obligación ineludible de garantizar la seguridad, confidencialidad, integridad y disponibilidad de los datos personales que maneja, implementando las medidas técnicas y organizativas adecuadas.

2. El Encargado del Tratamiento: La Empresa de Tecnología (tercero)

Cuando el prestador de servicios de telecomunicaciones contrata a un tercero (una empresa de tecnología que dispone de soluciones como “Identificación biométrica” o "Selfie to ID" + prueba de vida, para que, en su nombre, realice la recopilación, manejo y procesamiento de los datos personales, esta empresa de tecnología se convierte en el "Encargado del Tratamiento".

El Encargado del Tratamiento:

- **Procesa los datos por cuenta y en nombre del Responsable.** No decide sobre la finalidad ni los medios del tratamiento; simplemente ejecuta las instrucciones que le da el Responsable.

- **Debe cumplir las instrucciones** del Responsable y aplicar las medidas de seguridad que este le indique o las que la ley exija.
- Su relación con el Responsable **debe estar regulada por un contrato por escrito**, que especifique claramente las condiciones del tratamiento, las obligaciones de seguridad y la finalidad del procesamiento.

Así:

- La responsabilidad fundamental del manejo y la protección de los datos personales siempre es del Prestador de Servicios de Telecomunicaciones (Responsable del Tratamiento).
- No importa que el procesamiento técnico lo realice un tercero (Encargado del Tratamiento). La contratación de un tercero no exime al Responsable de su obligación final de velar por la protección de esos datos. Si el Encargado incumple, el Responsable puede ser también corresponsable o, en última instancia, deberá responder ante la Autoridad de Protección de Datos Personales y los titulares.

- El Responsable del Tratamiento (el prestador de servicios de telecomunicaciones) debe demostrar que ha implementado las medidas adecuadas para proteger los datos, incluyendo la diligencia debida en la selección y supervisión de sus Encargados del Tratamiento, como la empresa que ofrece la tecnología de verificación de identidad, pero no transfiere la responsabilidad última al tercero.

- Si bien el tercero puede ser el que físicamente almacena y gestiona la información, la obligación legal y la responsabilidad final de la conservación adecuada de los datos personales, es del prestador de servicios de telecomunicaciones como Responsable del Tratamiento.

3. VERIFICACIÓN DE IDENTIDAD EN CONTRATACIÓN DE SERVICIOS DE TELECOMUNICACIONES

OBSERVACIÓN:

La verificación de identidad debe realizarse obligatoriamente antes de la firma del contrato para prevenir la suplantación. Sin embargo, en relación con los mecanismos de validación de identidad que usan biometría, la Superintendencia de Protección de Datos Personales (SPDP) insiste en lo siguiente:

- El consentimiento para el uso de biometría debe ser realmente libre.
- La biometría no puede ser la única opción de verificación de identidad. Imponerla como vía exclusiva se considera una forma de consentimiento forzado o condicionado, lo que viciaría el consentimiento y haría ilegítimo el tratamiento de datos.
- Los prestadores están obligados a ofrecer múltiples mecanismos de validación de identidad, permitiendo al titular elegir libremente la opción que mejor se adapte a sus intereses.

Solo al ofrecer alternativas a la biometría se garantiza la legitimidad del consentimiento y se respeta plenamente el principio de autodeterminación informativa y el elemento de libertad del consentimiento dispuesto en la LOPDP.

RESPUESTA:

Conforme lo observado, de plantea los siguientes mecanismos adicionales a la validación biométrica de la identidad de los abonados, clientes, usuarios, o suscriptores:

- **Uso de "Selfie to ID" + Prueba de Vida**

Su objetivo es confirmar la identidad de una persona de forma remota, asegurando que es quien dice ser y que está presente en el momento de la verificación. El sistema se integra por los siguientes elementos fundamentales:

1. **"Selfie to ID" (Selfie a Identificación):**
   - Se refiere a la **comparación automatizada de la imagen facial en vivo** capturada del usuario (una "selfie" o un video corto) **con la fotografía que figura en su documento de identidad oficial** (como una cédula o pasaporte).
   - Utiliza tecnología de **reconocimiento facial biométrico** para determinar el grado de coincidencia entre ambas imágenes.
   - La finalidad es verificar que la persona que está realizando el proceso es, de hecho, la misma persona que aparece en el documento de identidad presentado.
2. **Prueba de Vida (Liveness Detection):**
   - Este es un elemento **crítico y diferenciador** que aborda la vulnerabilidad de las soluciones de reconocimiento facial.
   - Su función es **verificar que la persona frente a la cámara es un ser humano real, vivo y presente en el momento de la captura**, y no un intento de fraude.
   - Detecta y previene "ataques de presentación" (Presentation Attacks, PA), como el uso de fotos impresas, videos pregrabados, máscaras, o incluso sofisticados "deepfakes" para suplantar la identidad.
   - Las técnicas de detección de vida pueden ser:
     - **Pasivas:** Analizan sutiles características biométricas (ej. micromovimientos, parpadeo involuntario, reflejos de luz en los ojos, textura de la piel) sin requerir acciones explícitas del usuario.
     - **Activas:** Solicitan al usuario realizar acciones específicas (ej. girar la cabeza, parpadear a demanda, decir una frase aleatoria) para confirmar su vitalidad.
3. **Comparación automatizada de imagen + documento + detección de vida:**
   - Este punto sintetiza la integración de los elementos anteriores en un flujo de trabajo continuo.
   - El software gestiona la captura de la "selfie", la captura o escaneo del documento de identidad, realiza la comparación biométrica facial entre ambos, y simultáneamente ejecuta la prueba de vida.
   - Todo el proceso es **automatizado**, lo que permite una verificación rápida, eficiente y escalable sin intervención manual constante.
4. **Requiere software conforme a ISO/IEC 30107-3:2023:**
   - Esta es la **validación clave de seguridad** para el componente de prueba de vida.

- La norma **ISO/IEC 30107-3:2023** es la versión más reciente (publicada en 2023) del estándar internacional que especifica los **métodos y criterios de evaluación de los mecanismos de detección de ataques de presentación (PAD)** para tecnologías biométricas.
- Que un software esté "conforme a ISO/IEC 30107-3:2023" significa que ha sido **probado por un laboratorio independiente y acreditado** y ha demostrado su capacidad para **detectar y resistir un amplio y actualizado conjunto de ataques de suplantación de identidad**. Los diferentes "niveles" de certificación (ej., Nivel 1 o Nivel 2) indican la robustez del sistema frente a ataques cada vez más sofisticados.

- **Autenticación Multifactor (MFA)**

Según la Unión Internacional de Telecomunicaciones (UIT), la **autenticación multifactor (MFA)** es un método de seguridad que requiere que un usuario proporcione **dos o más factores de verificación** para obtener acceso a un recurso, como una aplicación, cuenta en línea o sistema.

El objetivo principal de la MFA es **mejorar significativamente la seguridad** más allá de la simple combinación de nombre de usuario y contraseña. Incluso si uno de los factores se ve comprometido (por ejemplo, una contraseña robada), la autenticación falla porque el atacante no tiene los otros factores.

La UIT clasifica los factores de autenticación en tres categorías principales, a menudo recordadas como "algo que sabes, algo que tienes y algo que eres":

1. **Conocimiento (algo que sabes):** Este factor se basa en información que solo el usuario debe conocer.
   - Ejemplos: contraseñas, PIN, preguntas de seguridad.
2. **Posesión (algo que tienes):** Este factor se basa en un objeto físico o dispositivo que el usuario posee.
   - Ejemplos: teléfonos inteligentes (para recibir códigos por SMS o mediante aplicaciones de autenticación), tokens de hardware (USB, tarjetas), llaves de seguridad físicas.
3. **Inherencia (algo que eres):** Este factor se basa en características biométricas únicas del usuario.
   - Ejemplos: huellas dactilares, reconocimiento facial, escaneo de iris, reconocimiento de voz.

En el contexto de la verificación de identidad, la combinación de "Selfie to ID" y prueba de vida, respaldada por software conforme a la norma ISO/IEC 30107-3:2023 y Autenticación Multifactor (MFA), se presenta como un mecanismo de seguridad robusto adicional.

En ese sentido, y conforme a las observaciones presentadas por la Superintendencia de Protección de Datos Personales (SPDP), se ajusta el texto respecto a la verificación de identidad, con la finalidad de que los prestadores puedan ofrecer múltiples mecanismos de validación de identidad, permitiendo al titular elegir libremente la opción que mejor se adapte a sus intereses, en concordancia con el ordenamiento jurídico vigente.

4. APLICACIÓN GENERAL DE LA VERIFICACIÓN DE IDENTIDAD A TODOS LOS PRESTADORES

OBSERVACIÓN:

Se enfatiza que la "verificación inequívoca de la identidad" de los abonados, clientes, usuarios o suscriptores debe ser una obligación general y de cumplimiento mandatorio para absolutamente todos los prestadores de servicios de telecomunicaciones y radiodifusión por suscripción, sin excepciones por tamaño, cobertura o tipo de servicio.

Se considera jurídicamente inadmisible y discriminatorio que esta exigencia sea opcional para ciertos prestadores, ya que contradice directamente la sentencia Nº 1068-19-JP de la Corte Constitucional del Ecuador. Dicha sentencia es de cumplimiento obligatorio, general e inmediato, y no contempla excepciones ni tratos diferenciados. Por lo tanto, cualquier norma que relativice u omita esta obligación incumple directamente el mandato constitucional.

El argumento de eximir a ciertos prestadores carece de sustento técnico y jurídico, dado que los riesgos de suplantación de identidad no se limitan a un tipo específico de proveedor o servicio, afectando tanto a grandes como a pequeños operadores. La realidad demuestra la ocurrencia de vulneraciones en ambos casos, lo que subraya la necesidad de un tratamiento normativo homogéneo y riguroso.

En conclusión, la normativa en discusión debe disponer de forma clara, expresa y sin excepción, que todos los prestadores, sin importar su escala, implementen mecanismos de validación inequívoca de identidad como condición previa a la contratación de cualquier servicio, para así asegurar el cumplimiento de la sentencia constitucional.

RESPUESTA:

La implementación de la verificación inequívoca de identidad para **todos los abonados, clientes, usuarios o suscriptores**, sin distinción de tamaño o tipo de prestador, además de ser una buena práctica operativa, puede considerarse como un **imperativo legal y constitucional**, sustentado en los siguientes pilares normativos:

1. **Mandato Constitucional y Ejecución de la Sentencia de la Corte Constitucional:**
    - La **Constitución de la República del Ecuador (CRE)** garantiza el derecho a la identidad, a la intimidad y a la protección de datos personales (Art. 66 Nums. 19 y 20). La suplantación de identidad atenta directamente contra estos derechos fundamentales.
    - La **Sentencia Nº 1068-19-JP de la Corte Constitucional del Ecuador** es el fundamento jurídico primordial. Esta sentencia, de **cumplimiento obligatorio, general e inmediato**, establece la necesidad de mecanismos efectivos de verificación de identidad para prevenir el fraude y la suplantación.
2. **Armonización y Cumplimiento con la Ley Orgánica de Protección de Datos Personales (LOPDP):**
    - La LOPDP, al proteger el derecho a la autodeterminación informativa, exige que todo tratamiento de datos personales sea **lícito, leal y transparente**, y que se base en una finalidad específica y legítima. La

verificación inequívoca de identidad es un **pre-requisito fundamental para asegurar la licitud** del tratamiento.

- **Prevención de la suplantación de identidad:** Una identificación precisa asegura que el consentimiento para el tratamiento de datos y la manifestación de voluntad para contratar provienen del titular legítimo, evitando que datos de una persona sean asociados fraudulentamente a otra. Esto es clave para el **principio de licitud y la validez del consentimiento** (Art. 7, 8 LOPDP).
- **Seguridad de los datos:** La identificación robusta es la primera línea de defensa para garantizar la **seguridad, confidencialidad e integridad** de los datos personales (Art. 29 LOPDP). Al mitigar la suplantación, se reducen los riesgos de accesos no autorizados o tratamientos ilegítimos posteriores.
- **Responsabilidad Proactiva:** La LOPDP impone a los Responsables del Tratamiento (prestadores de servicios) la obligación de aplicar medidas técnicas y organizativas adecuadas para garantizar y poder demostrar que el tratamiento es conforme a la Ley (Art. 13 LOPDP). La verificación inequívoca de identidad es una de estas medidas esenciales.

3. **Protección del Usuario y Seguridad del Servicio bajo la Ley Orgánica de Telecomunicaciones (LOT) y su Reglamento General:**
   - La **LOT (Art. 28)** establece derechos de los usuarios, como el de recibir servicios de calidad y seguridad. La imposibilidad de verificar la identidad de un contratante debilita la seguridad del servicio y expone a los usuarios legítimos a consecuencias de fraudes (ej., facturas a su nombre, uso ilícito de servicios).
   - Los prestadores de servicios de telecomunicaciones tienen **obligaciones inherentes a la prestación de un servicio público** (aunque sea prestado por privados), incluyendo la garantía de la seguridad y la prevención de usos ilícitos de sus redes y servicios. Una verificación de identidad deficiente facilita actividades fraudulentas o delictivas que utilizan las redes de telecomunicaciones.
   - El **Reglamento General a la LOT** y las normativas técnicas de ARCOTEL deben detallar los procedimientos, pero la obligación de identificar no puede ser opcional. Permite asegurar la **integridad de los contratos de adhesión** y la correcta imputación de responsabilidades y cobros.
4. **Equidad y Prevención de Riesgos Homogéneos:**
   - Los riesgos de suplantación de identidad y uso indebido de datos personales **no discriminan por el tamaño o tipo de prestador**. Tanto los grandes operadores como los pequeños proveedores están expuestos a estas amenazas y, de hecho, se han registrado incidentes en todos los segmentos del mercado.
   - Eximir a ciertos prestadores crearía un **vacío legal y una asimetría competitiva** injustificada, incentivando posiblemente a actores maliciosos a dirigirse a los proveedores con menores controles.
   - La **homogeneidad en la aplicación de la verificación inequívoca** es esencial para establecer un estándar mínimo de seguridad y protección para todos los ciudadanos que contratan servicios de telecomunicaciones en el país.

Así:

La exigencia de que **todos los prestadores de servicios de telecomunicaciones implementen mecanismos de verificación inequívoca de identidad antes de la contratación** es una medida indispensable. No solo asegura el **cumplimiento directo e ineludible de la normativa vigente**, sino que también fortalece la **protección fundamental de los datos personales** bajo la LOPDP, salvaguarda los **derechos y la seguridad de los usuarios** conforme a la LOT, y garantiza un **marco equitativo y robusto** para todo el sector de las telecomunicaciones.

5. Adopción de la Firma Electrónica Simple para Contratos de Adhesión

OBSERVACIÓN:

La normativa legal ecuatoriana, incluyendo la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (LCEFEMYD) y su Reglamento, junto con el Código de Comercio, reconoce explícitamente la validez de la firma electrónica simple.

- La LCEFEMYD (Artículos 13 y 15) define la firma electrónica como datos electrónicos que identifican al titular y expresan su aprobación del mensaje, estableciendo requisitos para su validez sin restringir métodos.
- El Reglamento de la LCEFEMYD (Artículos 7 y 10), bajo el principio de neutralidad tecnológica, valida firmas electrónicas sin certificado, siempre que cumplan con los requisitos de la Ley para asegurar la autoría, control exclusivo del signatario y la inalterabilidad del mensaje.
- Criterios jurídicos de ARCOTEL (ARCOTEL-CJDA-2020-0010 y ARCOTEL-CDJ-DA-2017-134) han confirmado la existencia de dos tipos de firmas electrónicas en Ecuador: la "firma electrónica reconocida" (con certificado) y la "firma electrónica simple" (sin certificado), ambas válidas si cumplen los requisitos legales.
- El Código de Comercio (Artículos 76, 77 y 80) valida la contratación mercantil por medios electrónicos y reconoce la expresión de voluntad a través de sistemas informáticos, incluyendo los "contratos inteligentes" que facilitan la firma y el cumplimiento automático.

Dado este marco jurídico, se solicita a ARCOTEL que el proyecto de reforma incluya expresamente la firma electrónica simple como un mecanismo válido para la aceptación de los contratos de adhesión, reconociendo su legalidad y utilidad.

RESPUESTA:

En respuesta a su observación sobre la validez de la firma electrónica simple en la normativa ecuatoriana, a continuación, se presenta una aclaración basada en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (LCEFEMYD), sus regulaciones y criterios relacionados:

1. Definición de Firma Electrónica (LCEFEMYD)

La **Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (LCEFEMYD)**, en su artículo 13, define la firma electrónica de manera amplia como:

"Los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar a su titular e indicar que el titular aprueba la información recogida en el mensaje de datos."

Esta definición es tecnológicamente neutral, permitiendo diversas formas de manifestación de la voluntad siempre que cumplan con los requisitos de validez.

2. Tipos de Firmas Electrónicas en Ecuador

La normativa ecuatoriana, a través de la LCEFEMYD y los criterios jurídicos de entidades como ARCOTEL (mencionados en la observación: ARCOTEL-CJDA-2020-0010 y ARCOTEL-CDJ-DA-2017-134), reconoce principalmente dos tipos de firmas electrónicas:

- **Firma Electrónica Reconocida (o Avanzada/Certificada):** Es aquella que ha sido creada bajo el soporte de un certificado de firma electrónica emitido por una entidad de certificación de información acreditada en Ecuador y que ha sido verificada por dicha entidad. Goza de la presunción legal de ser auténtica.
- **Firma Electrónica Simple:** Es cualquier otro tipo de firma electrónica que cumple con los requisitos de validez establecidos en la LCEFEMYD, pero que no está respaldada por un certificado de una entidad acreditada. Su validez no se presume, sino que debe ser probada en caso de disputa, demostrando que cumple con el Artículo 15 de la LCEFEMYD.

3. Manifestación de la Firma Electrónica en un Documento Digital

Dado el principio de **neutralidad tecnológica** que rige la LCEFEMYD, una firma electrónica puede manifestarse de diversas maneras en un documento digital, siempre que cumpla con los requisitos legales para asegurar su validez. Algunas formas comunes incluyen:

- **Aceptación explícita mediante clic:** Un clic en un botón "Aceptar" o una casilla de verificación que indique la aprobación de términos y condiciones.
- **Ingreso de credenciales:** El uso de nombre de usuario y contraseña verificados.
- **Códigos de un solo uso (OTP):** Códigos enviados a un dispositivo previamente registrado y bajo el control exclusivo del usuario (ej., por SMS o email).
- **Representaciones gráficas:** Una imagen digitalizada de la firma manuscrita o una firma trazada directamente en un dispositivo electrónico.
- **Biometría:** El uso de huellas dactilares, reconocimiento facial u otras características biométricas para autenticar la identidad y expresar la voluntad (siempre y cuando se garantice la libertad del consentimiento y la posibilidad de ofrecer alternativas, como se discutió previamente en relación con la LOPDP).
- **Asociación lógica de datos:** Cualquier método electrónico que vincule de forma inequívoca al signatario con el mensaje y exprese su aprobación.

4. Requisitos del Artículo 15 de la LCEFEMYD

Para que una firma electrónica (sea simple o reconocida) sea válida y produzca los mismos efectos jurídicos que una firma manuscrita, el Artículo 15 de la LCEFEMYD establece los siguientes requisitos esenciales:

1. **Atribuible exclusivamente al signatario:** Debe ser posible vincular la firma de manera única a la persona que la utilizó.
2. **Creada por medios que el signatario mantiene bajo su exclusivo control:** El método utilizado para generar la firma debe estar bajo el control único de la persona que firma.
3. **Asegura la integridad del mensaje de datos desde el momento de su generación:** Debe garantizarse que el contenido del documento o mensaje no ha sido alterado después de ser firmado.
4. **Adecuada al propósito para el cual fue generada:** La firma debe ser idónea para la finalidad específica del acto jurídico que se está realizando.
5. **Utiliza un método confiable, seguro y apropiado:** El sistema o proceso de firma debe ser de fiabilidad demostrable, seguro y pertinente para el tipo de transacción.

La normativa vigente, incluyendo la LCEFEMYD y su Reglamento General, así como criterios jurídicos emitidos por la ARCOTEL y disposiciones del Código de Comercio, **reconoce explícitamente la plena validez de la firma electrónica simple**.

Es fundamental comprender que la LCEFEMYD, bajo el **principio de neutralidad tecnológica**, no restringe los métodos de firma electrónica, sino que establece los requisitos para su validez (Artículo 15). Esto significa que cualquier mecanismo electrónico que permita identificar al titular, asegurar que la creación de la firma estuvo bajo su control exclusivo, garantizar la integridad del mensaje y ser adecuado y confiable para su propósito, constituye una firma electrónica válida, independientemente de si cuenta o no con un certificado emitido por una entidad acreditada.

El Reglamento a la LCEFEMYD (Artículos 7 y 10) reitera esta postura al validar firmas electrónicas sin certificado, siempre y cuando cumplan con los requisitos de autoría, control exclusivo del signatario y la inalterabilidad del mensaje, que son precisamente los establecidos en la Ley.

Finalmente, el **Código de Comercio (Artículos 76, 77 y 80)** complementa este marco al validar la contratación mercantil por medios electrónicos y reconocer la expresión de voluntad a través de sistemas informáticos, incluso mediante "contratos inteligentes" que facilitan la formalización y ejecución automatizada.

El Reglamento eIDAS de la Unión Europea (que aunque no es ley ecuatoriana, sirve de referencia para entender la clasificación internacional de firmas electrónicas) dentro de su clasificación se encuentra la Firma electrónica simple: Es la menos robusta, pero sigue siendo una manifestación de voluntad en formato electrónico (por ejemplo, escribir el nombre al final de un correo electrónico). Su validez dependerá de la valoración de cada caso y la prueba adicional que se pueda aportar.

Así:

La postura de que la firma electrónica simple es válida en Ecuador, siempre que cumpla con los requisitos del artículo 15 de la LCEFEMYD, es **legalmente sólida y fundamental para el desarrollo del comercio electrónico y la contratación digital** en el país.

6. SUSPENSIÓN DE COBROS POR RECLAMOS DE SUPLANTACIÓN DE IDENTIDAD

La propuesta normativa plantea la suspensión del cobro de valores y el registro en burós de crédito ante reclamos de suplantación de identidad, hasta que el prestador resuelva o exista un pronunciamiento de autoridad competente. CNT EP, como empresa pública sujeta al control de la Contraloría General del Estado (Art. 3 LOCGE sobre recursos públicos), argumenta que esta disposición es problemática:

- Los **ingresos por facturación son recursos públicos**, y CNT EP tiene la obligación de proteger el patrimonio estatal.
- Suspender el cobro sin un pronunciamiento de autoridad competente podría **fomentar el uso abusivo del derecho de reclamo** por parte de ciudadanos malintencionados.
- Se propone que la **suspensión del cobro proceda únicamente cuando exista un pronunciamiento de la autoridad competente** (Fiscalía). Esto garantizaría el derecho del prestador a recibir el pago oportuno por sus servicios y protegería el patrimonio público, sin menoscabar la responsabilidad del prestador de implementar mecanismos de verificación para reducir la suplantación.

RESPUESTA:

Es decisivo equilibrar la protección del patrimonio público con la **salvaguarda de los derechos fundamentales de los usuarios**, especialmente frente a un delito como la suplantación de identidad. La Ley Orgánica de Telecomunicaciones (LOT) y su Reglamento General establecen el marco para la protección de los derechos de los abonados y la provisión de servicios seguros y confiables. La suplantación de identidad impacta directamente la seguridad jurídica del usuario y la legitimidad de la relación contractual.

Para abordar ambas preocupaciones de manera justa y conforme a la normativa vigente, la reforma a la norma considerará el siguiente texto, que recoge la esencia de la propuesta:

El cobro de valores y el registro en el buró de crédito, con la presentación de la denuncia realizada ante la Autoridad Jurisdiccional Competente por parte del abonado, cliente o suscriptor perjudicado del presunto cometimiento del delito de suplantación de identidad, quedarán suspendidos.

Esta disposición garantiza que:

- **Se protege al usuario:** Al presentar una denuncia formal ante la autoridad competente (como la Fiscalía), el abonado, cliente o suscriptor perjudicado obtiene una medida de protección inmediata que detiene los cobros indebidos y el impacto en su historial crediticio mientras se investiga el delito. Esto se alinea con el espíritu de **protección de los derechos del consumidor** consagrado en la LOT y el respeto a la presunción de inocencia del afectado.
- **Se salvaguarda el patrimonio del prestador y la credibilidad del sistema:** La suspensión no es automática ni indiscriminada. Requiere la **presentación de una**

denuncia formal ante la autoridad jurisdiccional competente. Esta exigencia legal filtra los reclamos malintencionados o abusivos, proporcionando un respaldo jurídico que legitima la suspensión y permite al prestador tener una base sólida para la gestión de sus recursos y cobros, en línea con sus obligaciones de protección patrimonial.

- **Se fomenta la diligencia:** Esta medida incentivará a los prestadores de servicios a **fortalecer sus mecanismos de verificación de identidad** durante la contratación inicial de servicios, reduciendo proactivamente los casos de suplantación desde su origen. La LOPDP, en su enfoque de responsabilidad proactiva, ya exige esta diligencia.

Así:

La inclusión de este texto en la reforma crea un mecanismo equilibrado que, si bien protege al usuario de los efectos inmediatos de una suplantación de identidad, lo hace a través de un procedimiento formal que otorga seguridad jurídica al prestador, protegiendo sus legítimos intereses de cobro y fomentando la prevención del fraude en todo el ecosistema de telecomunicaciones.

7. DERECHO DE DEVOLUCIÓN DE LOS USUARIOS: REEQUILIBRIO DE COSTOS

OBSERVACIÓN:

La propuesta de eliminar completamente el cobro por instalación al ejercer el derecho de devolución es inadecuada. Si bien se reconoce el derecho del usuario a la devolución y que no se debe cobrar instalación si hay problemas técnicos o incumplimientos contractuales atribuibles al prestador (verificados por ARCOTEL), eliminar el cobro de manera generalizada vulneraría el derecho del prestador a recuperar costos legítimos de instalación. Esto podría, además, incentivar el uso abusivo del derecho de devolución en casos donde no existan causas imputables al servicio o al prestador.

RESPUESTA:

Se aclara que la normativa actual busca un equilibrio justo. El **derecho a retracto** permite al usuario desistir del servicio, pero los **costos de instalación** solo serán asumidos por el prestador si la devolución se debe a fallas o problemas técnicos imputables al servicio. Esto significa que:

- **Si el usuario devuelve el servicio por causas ajenas a problemas técnicos o incumplimientos del prestador**, es razonable que el usuario asuma los costos de instalación, ya que el prestador incurrió en un gasto legítimo para proveer el servicio.
- **Si la devolución se debe a fallas o problemas técnicos verificados**, el prestador no podrá cobrar los costos de instalación. Esta medida protege al usuario de servicios deficientes y asegura que el prestador cumpla con los estándares de calidad.

Es importante destacar que la **verificación y calificación de las fallas no recae directamente en ARCOTEL**, sino en el prestador del servicio. Esto agiliza el proceso de atención al usuario. Sin embargo, para garantizar la transparencia y evitar prácticas abusivas, **ARCOTEL ejerce un control aleatorio** sobre los análisis realizados por los prestadores. Este control permite a la entidad reguladora verificar si la falla o problema técnico que motivó la devolución del servicio por parte del usuario fue correctamente evaluado por el prestador.

Esta aproximación busca salvaguardar los derechos de ambas partes:

- **Para el usuario:** Se garantiza la posibilidad de devolver un servicio no satisfactorio sin incurrir en costos de instalación, promoviendo así la calidad y el cumplimiento contractual por parte de los prestadores.
- **Para el prestador:** Se protege su derecho a recuperar los costos legítimos de instalación en aquellos casos donde la devolución no se deba a una falencia propia del servicio, desincentivando así el uso indebido del derecho de retracto.

Así:

La propuesta normativa procura lograr un balance adecuado, fomentando la responsabilidad del prestador y protegiendo al usuario sin desincentivar la inversión y prestación de servicios de telecomunicaciones.

8. AMPLIACIÓN DEL PLAZO PARA IMPLEMENTAR MEJORAS EN LA ATENCIÓN DE RECLAMOS POR SUPLANTACIÓN DE IDENTIDAD

OBSERVACIÓN:

La Disposición Transitoria Séptima del proyecto establece un "cumplimiento inmediato" para la atención de reclamos por presunta suplantación de identidad. Sin embargo, implementar las mejoras necesarias en los mecanismos y procedimientos internos para gestionar estos reclamos es un proceso complejo y requiere tiempo.

Se propone a ARCOTEL que se otorgue un plazo determinado de seis (6) a nueve (9) meses para la implementación de estas mejoras. Esta extensión es crucial, ya que la experiencia previa indica que adaptar los sistemas internos y capacitar al personal para abordar eficazmente la suplantación de identidad demanda al menos seis meses.

Asimismo, se pide considerar la posibilidad de solicitar ampliaciones de plazo para la implementación de otras obligaciones, siempre con las justificaciones respectivas.

RESPUESTA:

Análisis y Propuesta para la Atención de Reclamos por Suplantación de Identidad

Respecto a la **Disposición Transitoria Séptima** y la implementación inmediata de mecanismos para la atención de reclamos por presunta suplantación de identidad. Reconocemos que este proceso puede ser complejo y requerir tiempo para adaptar sistemas internos y capacitar al personal de manera efectiva. Sin embargo, en línea con los derechos de los usuarios establecidos en la LOT y su Reglamento General, la premura de garantizar una protección efectiva ante este tipo de fraude es fundamental.

Si bien la sugerencia para la adaptación de sistemas y la capacitación del personal pueden demandar al menos seis meses, consideramos que un plazo de seis a nueve meses para la implementación de las mejoras se considera un plazo muy amplio dado las circunstancias. La suplantación de identidad es un delito grave que puede generar un perjuicio económico y moral significativo para los usuarios. Retrasar la implementación de mecanismos de atención eficientes pone en riesgo sus derechos y su patrimonio.

Proponemos que el plazo para la implementación de los mecanismos de atención ante reclamos por supuesta suplantación de identidad sea de **tres meses**. Este plazo, aunque ambicioso, es necesario para priorizar la protección de los usuarios. Para lograrlo, se considera una estrategia de implementación que incluya:

- **Identificación y priorización de mejoras críticas:** Enfocarse inicialmente en los cambios más urgentes y de mayor impacto para la atención de estos reclamos.
- **Capacitación intensiva:** Implementar programas de capacitación acelerados y enfocados en el personal que directamente atenderá estos casos.
- **Mecanismos de atención provisionales:** Durante el periodo de transición, se podrían establecer protocolos de atención prioritaria y provisional que, si bien no son la solución definitiva, permitan dar una respuesta más rápida a los usuarios, clientes y abonados afectados. Esto podría incluir la asignación de personal específico para estos casos y la habilitación de canales de comunicación directos.
- **Monitoreo y ajuste continuo:** Establecer un sistema de monitoreo constante durante estos tres meses para identificar cuellos de botella y realizar ajustes rápidos en los procesos.

Se considera que un plazo de **tres meses**, combinado con una estrategia de implementación enfocada y con mecanismos provisionales, permitiría a los prestadores del servicio cumplir con la **Disposición Transitoria Séptima** de manera más ágil, sin comprometer la efectividad a largo plazo de los mecanismos de atención. La protección de los derechos de los usuarios debe ser la prioridad, y un plazo más corto reflejaría la urgencia de esta situación.

Análisis y Respuesta a la Observación sobre Ampliación de Plazos para Otras Obligaciones

Se entiende que implementar nuevas regulaciones es un proceso complejo y que los proveedores de servicios podrían necesitar flexibilidad en diversas áreas. Sin embargo, es necesario encontrar un equilibrio. Debemos asegurar que los usuarios reciban servicios de manera oportuna y efectiva, garantizando así sus derechos de forma prioritaria.

Basándonos en los derechos de los usuarios establecidos en la LOT y su Reglamento General, y la necesidad imperante de implementar mecanismos que protejan al usuario, la postura de ARCOTEL es la siguiente:

1. **Prioridad en la Protección del Usuario:** La implementación de mecanismos de verificación de identidad y de aceptación de la contratación del servicio es vital para salvaguardar a los usuarios de fraudes, suplantaciones y contrataciones no deseadas. Estos derechos son irrenunciables y su plena aplicación debe ser una prioridad.
2. **Excepcionalidad de las Ampliaciones:** Si bien reconocemos la complejidad operativa, las ampliaciones de plazos para la implementación de obligaciones deben ser consideradas como **excepcionales y no la regla general**. La norma busca establecer un marco temporal claro para que los prestadores de servicios adapten sus operaciones.
3. **Análisis de Pertinencia Estricto y Justificación Fundamentada:** La Dirección Ejecutiva de ARCOTEL podría otorgar o ampliar plazos de manera excepcional. No obstante, enfatizamos que este proceso debe basarse en un **análisis de pertinencia estricto y una justificación fundamentada e irrefutable por parte del prestador**.
    - **Justificación Detallada:** La solicitud deberá detallar exhaustivamente las razones técnicas, operativas y/o financieras que impiden el cumplimiento en el plazo establecido, incluyendo un cronograma de hitos y un plan de acción concreto para subsanar los impedimentos.
    - **Evidencia Comprobatoria:** Se requerirá la presentación de evidencia documental que respalde la justificación (ej. contratos con proveedores de tecnología, informes de consultoría, análisis de impacto, etc.).
    - **Impacto en el Usuario:** La solicitud deberá incluir un análisis del impacto de la no implementación oportuna en los derechos de los usuarios y, en su caso, las medidas provisionales que el prestador implementará para mitigar dicho impacto durante el período de extensión.
4. **Criterios Específicos para Evaluación:** La Dirección Ejecutiva de ARCOTEL establecerá criterios claros y específicos para la evaluación de estas solicitudes, asegurando la objetividad y transparencia en el proceso. Se priorizarán los casos donde la complejidad técnica sea demostrablemente superior y donde la postergación no comprometa gravemente los derechos y la seguridad de los usuarios.

Así:

La Dirección Ejecutiva de ARCOTEL podrá extender plazos de forma excepcional para la implementación de los mecanismos y procedimientos que aseguren el cumplimiento de esta normativa. Para ello, los proveedores de servicios deberán justificar su solicitud detalladamente, presentando un análisis de las razones (técnicas, operativas, financieras), la evidencia que las respalde y una evaluación del impacto en el usuario, incluyendo las medidas provisionales que adoptarán.

9. **Delimitación de Atribuciones: Rol de los Prestadores vs. Funciones Investigativas**

OBSERVACIÓN:

La reforma, si bien busca instrumentar la Sentencia de la Corte Constitucional, asigna a los prestadores de servicios de telecomunicaciones funciones investigativas e indagatorias sobre delitos como la suplantación de identidad (Art. 212 COIP). CNT EP considera que esto excede sus competencias legales y constitucionales (Art. 226 de la Constitución, COIP Art. 444 sobre atribuciones fiscales).

- La Ley Orgánica de Telecomunicaciones (LOT, Art. 22) circunscribe la atención de reclamos a la prestación de servicios, no a la determinación de delitos.
- La investigación de delitos es atribución exclusiva de la Fiscalía General del Estado con el apoyo de la Policía Judicial.
- Se solicita que la norma clarifique y delimite que los "sistemas de investigación" que implementen las operadoras se restrinjan a mecanismos de verificación de identidad, sin asumir roles judiciales o policiales.
- La norma debe reforzar el derecho de los usuarios a acudir a las instancias públicas competentes para denunciar delitos.

RESPUESTA:

La propuesta de reforma normativa busca responder a la Sentencia de la Corte Constitucional y proteger a los usuarios de delitos como la suplantación de identidad, no pretende imponer a los prestadores de servicios funciones que por **naturaleza legal y constitucional** corresponden a las autoridades de investigación y judiciales.

Se reconoce que la Ley Orgánica de Telecomunicaciones (LOT, Art. 22) circunscribe la atención de reclamos a la **prestación de servicios**, y que la investigación de delitos es una atribución exclusiva de la **Fiscalía General del Estado** con el apoyo de la Policía Judicial (Art. 226 de la Constitución, COIP Art. 444).

Por lo tanto, la interpretación y aplicación de la norma deben ser precisas para **evitar cualquier ambigüedad**. Cuando la norma se refiere a "sistemas de investigación" que implementen los prestadores, se entiende y debe quedar claramente delimitado que estos sistemas se restringen a **mecanismos internos de verificación de identidad, autenticación de usuarios y gestión de reclamos relacionados con la prestación del servicio**. El objetivo es que los prestadores puedan identificar y prevenir actividades fraudulentas o no consentidas que afectan la relación contractual con sus usuarios, como la suplantación de identidad en la contratación de servicios o la gestión de números.

Estos "sistemas de investigación" no implican, bajo ninguna circunstancia, que los prestadores asuman roles **judiciales o policiales** de indagación criminal, recolección de pruebas para procesos penales o determinación de responsabilidades delictivas. Su función es la de **identificar indicios de actividades anómalas** que puedan constituir un delito, recopilar la información pertinente que esté a su alcance en el marco de la prestación del servicio, que le permita al abonado, cliente, suscriptor o usuario, **poner esta información a disposición de las autoridades competentes** (Fiscalía General del Estado y Policía Judicial) para que ellas realicen la investigación formal.

Así:

La reforma busca que los prestadores de servicios refuercen sus mecanismos internos para proteger a los usuarios y prevenir fraudes relacionados con la identidad en el ámbito de las telecomunicaciones.

5.2. OBSERVACIONES ESPECÍFICAS

El análisis de las observaciones al articulado consta en el Anexo 1 de este informe.

6. CONCLUSIONES Y RECOMENDACIÓN

a) La propuesta de reforma a la "REFORMA A LA NORMA TÉCNICA QUE REGULA LAS CONDICIONES GENERALES DE LOS CONTRATOS DE ADHESIÓN, DEL CONTRATO NEGOCIADO CON CLIENTES, Y DEL EMPADRONAMIENTO DE ABONADOS Y CLIENTES", conforme la disposición emitida por el Director Ejecutivo de ARCOTEL en sumilla inserta en el memorando Nro. ARCOTEL-CREG-2025-0298-M 05 de junio de 2025, ha sido sometida al procedimiento de consulta pública, cumpliendo con lo dispuesto en el Reglamento de Consultas Públicas aprobado con Resolución 03-03-ARCOTEL-2015 de 28 de mayo de 2015, y se realizó la audiencia pública presencial acorde con el Procedimiento para Realizar Audiencias Públicas emitido para el efecto.

b) Dentro del procedimiento de consultas públicas se recibieron sin el carácter de vinculantes para la ARCOTEL, observaciones, comentarios y sugerencias al proyecto, por correo electrónico, oficios por medio del sistema de gestión documental, y durante la audiencia pública presencial.

c) Las principales observaciones de carácter general y particular han sido analizadas por la ARCOTEL en el presente informe y en anexo 1 de Excel, habiéndose acogido luego del análisis respectivo las recomendaciones pertinentes y en función de ello, se presenta una propuesta final de resolución.

Por lo indicado, se recomienda al Coordinador Técnico de Regulación aprobar el presente informe y ponerlo en conocimiento de la Dirección Ejecutiva, juntamente con la propuesta del proyecto de resolución para la propuesta de reforma a la "REFORMA A LA NORMA TÉCNICA QUE REGULA LAS CONDICIONES GENERALES DE LOS CONTRATOS DE ADHESIÓN, DEL CONTRATO NEGOCIADO CON CLIENTES, Y DEL EMPADRONAMIENTO DE ABONADOS Y CLIENTES", a fin de considerarlo procedente y previo criterio jurídico de la Coordinación General Jurídica, lo ponga a consideración del Director Ejecutivo de la ARCOTEL, para su aprobación.

7. ANEXOS

- Proyecto de Resolución de la propuesta de REFORMA A LA NORMA TÉCNICA QUE REGULA LAS CONDICIONES GENERALES DE LOS CONTRATOS DE

ADHESIÓN, DEL CONTRATO NEGOCIADO CON CLIENTES, Y DEL EMPADRONAMIENTO DE ABONADOS Y CLIENTES.

- Cuadro con el análisis de las observaciones específicas presentadas.
- Acta de ejecución de Audiencia pública presencial.
- Listado de asistentes a audiencias pública presencial.

Atentamente,

Firmado electrónicamente por:
JUAN PABLO PUCHAICELA HUACA
Validar únicamente con FirmaEC

Mgs. Juan Pablo Puchaicela
DIRECTOR TÉCNICO DE REGULACIÓN DE SERVICIOS Y REDES DE TELECOMUNICACIONES

ELABORADO POR:
Firmado electrónicamente por: VICTOR HUGO SALAZAR ZAPATA Validar únicamente con FirmaEC Víctor Salazar Zapata **Especialista Jefe 1**
Firmado electrónicamente por: ALEX PATRICIO BECERRA CHINGAL Validar únicamente con FirmaEC Alex Becerra Chingal **Analista Jurídico de Regulación de Servicios y Redes de Telecomunicaciones 2**