INSTITUTO FEDERAL DE TELECOMUNICACIONES

Seguridad de las Comunicaciones de Voz a través de Redes Públicas de Telecomunicaciones

Instituto Federal de Telecomunicaciones

Unidad de Política Regulatoria
Dirección General de Regulación de Interconexión y
Reventa de Servicios de Telecomunicaciones

Diciembre 2023

Seguridad de las Comunicaciones de Voz a través de Redes Públicas de Telecomunicaciones

Aviso legal

Debido a que el Instituto Federal de Telecomunicaciones, (en adelante "el Instituto", o "el IFT") es la autoridad de competencia económica, así como el órgano autónomo regulador, con facultades exclusivas, en los sectores de telecomunicaciones y radiodifusión, conforme lo dispuesto en el artículo 28, párrafos décimo cuarto, décimo quinto y décimo sexto, de la Constitución Política de los Estados Unidos Mexicanos; 7 de la Ley Federal de Telecomunicaciones y Radiodifusión; además del 5, párrafo primero, de la Ley Federal de Competencia Económica. Y a que, en México, "*las llamadas no deseadas*" ponen en riesgo la seguridad de los usuarios de redes públicas, el presente documento aborda la problemática generada por estas y se comparan las medidas para su combate, con el objeto de dar a conocer las soluciones técnicas y mejores prácticas relacionadas con la seguridad en comunicaciones de voz.

Este documento acompaña una Consulta Pública de integración, a efecto de recabar información adicional y propuestas para la elaboración del "***Anteproyecto de lineamientos para garantizar la seguridad de las comunicaciones de voz a través de redes públicas de telecomunicaciones***.

El análisis, evita prejuzgar otros procedimientos llevados a cabo o que pudiera llevar el Instituto, en los que se analicen casos particulares, o se cuente con información específica, adicional o proveniente de fuentes distintas a las del presente; y/o sobre el ejercicio de las demás facultades que corresponden al Instituto.

Es importante resaltar que el contenido de este documento no refleja la postura institucional, ni es vinculante para el Pleno del Instituto, así como tampoco para los sectores regulados, sujetos obligados o el usuario.

Seguridad de las Comunicaciones de voz a través de Redes Públicas de Telecomunicaciones

Contenido

Introducción

Las llamadas no deseadas, como el spam a través de servicios de voz y las llamadas de suplantación de identidad (spoofing), son cada vez más comunes y ponen en riesgo la privacidad y seguridad de los usuarios de redes públicas de telecomunicaciones. En este documento se aborda la problemática de las llamadas no deseadas, se señalan las principales conductas asociadas a éstas y se valora su incidencia en México. También se realiza una comparación de las medidas regulatorias implementadas por algunos organismos a nivel internacional, además de analizar las alternativas técnicas para el combate de llamadas no deseadas, incluyendo soluciones basadas en estándar STIR/SHAKEN, *Blockchain*, filtrado, entre otros.

Ubicadas la problemática y alternativas de solución, se discutirán los puntos de vista iniciales y principios que deberán seguir los mecanismos de seguridad a implementarse en redes públicas de telecomunicaciones, que tienen por objeto reducir el número de llamadas no deseadas, mitigar el incremento de conductas fraudulentas asociadas al uso de servicios de telefonía, reducir su impacto, así como incrementar la confianza del usuario, en el uso de servicios de telecomunicaciones.

A. Llamadas no deseadas

Las **llamadas no deseadas** se han convertido en una molestia común para usuarios de telefonía fija y móvil, estas provienen de diferentes fuentes, tanto lícitas como ilegales, las realizan empresas que ofrecen productos o servicios con o sin el consentimiento de los usuarios; estafadores que buscan obtener información personal y financiera; encuestadores de temas diversos; o representan intentos de saturación de red; entre otros motivos.

El problema también genera inconvenientes para los proveedores de servicios, los cuales deben dar atención a las quejas, asumir costos asociados con la implementación de medidas de seguridad, además de atender el impacto que pueden tener las redes, al consumir recursos que disminuyen la capacidad del proveedor de servicios para proporcionar un servicio de calidad, en detrimento de la experiencia de los usuarios.

Diversas estimaciones de la industria sugieren que el costo anual del fraude en telecomunicaciones asciende a decenas de miles de millones de dólares. De acuerdo con la Encuesta Global de Fraude en Telecomunicaciones 2023 de la Asociación de Control de Fraude en Comunicaciones (en lo sucesivo, la "CFCA" por sus siglas en inglés) (CFCA, 2023), las pérdidas por fraude en telecomunicaciones en 2023 fueron de 38.95

mil millones de dólares en 2023, lo que representa un aumento del 12% respecto a las estimaciones de pérdidas por fraude reportadas en 2021, y un aproximado del 2.5% de los ingresos globales de telecomunicaciones.

La Unión Internacional de Telecomunicaciones (en lo sucesivo, la "UIT") ha señalado que un fraude en las telecomunicaciones es el uso de los recursos de numeración en la forma en que fueron concebidos, pero con la intención de generar ingresos por fraude (UIT, 2020). El fraude en las telecomunicaciones se facilita por el uso indebido de recursos de numeración, publicidad, servicio de mensajes cortos y las llamadas no autorizadas. Así, la UIT (2020) identifica, no limitativamente, las siguientes características de las llamadas fraudulentas:

- Llamadas abandonadas: llamadas que terminan antes de que sean contestadas por el usuario para que éste devuelva la llamada, ya que buscan confirmar que el número telefónico se encuentra activo. Este tipo de llamadas consumen recursos de red, por lo que la calidad de la comunicación de los usuarios puede verse afectada.

- Falsificación de llamadas: llamadas en las que el número del usuario que llama es parcial o totalmente falso, el cual puede intentar suplantar números telefónicos de bancos, autoridades de justicia, de departamentos gubernamentales y de familiares, entre otros. Algunos de los números falsificados no se ajustan al plan de numeración nacional o internacional, por lo que el código del país o el código de destino nacional pueden no coincidir.

- Alta frecuencia de marcado desde un mismo número: números telefónicos que realizan una gran cantidad de llamadas salientes.

- Marcación consecutiva: el número telefónico de la parte que llama realiza una marcación de cinco a diez números telefónicos consecutivos.

- Llamadas a intervalos muy cortos: el intervalo de llamada es siempre muy corto e incluso podría generarse una gran cantidad de llamadas simultáneas.

- Alta frecuencia de marcado al mismo número: algunos números telefónicos son llamados con mucha frecuencia debido a que se trata de llamadas fraudulentas.

Por otra parte, de acuerdo con el Informe de Fraude 2023 del ITW Global Leaders Forum, las mayores amenazas de fraude de voz en términos de volumen e impacto financiero

para los usuarios son la generación de llamadas hacia números de tarificación especial, las llamadas de suplantación de identidad, la intercepción y redireccionamiento de llamadas sin el consentimiento de las partes involucradas ("*Call Hijacking*") y las campañas de llamadas perdidas (ITW GLF, 2023).

I. Spam de Voz

El ***spam de voz*** corresponde a llamadas telefónicas pregrabadas, automáticamente marcadas y no solicitadas, que suelen tener por objetivo la comercialización de servicios o productos (UIT, 2015). La UIT distingue dos tipos principales de ***spam de voz****, a saber*:

- Llamada silenciosa: es una llamada telefónica con fines de ventas, generada por marcadores predictivos sin que un agente atienda la llamada. La llamada puede ser terminada por la parte que realizó la marcación, por lo que la parte llamada recibirá un silencio o un tono de la compañía telefónica que indica que la llamada se ha caído. Este tipo de llamadas buscan que la parte llamada efectúe una marcación al número de donde procedía la llamada abandonada.

- Llamada de acoso: es una llamada telefónica con fines de ventas y que también puede acosar, molestar o intimidar con contenido amenazante o ilegal. Este tipo de llamada no se abandona antes de su establecimiento.

Además, el ***spam de voz*** se puede enviar como "cebo" al utilizar una máquina automática de un solo tono, la cual establece una conexión con el receptor del ***spam de voz*** y termina la llamada tras uno o dos tonos de llamada o tras emitir una palabra corta. Si los receptores devuelven la llamada utilizando el identificador de llamada, entonces son conectados a un sistema de publicidad o a un servicio con costo.

Para mitigar este problema, el Proyecto Asociación de Tercera Generación (en lo sucesivo, "3GPP" por sus siglas en inglés) (2022) señala que las normativas pueden proporcionar algunos elementos para prevenir el ***spam de voz*** como:

- Listas nacionales de no llamar para telemercadeo y penalidades por su incumplimiento.
- Prohibir las llamadas publicitarias masivas sin el consentimiento del usuario.
- Prohibir el uso de la función de anonimato para llamadas publicitarias.

Sin embargo, el tiempo de reacción es lento y existen posibilidades de eludir la normativa nacional, si el tráfico se envía desde otros países. Asimismo, los operadores se enfrentan al problema del uso indebido de las tarifas planas para enviar tráfico.

La 3GPP (2022) indica que, para evitar el envío de tráfico no solicitado, el principal instrumento de prevención son las condiciones comerciales ya que restringen el uso de las tarifas planas[1] nacionales e internacionales en los siguientes términos:

- Para uso privado.
- Prohibir el uso comercial como los servicios de comunicación masiva, los centros de llamadas y la publicidad telefónica.
- Cobrar las comunicaciones que violen las condiciones del contrato a precio estándar.

Sin embargo, puede ser difícil probar el uso indebido de las tarifas planas, por lo que los contratos a menudo ofrecen la posibilidad de cancelarlos a corto plazo sin ofrecer explicaciones. También existen condiciones contractuales en las que se combinan tarifas planas con técnicas de medición de tráfico o tiempo.

En el caso de medición del tráfico, el ancho de banda se limita después de alcanzar determinado volumen de tráfico, mientras que, en el caso de medición del tiempo, las tarifas planas solamente son válidas si no se supera determinado umbral.

Además, las llamadas de voz sobre IP (en lo sucesivo, "VoIP" por sus siglas en inglés) son gratuitas si utilizan el Internet. Sin embargo, si las llamadas VoIP se conectan a redes legadas[2], entonces se debe pagar una tarifa correspondiente al uso de la red legada. Por lo anterior, los proveedores de servicio VoIP funcionan de manera similar a los operadores tradicionales cuando se conectan a redes legadas, y las tarifas por el uso de redes legadas disminuyen el uso indebido de la red.

Es así que, la 3GPP (2022) identifica una serie de problemas derivados de que la legislación referente a las comunicaciones no solicitadas difiere entre los países, entre los que destaca:

- Diferencias en la definición de comunicaciones no solicitadas.
- Diferencias en la definición de servicios de comunicación no solicitados.

[1] Cobro de servicios, generalmente de telecomunicaciones, durante un periodo determinado, por una cantidad fija y con independencia del tiempo y el tipo de su utilización.
[2] Redes basadas en conmutación de circuitos.

- Diferencias en el manejo de las comunicaciones no solicitadas.

En tal sentido, a nivel internacional, se carece de una definición aceptada de forma unánime respecto a lo que constituye una comunicación no solicitada; no obstante, las normativas suelen restringir las comunicaciones no solicitadas a la publicidad electrónica, lo que implica que pueden encontrarse desactualizadas en las definiciones más amplias, utilizadas por los organismos de estandarización.

Incluso las normas jurídicas difieren respecto a la definición de publicidad electrónica ya que, en algunos países como Estados Unidos de América, la publicidad electrónica debe tener además un trasfondo comercial mientras que en otros no. Así se observa que existe una zona gris respecto a los marcos jurídicos aplicables, ya que es confuso, por ejemplo, si está permitido enviar publicidad masiva religiosa desde los Estados Unidos de América, hacia la Unión Europea.

Por otra parte, la definición de los servicios de comunicación que son relevantes para las comunicaciones no solicitadas es otro punto donde difieren las normativas, ya que existen dos enfoques distintos: cubrir solamente los servicios de comunicación de bajo costo que son susceptibles de ser usados para enviar comunicaciones no solicitadas como el correo electrónico, o utilizar una definición más genérica e independiente de la tecnología que contemple tanto los servicios existentes como los futuros.

Asimismo, existen diferencias respecto a la forma de obtener el consentimiento de los usuarios para el envío de comunicaciones masivas, ya que existen dos formas principales de hacerlo:

> -*Opt-In*: el remitente de la comunicación masiva debe demostrar que el destinatario de la comunicación ha dado su consentimiento explícito.
>
> -*Opt-Out*: el remitente puede enviar comunicación masiva sin el consentimiento del destinatario, pero se debe proporcionar la posibilidad de que el destinatario sea eliminado de la lista de distribución para que éstos no vuelvan a llegar.

El volumen que implican las comunicaciones masivas es otro elemento que se tiende a tomar en cuenta al momento de definir las comunicaciones no solicitadas; sin embargo, no todas las comunicaciones masivas implican comunicaciones no solicitadas como puede ser el caso de los servicios de alerta.

II. Llamadas de Suplantación de Identidad

Las **llamadas de suplantación de identidad o *spoofed call*** son llamadas en las que el número telefónico de la parte que llama o la identidad de línea llamante (en lo sucesivo, "CLI" por sus siglas en inglés) es falsa (UIT, 2020).

Esta práctica se realiza para ocultar la identidad de la persona que llama o para imitar el número de una empresa u otra persona. Por ejemplo, la suplantación de identidad se utiliza para fingir que están llamando desde el banco, y así tratar de obtener información confidencial como la cuenta bancaria de los usuarios o los datos de inicio de sesión.

La 3GPP (2014) identifica los siguientes escenarios relativos a la suplantación de identidad:

- Llamada de Suplantación de Identidad usando VoIP: cuando se realiza una llamada en VoIP, la parte que llama incluirá su identificador de llamada o *Caller ID* como parte del paquete de datos que envía a la parte llamada. Un atacante puede realizar cambios en el paquete de datos y modificar el identificador de llamadas.

- Llamada de Suplantación de Identidad usando PRI/PBX: una Centralita Privada (en lo sucesivo, "PBX" por sus siglas en inglés) generalmente se conecta a la red local a través de una Interfaz de Tasa Primaria (en lo sucesivo, "PRI" por sus siglas en inglés). Los operadores de red generalmente no verifican los identificadores de llamada que pasan a través de éstas troncales, por lo que un atacante puede modificarlo.

- Falsificación de identidad desde un servidor de aplicaciones: los servidores de aplicaciones pueden ser implementados por proveedores de servicios de terceros. Estos pueden modificar las identidades y redirigir las llamadas.

- Falsificación de Identidad desde un IP-PBX hacia el Subsistema Multimedia IP (en lo sucesivo, "IMS" por sus siglas en inglés): los operadores móviles pueden carecer de los medios para detectar si un atacante dentro de la empresa que administra el IP-PBX está llevando a cabo prácticas sospechosas, como el realizar una gran cantidad de llamadas hacia muchos destinos diferentes.

- Falsificación del Identificador de Llamadas: un atacante puede modificar el identificador de llamadas que se muestra a la parte llamada para que parezca

el de una entidad legítima (banco, policía, etc.), o con un número diferente e inducir a la víctima a divulgar información confidencial.

- Falsificación de la ubicación de la persona que llama: el atacante puede modificar el identificador de llamadas que se muestra a la parte llamada para que parezca que se originó en otra ubicación.

- Suplantación de Identidad en la misma red: la parte que origina la llamada y la parte que la recibe pertenecen a la misma red. Este caso no es muy común, pero es el que ofrece las mejores posibilidades para detectar la suplantación de identidad. El escenario más común y el más difícil de determinar en donde se originó la llamada es en las interconexiones por tránsito.

Asimismo, la 3GPP (2014) ha identificado algunos requisitos de seguridad para detectar a las llamadas de suplantación de identidad:

- La red debe poder verificar que el identificador de llamadas proviene de la parte que originó la llamada o de una parte que está autorizada para usar ese identificador de llamadas.

- La red debe ser capaz de alertar a la parte llamada acerca de si la información del identificador de llamadas no está autorizada.

- La red debe ser capaz de registrar la información si el identificador de llamadas enviado a la parte llamada no está autenticado. La información registrada debe incluir el identificador de llamadas, el identificador de llamadas de la parte a la que se llamó, la hora de la llamada y cualquier parámetro que sea útil para realizar una auditoría.

- Si se detecta una llamada falsificada, entonces la red debe ser capaz de interrumpir la llamada y/o guardar la información de la llamada en una base de datos como la lista negra o *black list*.

B. Llamadas no deseadas en México

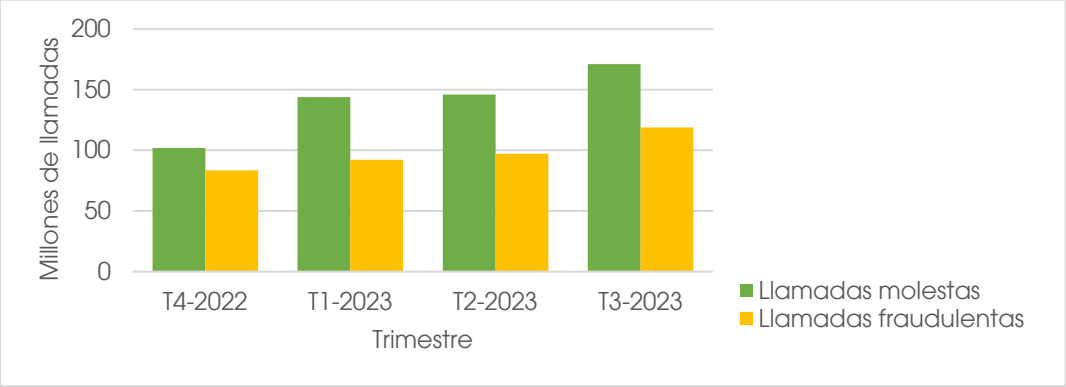
El Instituto Federal de Telecomunicaciones (2022), ha identificado que dentro de las prácticas ilícitas que más preocupan a los usuarios de telefonía móvil, se encuentran los correos electrónicos o las llamadas telefónicas fraudulentas a través de las cuales se solicitan datos personales, tales como información para el inicio de sesión en distintas

plataformas, información bancaria o de pago, entre otras, correspondiendo al 13.5% entre los delitos cibernéticos identificados por los usuarios.

Asimismo, de acuerdo con la información de la Procuraduría Federal del Consumidor (en lo sucesivo, la "PROFECO") (2023), desde la creación en el 2007 del Registro Público para Evitar Publicidad (en lo sucesivo, "REPEP") a la fecha, se han inscrito 3,781,105 números telefónicos; sin embargo, en el mismo periodo, también ha recibido 10,001 denuncias de consumidores que continuaron recibiendo comunicaciones no deseadas después de su inscripción en el registro.

Por otra parte, del análisis de datos recolectados a través de su red de usuarios, Hiya[3] estima que en México cada usuario recibe en promedio 17 llamadas de spam mensualmente. Además, durante el tercer trimestre de 2023, la aplicación de Hiya identificó 171 millones de llamadas no deseadas y 119 millones de llamadas con propósitos fraudulentos. De acuerdo con los datos de Hiya, esto sitúa a México como el cuarto país en América con la tasa más alta de llamadas de spam y el segundo con la tasa más alta de llamadas con propósitos fraudulentos (Hiya, 2023).

Tabla 1. Estimación de llamadas spam y fraudulentas



Fuente: Elaboración propia con información de Hiya.

Por otra parte, la Organización de Estados Americanos (en lo sucesivo, la "OEA") (2019) ha identificado las amenazas cibernéticas que enfrentan las entidades financieras en México, destacando la prevalencia del *phishing,*[4] como uno de los eventos de seguridad

[3] Hiya ofrece soluciones tecnológicas enfocadas en la identificación y gestión de llamadas telefónicas, particularmente en lo que respecta a la seguridad y la calidad del servicio en la telefonía. Hiya proporciona servicios como identificación de llamadas, protección contra el spam telefónico y análisis de llamadas.
[4] Estafa a través de una página web, correo electrónico, mensajes cortos o llamadas telefónicas en las que se suplanta a una persona o empresa de confianza para obtener datos privados de la persona usuaria, como claves de acceso o tarjetas de crédito.

digital más comúnmente identificados por las entidades del sistema financiero mexicano durante el 2018, con un 47% del total de entidades. Respecto a la ocurrencia del *phishing*, *vishing*[5] o *smishing*[6], la OEA (2019) refiere que un 18% de las entidades financieras identifican la ocurrencia de este tipo de eventos diariamente, 17% lo identifican semanalmente, 32% mensualmente y 34% trimestralmente.

Asimismo, en el Sistema Financiero Mexicano, en el 2018, el 100% de las instituciones financieras mayores han identificado eventos de *phising*, *vishing* o *smishing*. Además, 62% de las entidades medianas también sufrieron eventos de seguridad digital como el *phishing*, *vishing* o *smishing* durante el 2018. La OEA (2019), concluye que el *phishing* es uno de los eventos de seguridad digital que más usan los ciberdelincuentes contra los clientes de servicios financieros, así como contra las entidades e instituciones financieras en México.

Por su parte, el Instituto Nacional de Estadística y Geografía (en lo sucesivo, el "INEGI") (2022) señala que de los 4.9 millones delitos de extorsión cometidos durante el 2021, el 90.3% de los casos fueron realizados vía telefónica.

[5] Es un tipo de estafa de ingeniería social a través de una llamada telefónica mediante la cual se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima.
[6] Es una técnica que consiste en el envío de un mensaje corto por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada o realizarle un cargo económico.

PUNTOS CLAVE DE LAS LLAMADAS NO DESEADAS

- El fraude en las telecomunicaciones se facilita por el uso indebido de los recursos de numeración, la publicidad, el servicio de mensajes cortos y las llamadas no autorizadas.
- El spam de voz corresponde a llamadas telefónicas pregrabadas, automáticamente marcadas y no solicitadas que suelen tener por objetivo la comercialización de servicios o productos.
- Las llamadas de suplantación de identidad son llamadas en las que el número telefónico de la parte que llama o la identidad de la línea llamante son falsos.
- Las llamadas telefónicas fraudulentas solicitando datos personales se encuentra dentro de los delitos cibernéticos que más preocupa a los usuarios de los servicios de telecomunicaciones.

C. Experiencia Internacional

I. Panorama General y Políticas Implementadas en Estados Unidos de América

La Comisión Federal de Comunicaciones (en lo sucesivo, "FCC" por sus siglas en inglés) se encarga de vigilar el cumplimiento de la Ley de Protección al Consumidor Telefónico (en lo sucesivo, "TCPA" por sus siglas en inglés). La TCPA restringe la realización de llamadas comerciales, el uso de sistemas de marcación telefónica automática y los mensajes de voz pregrabados (FCC, 2018). Estas reglas son aplicables tanto a los operadores de telecomunicaciones como a otras empresas de telemercadeo.

La modificación realizada a la TCPA en el 2012 obliga a las empresas de telemercadeo a obtener el consentimiento expreso y por escrito de los consumidores antes de llamarlos, no permite a las empresas alegar la existencia de una relación comercial establecida para evitar obtener el consentimiento de los consumidores, y exige a las empresas que brinden una opción de *opt-out* al consumidor durante cada llamada (FCC, 2018).

Por otra parte, la Comisión Federal de Comercio (en lo sucesivo, "FTC" por sus siglas en inglés) se encarga de hacer cumplir las Reglas de Ventas por Telemercadeo (en lo sucesivo, "TSR" por sus siglas en inglés). Las TSR brindan un marco jurídico para combatir el fraude en el telemercadeo, aportan mecanismos de protección a la privacidad de los consumidores contra el telemercadeo y ayuda a los consumidores a diferenciar entre el telemercadeo legítimo y el fraudulento (FTC, 2023).

Las TSR prohíben a los vendedores abandonar las llamadas telefónicas salientes y establecen la obligación de transmitir el número telefónico y, cuando esté disponible, el nombre de la empresa de telemercadeo (FCC, 2003). Asimismo, la FCC y la FTC establecieron en el 2003 un Registro Nacional de No Llamar.

La FCC (2020) señala que los avances tecnológicos y el desarrollo del mercado de VoIP han permitido que la suplantación de identidad sea más fácil de realizar, ya que ésta puede ser llevada a cabo por personas con poca experiencia y a un costo mínimo. Los delincuentes aprovechan la capacidad de enmascarar la verdadera identidad de una llamada entrante para realizar fraudes.

Por lo anterior, la FCC (2020) mandató que todos los proveedores de servicio de voz implementen el estándar *STIR/SHAKEN* en las redes basadas en el Protocolo de Internet (en lo sucesivo, "IP" por sus siglas en inglés) para autenticar el identificador de llamadas.

Sin embargo, debido a que el estándar *STIR/SHAKEN* se basa en la transmisión de información en el encabezado de identidad del Protocolo de Inicio de Sesión (en lo sucesivo, "SIP" por sus siglas en inglés), éste solamente opera en las redes IP por lo que, si una llamada es terminada o enrutada a través de una red que no soporte el protocolo SIP, el encabezado de identidad se perderá.

El estándar *STIR/SHAKEN* requiere que el proveedor de servicios en donde se origina la llamada pueda certificar la identidad del usuario, este ofrece tres niveles de certificación:

- Certificado Completo o "A": el proveedor de servicio en donde se origina la llamada puede confirmar la identidad del usuario y que éste está utilizando su número telefónico.
- Certificado Parcial o "B": el proveedor de servicio en donde se origina la llamada puede confirmar la identidad del usuario, pero no la de su número telefónico.
- Certificado "C": el proveedor de servicio solamente puede confirmar que es el punto de entrada a la red IP para una llamada que se originó en otro lugar, como

puede ser el caso de llamadas originadas en el extranjero o en redes locales que no tienen implementado el estándar *STIR/SHAKEN*.

El estándar *STIR/SHAKEN* utiliza certificados digitales emitidos por una entidad neutral. El estándar requiere que cada proveedor de servicio posea su propio certificado, el cual sirve para asegurar:

- La identidad del proveedor de servicio.
- Que el proveedor de servicio está autorizado para autenticar la información de la persona que llama.

Cada vez que una llamada de voz es autenticada por un proveedor de servicio, éste transmite la ubicación de su certificado en el encabezado de identidad del protocolo SIP. Asimismo, el modelo de *STIR/SHAKEN* requiere la implementación de diversos roles:

- Una Autoridad de Gobierno, encargada de definir las políticas y procedimientos a través de los cuales las entidades pueden emitir o adquirir los certificados digitales.
- Un Administrador de Políticas, encargado de aplicar las reglas establecidas por la Autoridad de Gobierno y de asegurar que las autoridades de certificación están autorizadas para emitir los certificados digitales, además garantiza que los proveedores de servicio están autorizados para solicitar y recibir certificados digitales.
- Autoridades de Certificación, encargados de emitir los certificados digitales utilizados para autenticar y verificar las llamadas.
- Los proveedores de servicio, encargados de seleccionar una Autoridad de Certificación para solicitar un certificado digital cuando la llamada se origine en su red y, en el caso de que la llamada se termine en su red, deberán verificar con las Autoridades de Certificación que el certificado que reciben haya sido emitido por la autoridad de certificación correcta.

Una de las razones por las que la FCC (2020) mandató la implementación del estándar *STIR/SHAKEN* es que espera que éste, junto con las herramientas analíticas para llamadas, puedan proteger a los consumidores de los esquemas de fraudes a través de llamadas telefónicas que merman económicamente en un aproximado de $10 mil millones de dólares anualmente en los Estados Unidos de América. Además, la FCC indica que la implementación de este estándar permitirá a los proveedores de servicio reducir los costos al eliminar la congestión de red causada por este tipo de llamadas, así como disminuir el número de quejas de los usuarios por llamadas automáticas.

Para la implementación del estándar *STIR/SHAKEN*,, la FCC (2020) realizó los siguientes requerimientos a los proveedores de servicio para la implementación del estándar *STIR/SHAKEN*:

- Los proveedores de servicios deben autenticar y verificar la información del identificador de llamadas para aquellas llamadas que se originen y terminen exclusivamente en las porciones IP de su propia red.
- Los proveedores de servicios que originan una llamada y que será intercambiada con otro proveedor de servicio o con un intermediario, deberá usar el servicio de autenticación e insertar el encabezado de Identidad del método INVITE del protocolo SIP, y deberá transmitir la llamada autenticada al siguiente proveedor de servicio o intermediario en la ruta para terminar la llamada. Adicionalmente, un proveedor de servicio que termina una llamada autenticada que recibe de otro proveedor de servicio o intermediario, deberá usar el servicio de verificación para revisar la información almacenada en el encabezado de Identidad.

La FCC (2020) señaló que, para dar cumplimiento a la definición del modelo de autenticación *STIR/SHAKEN*, se deben seguir los tres estándares de la Alianza para Soluciones de la Industria de las Telecomunicaciones (en lo sucesivo, "ATIS" por sus siglas en inglés) que son la base del modelo *STIR/SHAKEN*: ATIS-1000074, ATIS-1000080 y ATIS-1000084, así como todos los documentos a los que se hace referencia en éstos. Además, la FCC permitió que los proveedores de servicio incorporen estándares adicionales siempre y cuando se mantenga el modelo de *STIR/SHAKEN* establecido por ATIS.

La FCC (2020) determinó inicialmente que las reglas para la implementación del modelo *STIR/SHAKEN* solamente eran aplicables para los proveedores de servicio que originan y terminan llamadas, excluyendo a los proveedores de servicio intermediarios. Sin embargo, la FCC (2020) decidió que para garantizar que la autenticación del identificador de llamadas se realice a través de toda la ruta por la que se establece una llamada, también mandató a los proveedores de servicio intermediarios a implementar el estándar *STIR/SHAKEN.*

La FCC también reconoció que, debido a que el modelo *STIR/SHAKEN* está basado en el protocolo SIP, se limitó la aplicación de las reglas a las porciones de la red de los proveedores de servicio que son capaces de iniciar, mantener y terminar llamadas mediante el protocolo SIP. Sin embargo, la FCC (2020) señaló que una cantidad significativa de llamadas estarán fuera del modelo de autenticación *STIR/SHAKEN*, ya

que una gran proporción de redes basadas en tecnología de Acceso Múltiple por División del Tiempo (en lo sucesivo, "TDM" por sus siglas en inglés) todavía están en uso.

Por lo anterior, la FCC (2020) señaló que los proveedores de servicio deberán tomar medidas razonables para implementar un modelo de autenticación del identificador de llamadas en las porciones de red que no están basadas en tecnología IP. Para cumplir esta obligación un proveedor de servicio deberá:

- Actualizar toda su red a tecnología IP e implementar el modelo *STIR/SHAKEN.*
- Trabajar en el desarrollo de una solución para la autenticación del identificador de llamadas para redes que no están basadas en tecnología IP.

La FCC (2020) aclaró que la adopción de las reglas para la implementación del modelo *STIR/SHAKEN* no son aplicables a los proveedores de servicio que carecen de control de la infraestructura de red necesaria para implementar este estándar. Sin embargo, la FCC (2020) determinó que las OTT[7] que brinden servicios de voz y tengan control de la infraestructura de red necesaria para implementar el estándar *STIR/SHAKEN*, están obligados a implementarlo.

La FCC (2020) indicó que entre los beneficios previstos de la implementación de modelo *STIR/SHAKEN* se incluyen la reducción de llamadas no solicitadas, mayor protección contra llamadas de suplantación de identidad, así como menores irrupciones de las comunicaciones de atención médica y de emergencia generadas por llamadas automáticas.

Los costos por la implementación del modelo *STIR/SHAKEN* variarán con base a la configuración actual de la red de cada proveedor de servicio (FCC, 2020). Entre los costos estimados por la FCC se encuentran las licencias de software para servicios de autenticación y verificación, actualizaciones del hardware de la red, así como cambios en la configuración de la red.

Los costos recurrentes anuales incluyen las tarifas asociadas al servicio de autenticación y verificación de las llamadas, así como las tarifas por los certificados digítales (FCC, 2020). La FCC estima que los costos recurrentes anuales oscilarán entre los $15,000 y los $300,000; y que los proveedores de servicios de voz de manera conjunta gastarían entre $39 millones y $780 millones de dólares anualmente en costos operativos, sin embargo,

[7] Servicios de video, audio, voz o datos que se transmiten sobre la plataforma de internet fijo o móvil y que generalmente no son provistos por los operadores tradicionales de telecomunicaciones.

reconoce que los proveedores de servicio de menor tamaño pueden tener diferentes costos y desafíos que los proveedores de servicio más grandes.

La FCC (2020) decidió no exigir a los proveedores de servicio que muestren los resultados de la verificación del modelo *STIR/SHAKEN* a sus usuarios o exigir alguna especificación en particular, ya que prefieren que los proveedores de servicio determinen las soluciones que funcionen mejor para sus usuarios.

Por otra parte, la FCC (2020) declinó modificar la estructura del modelo de *STIR/SHAKEN* para que éste resolviera las disputas que pudieran surgir entre proveedores de servicio o instruir a la Autoridad de Gobierno para que tome determinadas acciones en casos específicos.

Asimismo, la Oficina de Competencia de Telefonía Fija de la FCC emitió las Mejores Prácticas de Autenticación del Identificador de Llamadas, las cuales son de aplicación voluntaria. En ésta la FCC (2020) contempló los siguientes temas:

- Verificación de Suscriptores. Se recomienda que los proveedores de servicio verifiquen la identidad de los suscriptores minoristas y mayoristas cuando: (i) se apruebe una solicitud de servicio, (ii) se brinde el aprovisionamiento de conectividad de red, (iii) se celebre un contrato, o (iv) se permita el uso de recursos de numeración.
- Validación del número telefónico. Se determinan las mejores prácticas para que los proveedores de servicio confirmen el derecho del usuario final o del cliente a utilizar determinado número telefónico.
- Servicios de validación por parte de terceros. Se establecen las mejores prácticas para un proveedor de servicio que elige a un tercero para realizar el servicio de validación.
- *Originación* de llamadas Internacionales. Se establecen las mejores prácticas para los proveedores de servicio que utilizan recursos de numeración del Plan de Numeración de Norteamérica para brindar servicios a originadores de llamadas internacionales. El objetivo es desarrollar procesos para validar que la parte que llama está autorizada a usar determinado número telefónico o para validar la identidad de la persona que llama.

Además, la FCC (2022) impuso las siguientes obligaciones a los proveedores de servicio que reciben llamadas internacionales hacia los Estados Unidos:

- Aplicar la autenticación del identificador de llamadas a todas las llamadas no autenticadas originadas en el extranjero en protocolo SIP y que utilicen numeración del Plan de Numeración de Norteamérica.
- Responder a las solicitudes de rastreo en 24 horas y bloquear las llamadas que sirvan para conducir tráfico ilegal.

La FCC (2021) señala en el Segundo Informe sobre Bloqueo de Llamadas que las llamadas ilegales y no autorizadas constituyen la principal causa de quejas por parte de los consumidores. También indica que, tanto los operadores como otras empresas que ofrecen servicios de analíticos utilizan nueva información para actualizar continuamente sus procedimientos de análisis para detectar llamadas automáticas. Éstos informan pocos falsos positivos, es decir, llamadas incorrectamente identificadas como "*spam"* o fraudulentas y por lo tanto bloqueadas por error.

Las herramientas que los operadores y las empresas de analíticos ofrecen para el bloqueo de llamadas no solicitadas permiten bloquear llamadas de números específicos y de números que éstos consideran como ilegales (FCC, 2021). También ofrecen el servicio de etiquetado de llamadas a través del cual se puede catalogar a las llamadas no solicitadas o ilegales como "*spam*" o "probablemente *spam*". Asimismo, casi todos los operadores bloquean las llamadas provenientes de números telefónicos inscritos en la lista de no *originación*, de números telefónicos no válidos o no asignados.

En marzo del 2020 la FCC (2021) ordenó implementar el estándar *STIR/SHAKEN* en las redes IP de todos los operadores de telecomunicaciones que brinden servicios de voz para el 30 de junio del 2021. Sin embargo, se brindó una extensión en el plazo para la implementación del estándar *STIR/SHAKEN* a los operadores que enfrentaron grandes dificultades en la implementación de este estándar según los propios criterios de la FCC.

Hasta junio del 2021, un total de 207 operadores han implementado el estándar *STIR/SHAKEN*, 290 operadores han implementado parcialmente el estándar *STIR/SHAKEN* y 830 operadores no han implementado el estándar *STIR/SHAKEN* (FCC, 2021).

PUNTOS CLAVE DE LA EXPERIENCIA EN
ESTADOS UNIDOS DE AMÉRICA

- La FCC obliga a las empresas de telemercadeo a obtener el consentimiento expreso y por escrito de los consumidores antes de llamarlos, así como brindarles una opción de *opt-out* durante cada llamada.
- El desarrollo de VoIP ha permitido que la suplantación de identidad sea más fácil de realizar, ya que ésta puede ser llevada a cabo por personas con poca experiencia y a un costo mínimo.
- La FCC mandató que todos los proveedores de servicio de voz implementen el estándar *STIR/SHAKEN* en sus redes basadas en el protocolo IP para autenticar el identificador de llamadas.
- La FCC mandató que los proveedores de servicio deberán tomar medidas razonables para implementar un modelo de autenticación del identificador de llamadas en las porciones de red que no están basadas en tecnología IP.
- La FCC determinó que aquellas OTT que brinden servicios de voz y tengan control de la infraestructura de red necesaria para implementar el estándar STIR/SHAKEN, están obligadas a hacerlo.

II. Panorama General y Políticas Implementadas en Reino Unido

La responsabilidad de regular las llamadas no solicitadas se divide entre la Oficina de Comunicaciones (en lo sucesivo, "OFCOM" por sus siglas en inglés), quién es el encargado de regular las llamadas silenciosas y abandonadas debido a que no tienen contenido comercial, y la Oficina del Comisionado (en lo sucesivo, "ICO" por sus siglas en inglés) la cual es responsable de regular las llamadas comerciales y los mensajes de texto no deseados.

En este contexto, ICO publicó la Guía para las Comunicaciones Electrónicas en la cual se establecen los lineamientos que las organizaciones deberán seguir para el envío de mensajes comerciales por medios electrónicos como teléfono, fax, correo electrónico y mensajes de texto (ICO, 2018). Dentro de las obligaciones establecidas en esta Guía se encuentran (ICO Ofcom):

- Garantizar que se ha obtenido de forma clara el consentimiento del consumidor y que el mismo se encuentra vigente.
- Asegurarse de que el consentimiento del consumidor se ha obtenido si es que existen terceras partes involucradas.
- Verificar que el número del consumidor no se encuentre en la lista de no llamar.
- Cuando se llame a los consumidores se debe identificar claramente a la empresa, explicar la forma en que se obtuvo el consentimiento y la razón por la que se está llamando.
- Tener un sistema de quejas que responda a las inquietudes de los consumidores.

Asimismo, OFCOM emitió la "*Declaración sobre las llamadas abandonadas y silenciosas*" en la que establece las medidas que los usuarios de tecnologías de Sistemas Automáticos de Llamadas (en lo sucesivo, "ACS" por sus siglas en inglés) y Detección de Máquinas Contestadoras (en lo sucesivo, "AMD" por sus siglas en inglés) deberán seguir para evitar realizar este tipo de llamadas o, en su caso, limitar el daño que causan (Ofcom, 2010). Entre estas medidas se encuentran (ICO Ofcom):

- Asegurar una tasa de llamadas abandonadas menor al 3% de llamadas realizadas por campaña o por centro de llamadas durante un periodo de 24 horas.
- Garantizar que las personas no sean contactadas dentro de las siguientes 72 horas después de haber recibido una llamada abandonada si no se puede asegurar la presencia de un operador.
- En caso de una llamada abandonada, se debe reproducir un mensaje automático que le informe a la persona quién realizó la llamada y se le debe proporcionar un número telefónico para evitar futuras llamadas comerciales.
- La información del CLI debe ser válida y precisa para que la persona que recibe la llamada pueda identificar quién los llamó.
- Garantizar que, cuando un equipo de AMD identifique que la llamada ha sido atendida por un contestador automático, cualquier llamada a ese número telefónico dentro de las siguientes 24 horas deberá ser realizada por un operador.

Por otra parte, ICO y OFCOM han realizado la actualización de su Plan de Acción conjunto para regular las llamadas y mensajes molestos en el que señalan que el uso de VoIP facilita falsificar el número telefónico de la persona que llama (ICO Ofcom, 2021). Además, se pueden eludir las listas de bloqueo de llamadas molestas al cambiar constantemente el número telefónico de la persona que llama.

Asimismo, señalan que se requiere autenticación adicional para asegurar que las personas que llaman tienen autorización para utilizar el número telefónico desde el que marcan. Por otra parte, refieren que la autenticación del CLI en el Reino Unido mediante estándares como el *STIR/SHAKEN* puede tomar un largo tiempo ya que se requiere que los servicios de voz sean migrados a IP.

OFCOM (2022) ha requerido a los operadores que los datos proporcionados por el CLI en una llamada telefónica cumplan con los siguientes requisitos:

- Utilizar un número valido: es aquel que cumple con el plan internacional de numeración conforme a la recomendación E.164 de la UIT.
- Utilizar un número al que se pueda marcar: es aquel número que se encuentra en servicio y al que se puede devolver una llamada.
- Utilizar un número que identifique de forma inequívoca a la persona que llama: es un número que puede ser utilizado por una persona o por una organización, ya sea que se le haya asignado o tenga permiso para usarlo.

OFCOM también publicó los Lineamientos del CLI[8] para especificar los requisitos que el CLI deberá cumplir para asegurar que se cumplan los principios de validez, privacidad e integridad. En estos se establece que los operadores en cuya red se origine la llamada deben garantizar que la información del CLI sea precisa, y los operadores que ofrezcan el servicio de tránsito o en cuya red se termine la llamada deben verificar que el número pertenezca a un rango válido (Ofcom, 2022).

Los Lineamientos del CLI también establecen que todas las llamadas deben estar asociadas a un número telefónico que identifique el origen de ésta. Sin embargo, el CLI que se muestra a la parte llamada puede cambiarse a otro número telefónico válido siempre y cuando éste se pueda marcar e identifique de manera inequívoca a la parte que llama. Este escenario está pensado para servicios comerciales en los que un centro de llamadas o *call center* realiza llamadas en nombre de más de un cliente. Asimismo, el CLI presentado no debe estar asociado a un número telefónico que genere un cargo inesperado.

Por otra parte, un operador debe evitar que se complete una llamada si considera que un CLI no es válido o que el mismo no puede ser utilizado para devolver la llamada. Además, si la llamada es originada fuera del Reino Unido, entonces el operador en el primer punto de ingreso es el responsable de verificar que el CLI contenga datos válidos

[8] "Guidance on the provision of Calling Line Identification facilities and other related services"

y, en caso contrario, deberá reemplazar los datos inválidos o faltantes del CLI con un número que se le ha proporcionado para estos fines.

Además, OFCOM ha realizado las siguientes acciones para el bloqueo de llamadas sin un CLI confiable:

- Realizar grupos de trabajo en donde los miembros comparten información sobre números bloqueados en casos de fraude y uso indebido.
- Proporcionar una lista de números no asignados en el Plan Nacional de Numeración de Reino Unido, por lo que no son números válidos y no deberían estar en uso. Los operadores pueden utilizar esta lista para bloquear cualquier llamada con esos CLI.
- Lista de números telefónicos de no *originación*, la cual contiene los números telefónicos que las organizaciones no utilizan para realizar llamadas salientes.
- Trabajar con los operadores móviles y la policía para encontrar soluciones técnicas a las estafas a través de mensajes de texto que fomentan la devolución de llamadas a números falsos.

OFCOM también publicó la Precisión de los Datos de CLI en el que requiere a los operadores, cuando sea técnicamente factible, bloquear las llamadas con CLI que no sean válidos, que no identifiquen de manera inequívoca a la persona que llama o que no contengan un número que se pueda marcar (Ofcom, 2022). Asimismo, realizó una serie de cambios a los Lineamientos del CLI, entre los que se incluyen:

- Precisa que el formato del CLI debe ser de 10 u 11 dígitos.
- Utilizar la información disponible sobre números que no deben ser utilizados en el CLI como la lista de no *originación*.
- Bloquear las llamadas originadas en el extranjero y que no tienen un CLI valido.
- Bloquear las llamadas originadas en el extranjero y que falsifican un CLI del Reino Unido.
- Prohibir el uso de números no geográficos como CLI.

En 2023 OFCOM sometió a consulta pública el documento "Autenticación de identificación de línea de llamada (CLI): un enfoque potencial para detectar y bloquear números falsos", a través del cual invita a los interesados a compartir opiniones sobre cómo podría funcionar la autenticación CLI en el Reino Unido. La consulta se centró en evaluar en qué medida las acciones que los proveedores ya están tomando podrían abordar el problema del spoofing de números. Aunque no se propusieron intervenciones regulatorias específicas en esta etapa, OFCOM indicó que, si su visión provisional tras la

consulta apunta a la necesidad de implementar la autenticación CLI, publicarán una evaluación completa del impacto probable y propuestas para las reglas regulatorias necesarias.

PUNTOS CLAVE DE LA EXPERIENCIA EN REINO UNIDO

- Se han establecido lineamientos que las organizaciones deberán seguir para el envío de mensajes comerciales por medios electrónicos como teléfono, fax, correo electrónico y mensajes de texto.
- Las organizaciones deben garantizar que se ha obtenido de forma clara el consentimiento del consumidor y que el mismo se encuentra vigente, además de verificar que el número del consumidor no se encuentre en la lista de "no llamar".
- OFCOM ha fortalecido reglas y directrices para requerir que todas las redes telefónicas involucradas en la transmisión de llamadas garanticen y verifiquen que la información del CLI sea válida.
- La posible implementación de autenticación de CLI en Reino Unido se encuentra en fase de análisis.

III. Panorama General y Políticas Implementadas en Canadá.

La Comisión Canadiense de Radio, Televisión y Telecomunicaciones (en lo sucesivo, "CRTC" por sus siglas en inglés) (2016), determinó que las soluciones técnicas disponibles hasta entonces para proteger a los canadienses de las telecomunicaciones no deseadas, no solicitadas o ilegitimas no bastaban para combatir dichas conductas. Por lo tanto, la CRTC (2017) realizó la consulta de comentarios sobre las medidas para reducir la suplantación de identidad de las personas que llaman y determinar el origen de las llamadas no deseadas, en el que se aborda la idoneidad, eficacia, viabilidad de la implementación de *STIR/SHAKEN.*

En 2018, la CRTC determinó que los Proveedores de Servicios de Telecomunicaciones (en lo sucesivo, "TSP" por sus siglas en inglés) debían de implementar la autenticación y verificación de la identificación de llamadas para las llamadas de voz mediante el protocolo *STIR/SHAKEN,* a más tardar el 31 de marzo de 2019.

Las determinaciones por parte de la CRTC para cumplir con la implementación *STIR/SHAKEN* fueron las siguientes:

- La CRTC señaló que *STIR/SHAKEN* es la mejor solución viable en la identificación de llamadas, además de que puede aumentar la eficacia de las soluciones de filtrado de llamadas y el bloqueo a nivel de red.
- La CRTC determinó que se debía de establecer un administrador canadiense para la emisión y administración de certificados para *STIR/SHAKEN*.
- Con el fin de monitorear el progreso, los TSP debían de presentar al Comité Directivo de Interconexión de la CRTC (en lo sucesivo "CISC" por sus siglas en inglés) un informe cada seis meses sobre los avances e implementación de las medidas de autenticación y verificación para la identificación de las llamadas.
- La CRTC, ordenó a la CISC el desarrollo de un proceso de rastreo de las llamadas.

Como parte de lo anterior, la CRTC identificó la necesidad de establecer un proceso estandarizado de rastreo de llamadas en toda la industria con independencia del tipo de tecnología utilizada para originar la llamada, con el fin de determinar el origen de las llamadas molestas y tomar las medidas correctivas para que su volumen se reduzca y a su vez se proteja la privacidad de los canadienses. El objetivo de sistema de rastreo de llamadas es el facilitar el cumplimiento de las Reglas de Telecomunicaciones No Solicitadas de Canadá.

Las principales reglas y obligaciones establecidas las Reglas de Telecomunicaciones No Solicitadas de la CRTC incluyen:

- Las empresas de telemercadeo no deben iniciar comunicaciones hacia los usuarios cuyos números se encuentren registrados en la "Lista de No Llamar Nacional" (en lo sucesivo, "DNCL Nacional"), a menos que cuenten con su consentimiento expreso de los usuarios.
- Las empresas de telemercadeo están obligadas a registrarse ante el administrador del DNCL Nacional.
- Las empresas de telemercadeo deben proporcionar información clara al contactar a los usuarios, incluyendo nombre y si están llamando en nombre propio o de un cliente. Además, deben proporcionar un número de teléfono y una dirección para consultas o solicitudes de no llamar.
- Las comunicaciones comerciales están restringidas a ciertos horarios y deben mostrar el número de origen o un número alternativo donde se pueda contactar a las empresas que originan la comunicación.

- El marcado secuencial está prohibido y el marcado aleatorio está permitido con ciertas restricciones.
- Las empresas de telemercadeo que utilizan dispositivos de marcación predictiva no deben superar una tasa de abandono de llamadas del 5% en cualquier mes calendario.

Por otra parte, la CRTC puntualizó que, para garantizar el uso efectivo de los certificados de autenticación, se deben establecer las siguientes entidades:

- Una Autoridad de Gobierno (en lo sucesivo, "AG"), que garantice la integridad de la emisión, gestión, seguridad y uso de los certificados emitidos.
- Un Administrador de Políticas, el cual es fijado por la AG y se encarga de aplicar las reglas definidas por la AG, dentro de las cuales incluye garantizar que las autoridades de certificación (en lo sucesivo, "CA" por sus siglas en inglés) implementen prácticas de gestión de certificados adecuadas y que estos sean emitidos solo a los TSP autorizados.
- La CA, que se encarga de emitir los certificados a los TSP validados.

Ahora bien, el Grupo de Trabajo de la Red CISC (en lo sucesivo, "NTWG" por sus siglas en inglés) en su informe sobre el avance de la implementación de la autenticación y verificación de *STIR/SHAKEN* (2019), señaló que la fecha de cumplimiento establecida, 31 de marzo de 2019, no era factible de alcanzar. Aunado a lo anterior, el NTWG indicó problemas para llevar la implementación de *STIR/SHAKEN* en tiempo y forma, los cuales tuvieron que ver con retrasos e inconvenientes en; preparación y adecuación de la red, pruebas en los equipos, el estado de los estándares de autenticación y verificación, las interconexiones de voz basadas en IP y las Autoridades de Gobernanza. En consecuencia, la CRTC estableció como fecha de implementación de *STIR/SHAKEN* en Canadá a más tardar el 30 de septiembre de 2020.

Simultáneamente, la CRTC (2019) aprobó el establecimiento de la Autoridad Canadiense de Gobernanza de Token Seguro (en lo sucesivo, "CSTGA" por sus siglas en inglés) como la autoridad de gobernanza del despliegue y la implementación de *STIR/SHAKEN*. Asimismo, dentro de la conformación de la CSTGA (2019), se estableció una relación de trabajo con la Autoridad de Gobernanza de Identidad de Teléfono Seguro (en lo sucesivo, "STI-GA" por sus siglas en inglés) de Estados Unidos de América, con el fin de participar en el desarrollo e implementación de los estándares *STIR/SHAKEN*.

En junio de 2020 la CRTC recibió solicitudes por parte de diversos TSP para aplazar la implementación de *STIR/SHAKEN* (2020) debido a la reasignación de recursos y la renegociación de los contratos con proveedores, contratistas y el readquirir capital

financiero para la implementación de *STIR/SHAKEN*, lo anterior debido a crisis de la pandemia, asimismo debido a la falta de interconexiones IP entre varios TSP, a que algunas normas técnicas relativas a *STIR/SHAKEN* no se encontraban totalmente definidas y también el hecho de que la fecha de implementación de *STIR/SHAKEN* en los Estados Unidos de América se encontraba fijada el 30 de junio de 2021.

Conforme lo anterior y debido a que aún se presentaban problemas técnicos y de políticas para la implementación de *STIR/SHAKEN*, la CRTC (2021) aprobó la ampliación del plazo para su implementación estableciendo como fecha límite el 30 de noviembre de 2021.

Adicional a las medidas anteriores, la CRTC estableció reglas para el bloqueo universal de llamadas y filtrado de llamadas, a través de las cuales se obliga a los proveedores de servicios telefónicos que no ofrecen un sistema de filtrado de llamadas opcional a sus usuarios, bloquear todas las llamadas con identificadores de llamadas que no se apeguen al Plan de Numeración de América del Norte.

Además, han surgido iniciativas conjuntas entre la CRTC y la industria, como el caso de *Bell Canada,* operador que implementó un sistema de bloqueo de llamadas basado en inteligencia artificial el cual analiza el tráfico de telecomunicaciones y detecta anomalías que sugieren una posible actividad fraudulenta a nivel de red. La CRTC aprobó su implementación como resultado directo de un período de prueba exitoso, durante el cual se bloquearon más de mil millones de llamadas fraudulentas (CRTC, 2023).

PUNTOS CLAVE DE LA EXPERIENCIA EN CANADÁ

- La CRTC determinó la obligación de los Proveedores de Servicios de Telecomunicaciones de implementar la autenticación y verificación de la identidad de llamadas mediante el protocolo STIR/SHAKEN.
- La CRTC ordenó establecer un proceso estandarizado de rastreo de llamadas a nivel industria, con el fin de determinar el origen de las llamadas molestas y vigilar el cumplimiento de las Reglas de Telecomunicaciones No Solicitadas de Canadá.
- La CRTC estableció reglas para el bloqueo universal de llamadas y filtrado de llamadas, a través de las cuales se obliga a los proveedores de servicios telefónicos bloquear todas las llamadas con identificadores de llamadas que no se apeguen al Plan de Numeración de América del Norte.
- Han surgido iniciativas conjuntas entre la CRTC y la industria, como el caso de *Bell Canada* y la implementación de un sistema de bloqueo de llamadas basado en inteligencia artificial.

IV. Panorama General y Políticas Implementadas en la India

La regulación asociada a las comunicaciones no solicitadas en la India se encuentra a cargo de la Autoridad Reguladora de Telecomunicaciones de la India (en lo sucesivo, "TRAI" por sus siglas en inglés), la cual por medio del Reglamento de Preferencia del Cliente de Comunicaciones Comerciales de Telecomunicaciones (en lo sucesivo, "TCCCPR" por sus siglas en inglés), protege a los usuarios de las comunicaciones comerciales no solicitadas (TRAI, 2018).

El TCCCPR, establece las pautas a las que las entidades encargadas de enviar comunicaciones comerciales deberán apegarse. Dicho reglamento plantea la adopción de la Tecnología de Contabilidad Distribuida (en lo sucesivo, "DLT" por sus siglas en inglés), el cual es un sistema de registro basado en cadena de bloques que tiene como fin garantizar la transparencia y reducir la incidencia de comunicaciones no solicitadas. Además, el TCCPPR prevé, lo que sigue:

- Se lleva a cabo el registro de los remitentes, lo cual disminuye la capacidad de empresas desconocidas de llegar a los suscriptores con llamadas o SMS que resultan ser molestos, fraudulentos o de dudosa naturaleza.
- Se registran encabezados con el propósito de que puedan segregar los tipos de mensajes.
- Se realizan registros de plantillas para SMS y comunicaciones de voz para evitar la mezcla deliberada con información promocional.
- Se registra el consentimiento de los suscriptores, permitiendo a los usuarios tener el control sobre el consentimiento de recibir comunicaciones comerciales.
- Existe un control de horarios en los que se permite tipos específicos de comunicaciones comerciales.

Con la implementación del TCCCPR se ha creado un ecosistema basado en *Blockchain* conocido como DLT, el cual brinda transparencia entre los proveedores y el regulador, en torno en la gestión de las comunicaciones comerciales no solicitadas.

Por tanto, los proveedores de servicios deben de asegurarse que las comunicaciones comerciales sólo se realicen con la utilización de encabezados asignados a los remitentes y que los remitentes registrados para llevar a cabo comunicaciones comerciales tomen medidas para que no inicien llamadas con un marcador automático que resulten en llamadas abandonadas o silenciosas.

Cabe señalar que sólo las entidades que se encuentran registradas en el DLT y cuentan con las plantillas, encabezados y los formatos adecuados pueden mandar comunicaciones comerciales, por el contrario, si el sistema detecta que una comunicación comercial no tiene el formato o el encabezado autorizado el sistema bloquea el envío de dicha comunicación.

Hasta el 2022, se han registrado en la DLT aproximadamente 285,094 entidades principales con 700,394 cabeceras y más de 50, 000 mil plantillas de mensajes aprobadas (BSNL DLT, 2022), lo cual ha reducido las quejas de los clientes en un 60% para las entidades registradas.

Además, como parte de las acciones para hacer frente a las comunicaciones comerciales no deseadas, la TRAI se encuentra en constante revisión del marco regulatorio aplicable a dichas comunicaciones, con el fin de emprender acciones que contribuyan a erradicar las conductas que causan molestias y son fraudulentas a los suscriptores por parte de las entidades que no se han registrado en la DLT, por lo que la TRAI (2022) ha emitido las siguientes medidas:

- Implementación de sistemas de detección de comunicaciones comerciales no solicitadas.
- Depuración inteligente de plantillas de encabezados y mensajes.
- Uso de inteligencia artificial y lenguaje máquina.
- Control y provisión del consentimiento digital de los usuarios.

Así, con el objeto de contar con el control del consentimiento del consumidor en la plataforma tecnológica DLT, la TRAI se encuentra implementando una plataforma de Autorización de Consentimiento Digital (en lo sucesivo, "DCA" por sus siglas en inglés), el cual permitirá a los suscriptores incluir en la lista blanca sus números de teléfono.

La DCA (TRAI, 2018) busca regular y autorizar el consentimiento digital de los usuarios para recibir comunicaciones comerciales. Esto implica que las entidades comerciales deben obtener un consentimiento explícito de los usuarios antes de enviarles mensajes promocionales o llamadas. Para su implementación, se utiliza una plataforma tecnológica que registra y verifica el consentimiento de los usuarios. Los usuarios pueden dar su consentimiento a través de medios digitales, lo que se registra en un sistema centralizado. Además, la DCA permite a los usuarios controlar y gestionar su consentimiento al permitir elegir qué tipos de comunicaciones desean recibir y de qué entidades, así como retirar su consentimiento en cualquier momento. Los datos de consentimiento recopilados se compartirán en la DLT para ser observados por los proveedores de servicios.

Por otra parte, como parte de la regulación para erradicar las llamadas fraudulentas y a los emisores de *spam,* la TRAI está implementando un sistema unificado denominado KYC (del inglés, "Know Your Customer"), diseñado para prevenir el uso indebido de servicios de telecomunicaciones y asegurar la identificación adecuada de los usuarios de dichos servicios.

A través del KYC, los operadores de telecomunicaciones están obligados a verificar la identidad y la dirección de sus usuarios mediante documentos oficiales. Al garantizar que cada cuenta esté vinculada a una identidad verificable, el sistema KYC ayuda a prevenir el fraude, como la suplantación de identidad y el uso ilegal de servicios de telecomunicaciones.

PUNTOS CLAVE DE LA EXPERIENCIA EN LA INDIA

- Se ha creado un ecosistema basado en *blockchain*, el cual brinda transparencia entre los proveedores y el regulador, en torno en la gestión de las comunicaciones comerciales no solicitadas.
- Se realiza el registro de remitentes y encabezados de comunicaciones para segmentar los tipos de mensajes y evitar el envío de comunicaciones no deseadas o fraudulentas.
- A través de un sistema centralizado, DCA, se realizará el registro digital del consentimiento de los usuarios, dándoles control sobre la recepción de comunicaciones comerciales.
- Se encuentra en implementación un sistema para verificar la identidad de los usuarios al momento de adquirir servicios de telefonía móvil o fija. Su objetivo es prevenir el fraude y el uso indebido de los servicios de telecomunicaciones.

V. Enfoque de la Unión Internacional de Telecomunicaciones

La UIT (2021) ha señalado que los mecanismos de autenticación del número de la persona que llama, no son una solución global contra el fraude o la suplantación de identidad. Asimismo, señala que la suplantación de identidad es especialmente nociva para los operadores ya que no tienen forma de prevenir estas llamadas ilegales a través de su numeración y solo se enteran de ellas, por otros operadores o por los usuarios. Además, la falsificación del identificador de llamadas es particularmente efectivo contra el bloqueo estático de llamadas.

La suplantación de identidad es un problema a nivel mundial. En la actualidad se están desarrollando diferentes mecanismos para contrarrestar esta actividad, incluido la detección y bloqueo de la infraestructura utilizada para realizar la suplantación de identidad, así como la autenticación y el bloqueo del CLI. Asimismo, la UIT (2021) ha señalado que las soluciones en tiempo real basadas en el protocolo SIP, son muy complejas de implementar a nivel internacional e impactará a las redes con costosas modificaciones.

El problema del estándar *STIR/SHAKEN*, y de todas las soluciones que marcan las llamadas en el protocolo de señalización, es que no es posible determinar las causas de inconsistencia en las firmas digitales, como pueden ser certificados caducados o errores de transmisión en la red, por lo que no se pueden terminar las llamadas (UIT, 2021).

La UIT (2021), ha indicado que las soluciones basadas en *Blockchain*, en cuanto se definan y adopten ampliamente, deben considerarse más adecuadas, ya que no afectan las redes existentes y son independientes de la tecnología, ya sean redes legadas o VoIP, debido a que actúan al superponer una plataforma de tecnología de la información y las comunicaciones para verificar la información transmitida y llevar a cabo las acciones correspondientes en caso de inconsistencias.

La UIT (2021), ha categorizado los distintos enfoques para resolver este problema en las siguientes soluciones técnicas:

- La autenticación de la línea de llamada como *STIR/SHAKEN.*
- El bloqueo estático de llamadas.
- El bloqueo dinámico de llamadas, el cual es análogo a las soluciones actualmente en uso para filtrar el correo electrónico no deseado.
- Bloqueo de la infraestructura utilizada para realizar llamadas no deseadas.

La autenticación de la línea de llamada es un mecanismo criptográfico para certificar el CLI con el fin de determinar, si el número telefónico de la parte que llama ha sido modificado o si la parte que llama tiene autoridad sobre el número telefónico.

El sistema utiliza un sistema de encriptación para que el operador que termina la llamada pueda validar que ésta fue originada por el operador asociado con el CLI. Las llamadas que no puedan validarse serán bloqueadas por el operador encargado de terminar la llamada.

Para que este sistema sea efectivo, se requiere que los mecanismos de autenticación sean aplicados a nivel mundial y que los operadores bloqueen las llamadas provenientes del extranjero, que no se adhieran a los mismos (UIT, 2021). Esto requerirá de un acuerdo a nivel internacional y las correspondientes modificaciones a las regulaciones nacionales de cada país, por lo que no es probable que sea efectiva la aplicación de este sistema solo a nivel nacional.

Por otra parte, el bloqueo dinámico de llamadas permite que los números telefónicos identificados por el operador como llamadas no solicitadas, sean agregados a una lista

negra o *blacklist*, las cuales serán enviadas automáticamente al correo de voz. La lista negra se puede actualizar de forma continua, con información proveniente de una lista dinámica que contiene los números telefónicos de generadores de spam.

La lista dinámica, incluye los números telefónicos de los centros de llamadas no deseadas, que llaman en horarios inconvenientes o que no cumplen con un código de conducta nacional, como el respetar las listas para no recibir llamadas no solicitadas y el desplegar el número telefónico desde el que se llama. Además, es recomendable que los usuarios puedan establecer su propia lista negra para que todas las llamadas provenientes de los números telefónicos agregados a ésta sean enviadas automáticamente al correo de voz.

PUNTOS CLAVE DEL ENFOQUE DE LA UIT

- La UIT señala que los mecanismos de autenticación del número de la persona que llama no son una solución global contra el fraude o la suplantación de identidad.
- La UIT, ha indicado que las soluciones en tiempo real basadas en el protocolo SIP son muy complejas de implementar a nivel internacional e impactará a las redes con costosas modificaciones.
- El problema de todas las soluciones que marcan las llamadas en el protocolo de señalización es que no es posible determinar las causas de inconsistencias en las firmas digitales, como pueden ser certificados caducados o errores de transmisión en la red.
- La UIT ha señalado que las soluciones basadas en *Blockchain*, en cuanto se definan y adopten ampliamente, deben considerarse más adecuadas, ya que no afectan a las redes existentes y son independientes de la tecnología.

D. Análisis de las alternativas técnicas para el combate de llamadas no deseadas

I. STIR/SHAKEN

La confirmación de la identidad telefónica en redes IP se realiza generalmente a través del encabezado *P-Asserted-Identity* del protocolo SIP. Este modelo asume que existe una relación de confianza entre los proveedores de servicio; sin embargo, existen muchos escenarios en donde las llamadas telefónicas siguen rutas indirectas entre el proveedor de servicio que origina la llamada y aquel encargado de terminarla, por lo que a menudo no es posible identificar el verdadero origen de la llamada telefónica (ATIS, 2022). Por lo anterior, el uso de firmas digitales criptográficas estandarizadas, brinda un mecanismo para validar la identidad del originador de una llamada en redes IP.

El modelo de *STIR/SHAKEN,* es un conjunto de estándares interrelacionados que permiten la verificación del identificador de llamadas entre proveedores de servicio. *STIR* está conformado por una serie de estándares técnicos desarrollados por el Grupo de Trabajo de Ingeniería de Internet (en lo sucesivo, el "IETF" por sus siglas en inglés), para verificar que la parte que llama está autorizada a usar un número telefónico en particular; sin embargo, *STIR* no define como se deben implementar estos estándares (ATIS, 2021).

El modelo de *SHAKEN,* establece una arquitectura de extremo a extremo, que permite tanto a un proveedor de servicio que origina una llamada autenticar la identidad de la persona que llama, así como, al proveedor de servicio que termina la llamada, verificar la identidad de la persona que llama. Los encabezados del protocolo SIP contendrán un indicador del nivel de confianza a través del campo de atestación, para indicar si la persona que llama tiene derecho a utilizar determinado número telefónico.

ATIS (2021), ha identificado tres niveles de atestación, que pueden ser indicados por parte del proveedor de servicio que origina una llamada:

- Atestación Completa: el proveedor de servicio autentica que su cliente ha originado la llamada y que está autorizado a utilizar el número telefónico desde el que llama.
- Atestación Parcial: el proveedor de servicio autentica que su cliente ha originado la llamada, pero no puede verificar que esté autorizado a utilizar el número telefónico desde el que llama.
- Atestación de Puerta de Enlace: el proveedor de servicio autentica desde donde recibió la llamada, pero no puede autenticar el origen de ésta.

El modelo *STIR/SHAKEN,* no previene las llamadas automáticas no solicitadas, pero ayuda a mitigar las llamadas de suplantación de identidad (ATIS, 2021). Existen técnicas de análisis de llamadas para evitar las llamadas automáticas, pero son menos efectivas cuando el número telefónico ha sido suplantado. Para prevenir eficazmente las llamadas automáticas se requiere tanto del modelo *STIR/SHAKEN*, como del servicio de análisis de llamadas.

Además, ATIS (2021) ha identificado las siguientes limitantes del modelo *STIR/SHAKEN*:

- Las redes diversas a las basadas en la tecnología IP, no pueden transmitir el encabezado de identidad.
- Algunos equipos de red que utilizan el protocolo SIP, eliminan el *token* de identidad.
- Algunas redes SIP, utilizan el Protocolo de Datagramas del Usuario (en lo sucesivo, "UDP" por sus siglas en inglés), el cual es propenso a la pérdida y fragmentación de paquetes.
- Si una llamada se transfiere a una interconexión TDM, en cualquier punto de la trayectoria, el *token* de identidad se perderá y no se podrá autenticar el identificador de llamadas.
- Los proveedores de servicio más pequeños que tengan redes basadas en tecnologías legadas como TDM, pueden no tener los recursos necesarios para implementar el modelo *STIR/SHAKEN*.

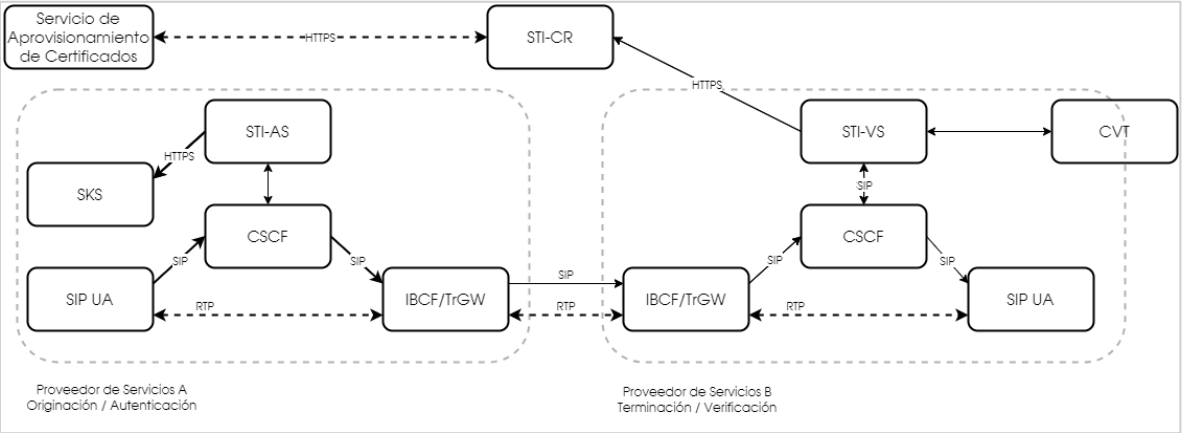
Debido a que el estándar *STIR/SHAKEN,* funciona en redes basadas en tecnología IP, se desarrolla una solución denominada "*Out-of-Band STIR*", en la cual, la información de autenticación del identificador de llamadas se envía a través del Internet, es decir por una ruta diferente a la que se utiliza para establecer la llamada.

Además, la señalización SIP no siempre se transporta de extremo a extremo, ya que las llamadas todavía atraviesan las redes PSTN en algún punto (ATIS, 2021). Generalmente existen tres escenarios:

- Uno o ambos extremos corresponden a redes PSTN.
- Ambos extremos corresponden a redes SIP, pero la llamada transita por la red PSTN en algún punto.
- Las llamadas que transitan por redes SIP de extremo a extremo.

La arquitectura de referencia del modelo *SHAKEN,* conforme ATIS (2022), incluye los siguientes elementos:

Diagrama 1. Arquitectura de Referencia del modelo SHAKEN



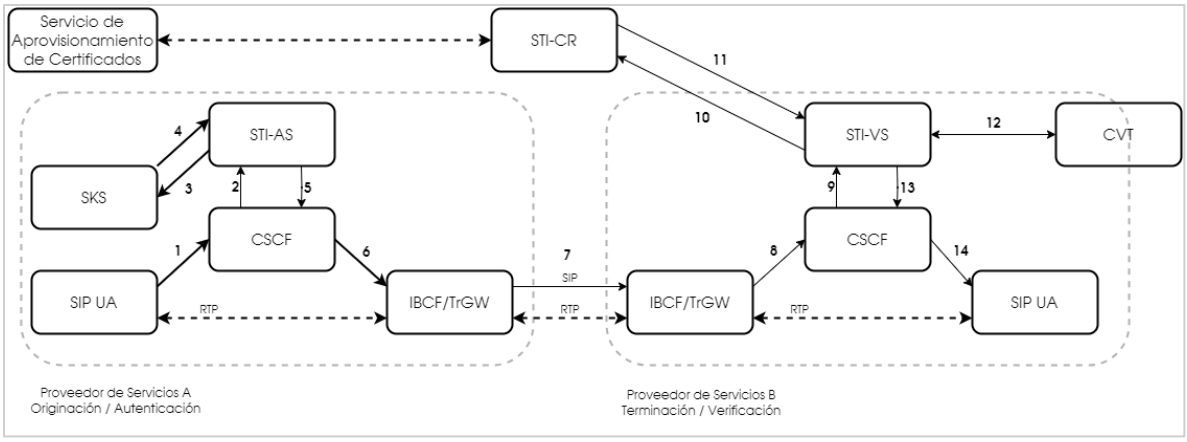
Fuente: Elaboración propia con base en ATIS (2022).

- Agente de Usuario SIP (en lo sucesivo, "UA" por sus siglas en inglés): el proveedor de servicio que origina la llamada puede confirmar la identidad de la parte que llama, cuando el UA está bajo su control directo.
- Función de Control de Sesión de Llamadas (en lo sucesivo, "CSCF" por sus siglas en inglés): este componente realiza la función de enrutamiento y registro SIP.
- Servicio de Autenticación (en lo sucesivo, "STI-AS" por sus siglas en inglés): es un servidor de aplicaciones SIP, el cual realiza la autenticación de los servicios.
- Almacén de Claves Seguras (en lo sucesivo, "SKS" por sus siglas en inglés): es un elemento lógico que almacena las claves secretas para el servicio de autenticación.
- Función de Control de Fronteras de Interconexión (en lo sucesivo, "IBCF" por sus siglas en inglés) / Puerta de Enlace de Transición (en lo sucesivo, "TrGW" por sus siglas en inglés): esta función representa la interfaz de red a red (en lo sucesivo, "NNI" por sus siglas en inglés) o punto de interconexión entre proveedores de servicios telefónicos.
- Servicio de Verificación (en lo sucesivo, "STI-VS" por sus siglas en inglés): es el servidor de aplicaciones SIP, que realiza la función de verificación definido en la recomendación RFC 8224 del IETF. Tiene una interfaz del Protocolo de Transferencia de Hipertexto Seguro (en lo sucesivo, "HTTPS" por sus siglas en inglés), al Repositorio de Certificados de Identidad Telefónica (en lo sucesivo, "STI-CR" por sus siglas en inglés), para recuperar el certificado digital del proveedor de servicio.
- Validación de Llamadas (en lo sucesivo, "CVT" por sus siglas en inglés): es una función lógica que aplica técnicas de análisis y tratamiento de llamadas, una vez que la firma digital ha sido verificada de forma positiva o negativa.

- Repositorio de Certificados de Identidad Telefónica (STI-CR): es un servicio web HTTPS para validar al propietario de un certificado digital.
- Servicio de Aprovisionamiento de Certificados: es un servicio lógico para el aprovisionamiento de certificados digitales utilizados por el STI-CR.

Ahora bien, el flujo de llamada *SHAKEN* conforme ATIS (2022) es el siguiente:

Diagrama 2. Flujo de llamada *SHAKEN*



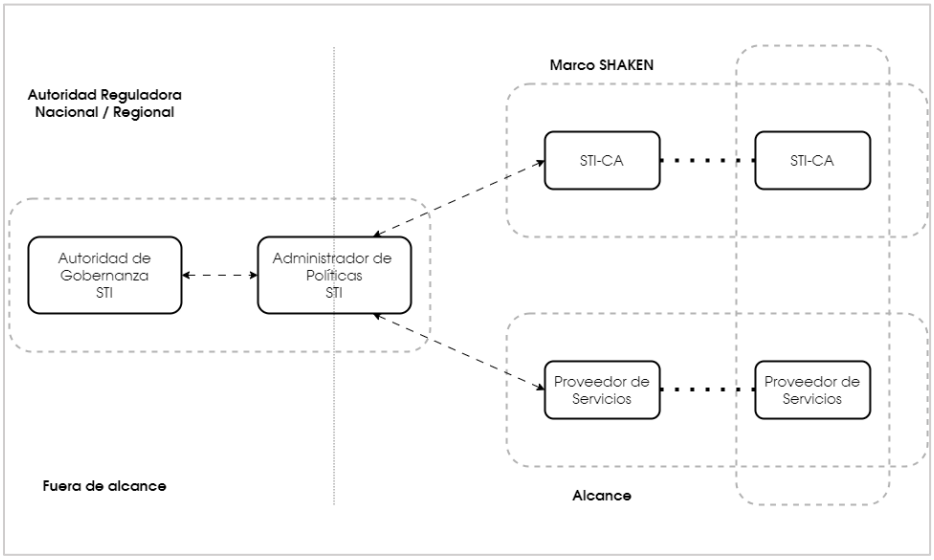
Fuente: Elaboración propia con base en ATIS (2022).

1. El SIP UA que origina la llamada, crea un mensaje SIP INVITE con su identidad telefónica.
2. El CSCF del proveedor de servicio, agrega el encabezado *P-Asserted-Identity* para confirmar la identidad del identificador de llamadas del SIP UA que origina la llamada.
3. El STI-AS del proveedor de servicio, determina la legitimidad de la identidad telefónica utilizada en el mensaje SIP INVITE. Posteriormente el STI-AS solicita sus claves del SKS.
4. El SKS proporciona las claves y el STI-AS las utiliza para firmar el mensaje SIP INVITE, además el STI-AS agrega el encabezado de identidad y utiliza el identificador de llamadas en el encabezado *P-Asserted-Identity*.
5. El STI-AS regresa el mensaje SIP INVITE al CSCF.
6. El CSCF enruta el mensaje SIP INVITE al IBCF.
7. El mensaje SIP INVITE se enruta a la NNI.
8. El IBCF del proveedor de servicio encargado de terminar la llamada, recibe el mensaje SIP INVITE a través de la NNI.
9. El CSCF del proveedor de servicio encargado de terminar la llamada, invoca al STI-VS.

10. El STI-VS del proveedor de servicio encargado de terminar la llamada, utiliza el campo "x5u" del encabezado *PASSporT,* para determinar el Identificador de Recursos Uniforme (en lo sucesivo, el "URI" por sus siglas en inglés) del STI-CR y realizar una solicitud HTTPS al mismo.
11. El STI-VS valida el certificado digital recibido del STI-CR y luego extrae las claves. Posteriormente utiliza las claves para verificar la firma del encabezado de identidad y validar el identificador de llamadas utilizado en el mensaje SIP INVITE del STI-AS del proveedor de servicio, en donde se originó la llamada.
12. El CVT, es una función opcional que se utiliza para el análisis de llamadas y otras técnicas para la mitigación del *spam*. El CVT puede estar integrado en la red del proveedor de servicio o puede realizarse externamente por un tercero.
13. Dependiendo del resultado de la verificación, el STI-VS puede determinar que la llamada debe completarse y que el mensaje SIP INVITE debe regresarse al CSCF, para terminar la llamada en el SIP UA correspondiente.
14. El SIP UA en el que se terminara la llamada, recibe el mensaje SIP INVITE y la señalización se establece con normalidad.

El modelo de *STIR/SHAKEN,* requiere la implementación de los siguientes roles para la gestión de los certificados digitales, según ATIS (2022):

Diagrama 3. Modelo de Gobernanza para la Gestión de Certificados



Fuente: Elaboración propia con base en ATIS (2022).

- Autoridad de Gobierno de Identidad Telefónica Segura (en lo sucesivo, "STI-GA" por sus siglas en inglés): es el encargado de supervisar el cumplimiento de las políticas establecidas o respaldadas por un organismo regulador nacional.

Asimismo, es responsable de establecer las políticas y procedimientos que se deben seguir para la obtención de los certificados digitales y define qué entidades pueden emitir los mismos.

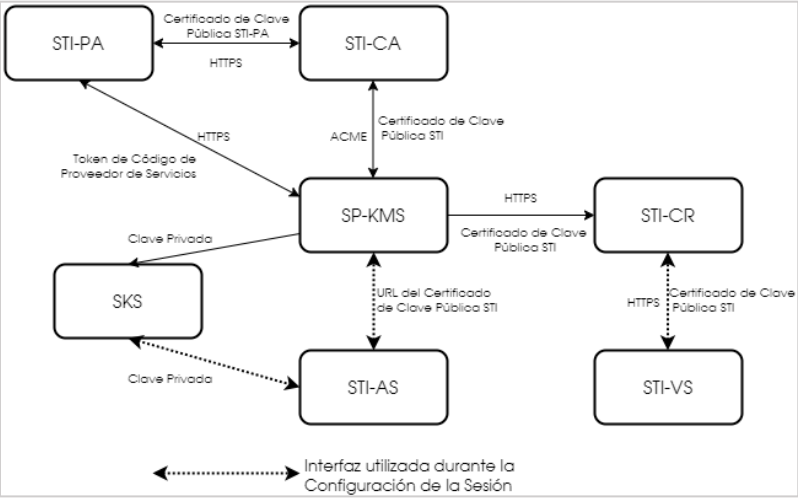
- Administrador de Políticas de Identidad Telefónica Segura (en lo sucesivo, "STI-PA" por sus siglas en inglés): se encarga de aplicar las políticas y reglas definidas por el STI-GA, para asegurar que los proveedores de servicio están autorizados a solicitar los certificados digitales y autoriza al STI-CA a emitir los mismos. Asimismo, administra y proporciona una lista de los STI-CA aprobados a los proveedores de servicio a través de una interfaz HTTPS.
- Autoridad de Certificación de Identidad Telefónica Segura (en lo sucesivo, "STI-CA" por sus siglas en ingles"): se encarga de emitir los certificados digitales a los proveedores de servicio autorizados.
- Proveedores de Servicio: se encarga de obtener los certificados digitales a través del STI-CA para realizar el proceso de autenticación. Asimismo, durante el proceso de verificación se asegura que el STI-CA que emitió el certificado digital, se encuentra en la lista de STI-CA aprobados.

La administración de los certificados digitales requiere la implementación de las siguientes funcionalidades conforme ATIS (2022):

1. Un mecanismo para determinar las STI-CA que pueden emitir certificados digitales.
2. Un procedimiento para crear una cuenta con el STI-CA.
3. Un proceso para solicitar la emisión de certificados digitales.
4. Un mecanismo para validar al proveedor de servicios solicitante.
5. Un proceso para agregar certificados digitales a un repositorio de certificados.
6. Un mecanismo para renovar/actualizar los certificados digitales.
7. Un mecanismo para revocar certificados digitales.

Por lo anterior, ATIS (2022) recomienda la siguiente arquitectura para la administración de certificados digitales:

Diagrama 4. Arquitectura de Gestión de Certificados *SHAKEN*

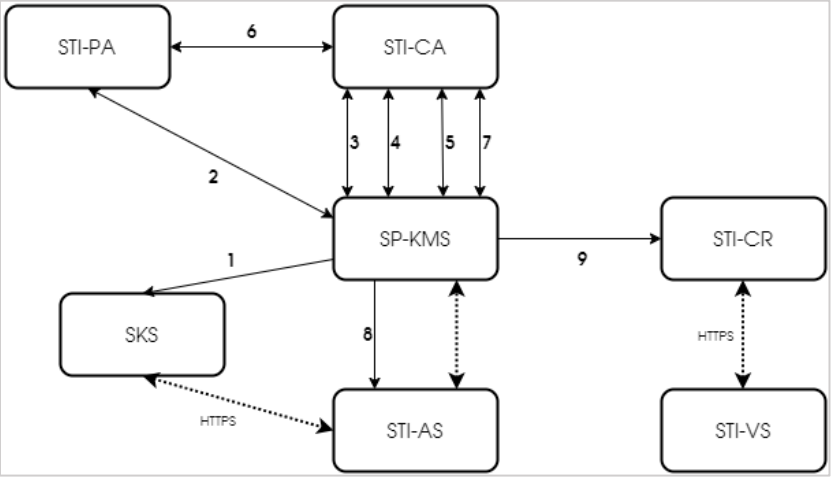


Fuente: Elaboración propia con base en ATIS (2022).

- Servidor de Administración de Claves del Proveedor de Servicio (en lo sucesivo, "SP-KMS" por sus siglas en inglés): es el servidor que genera la dupla de claves privada/pública para firmar, solicitar y recibir un *token* SPC del STI-PA y solicitar un certificado digital del STI-CA.
- Almacén de Claves Seguras (en lo sucesivo, "SKS" por sus siglas en inglés): es donde se guardan las claves privadas utilizadas por el STI-AS del proveedor de servicio que origina la llamada.
- Repositorio de Certificados de Identidad Telefónica Segura (en lo sucesivo, "STI-CR" por sus siglas en inglés): es el servidor HTTPS que contiene la clave pública utilizada por el STI-VS del proveedor de servicio que termina la llamada para validar las firmas.

La administración de los certificados digitales se realiza mediante el siguiente procedimiento definido por ATIS (2022):

Diagrama 5. Gestión de Certificados *SHAKEN*



Fuente: Elaboración propia con base en ATIS (2022).

1. El SP-KMS distribuye la clave privada a su SKS.

Posteriormente, el proveedor de servicio selecciona un STI-CA y realiza los siguientes pasos:

2. El proveedor de servicio genera una dupla de claves públicas/privadas para realizar las transacciones con el STI-CA. Si se trata de la primera transacción que el proveedor de servicio realiza con el STI-CA o si el *token* ha expirado, el SP-KMS envía una solicitud de *token* al STI-PA. El *token* es utilizado por el proveedor de servicio para la obtención del certificado digital.
3. Si aún no lo ha hecho, el STI-KMS se registra en el STI-CA antes de solicitar un certificado digital.
4. Una vez que el SP-KMS se ha registrado en el STI-CA, se puede enviar una solicitud para un nuevo certificado digital. La respuesta a la solicitud incluye una dirección URL para la autorización.
5. El proveedor de servicio que solicita el certificado digital responde proporcionando el *token* vigente adquirido del STI-PA.
6. Si no se ha obtenido previamente, el STI-CA envía una solicitud al STI-PA para validar que el *token* haya sido proporcionado por éste. El STI-CA puede emitir el certificado digital, una vez que ha verificado que el *token* es válido.
7. Se descarga el certificado digital, para ser usado por el SP-KMS.
8. El SP-KMS notifica al STI-AS, que el certificado digital está disponible.
9. El SP-KMS coloca el certificado digital en el STI-CR.

Después de obtener el certificado digital, el proveedor de servicio contactará periódicamente al STI-CA para obtener un certificado digital actualizado y mantener sus

credenciales vigentes. Un proveedor de servicio deberá obtener un *token* valido y actualizado del STI-PA, antes de solicitar la emisión de un certificado digital al STI-CA.

Generalmente se establece una Autoridad de Gestión de Políticas (en lo sucesivo, "PMA" por sus siglas en inglés) encargada de vigilar el cumplimiento de las políticas establecidas (ATIS, 2020). El PMA, se encarga de definir las políticas para la emisión de los certificados y la cual deberá ser seguida por los STI-CA aprobados. Asimismo, los STI-CA deberán proporcionar una declaración de sus prácticas de certificación durante el proceso de aprobación, para asegurar el cumplimiento de las políticas.

PUNTOS CLAVE DE *STIR/SHAKEN*

- El uso de firmas digitales criptográficas estandarizadas brinda un mecanismo para validar la identidad del originador de una llamada en redes VoIP.
- El modelo STIR/SHAKEN, establece una arquitectura que permite tanto a un proveedor de servicio que origina una llamada autenticar la identidad de la persona que llama, así como al proveedor de servicio que termina la llamada verificar la identidad de la persona que llama, antes de que la llamada llegue al destinario.
- Requiere la cooperación entre operadores de redes de telecomunicaciones para intercambiar información de autenticación y verificación y la definición de autoridades que establezcan y vigilen las políticas de operación, así como para la emisión de los certificados digitales.
- El modelo STIR/SHAKEN, no previene de manera directa las llamadas automáticas no solicitadas, pero ayuda a mitigar las llamadas de suplantación de identidad y puede combinarse con otras soluciones para el filtrado de llamadas.
- Debido a que el modelo STIR/SHAKEN, solo funciona en redes basadas en tecnología IP, se está desarrollando una solución denominada "Out-of-Band STIR", en la cual la información de autenticación se envía a través del Internet.

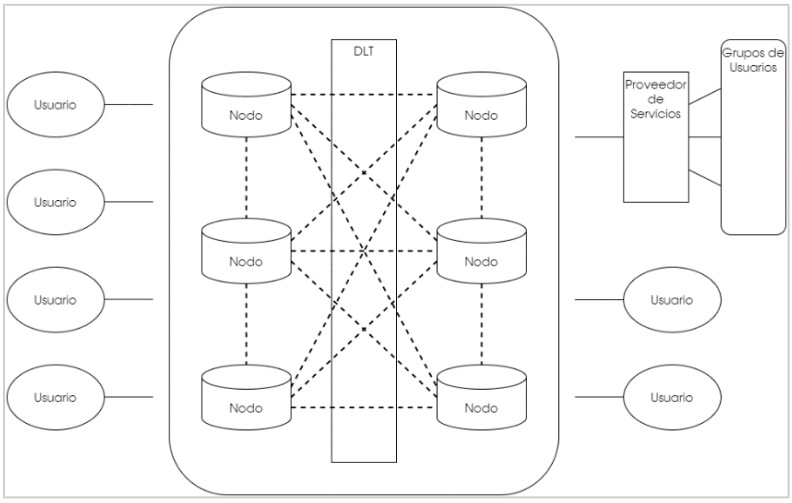
II. Soluciones basadas en *Blockchain*

Las Tecnologías de Registros Distribuidos (en lo sucesivo, "DLT" por sus siglas en inglés) o *Blockchain* permite que los nodos de red registren información sin la necesidad de una autoridad central. El *Blockchain* permite el almacenamiento de datos en grupos denominados bloques, los cuales son validados criptográficamente y vinculados al bloque anterior, por lo que forma de esta manera, una cadena de datos en constante crecimiento (UIT, 2019). Cada nodo mantiene una copia de la información, por lo que no es necesario que la información se almacene en una ubicación central.

Los componentes involucrados en la implementación del DLT, conforme a la UIT (2019) incluyen:

- Nodo: es un sistema individual dentro del entorno DLT. Los denominados "nodos completos", tienen la capacidad de almacenar datos y pasarlos a otros nodos, así como asegurar que los bloques recién agregados sean válidos.
- Proveedor de Servicios: se encarga de ofrecer servicios basados en DLT, a otras partes por medio de las interfaces habilitadas para este fin.
- Usuario: es aquel que utiliza un servicio o consume el producto proporcionado por otro componente. Un componente puede ser el proveedor de algunos servicios y el consumidor de otros.
- Grupo de Usuarios: es un conjunto de usuarios del sistema DLT, los cuales pueden ser grupos de personas y organizaciones.

Diagrama 6. Actores y Componentes DLT



Fuente: Elaboración propia con base en UIT (2019).

Las principales características de los sistemas DLT, conforme a la UIT (2019) son:

- Agregado solamente: a diferencia de las bases de datos tradicionales, las transacciones y los valores en un sistema DLT no se sobrescriben, por lo que solamente se permite agregar información para proporcionar un historial transaccional completo.
- Inmutable: la información se encuentra encriptada para asegurar su seguridad e inmutabilidad, lo cual garantiza, además, que la información no haya sido manipulada y que la misma sea comprobable.
- Compartido: la información es compartida entre varios nodos y solamente algunos contienen toda la información para proporcionar transparencia y una eficiencia óptima.
- Distribuido: la naturaleza distribuida de un sistema DLT, permite escalar los nodos, ya que, al aumentar la cantidad de éstos, se reduce la capacidad de un mal actor para afectar el protocolo de consenso utilizado por los sistemas DLT.

La UIT (2019), ha identificado tres tipos de sistemas DLT, los cuales son:

- Sin permiso: son sistemas abiertos a cualquiera que valide los bloques de información, sin necesidad de permiso de ninguna autoridad. Los usuarios no están obligados a obtener permisos para mantener y operar estos sistemas. Generalmente son implementados utilizando software de código abierto, disponible para cualquier persona que desee descargarlo.
- Autorizado: son sistemas que requieren permisos, por lo que los usuarios que validan los bloquees de información deben estar autorizados. Debido a que solamente los nodos autorizados mantienen copia de la información, es posible restringir el acceso a la lectura de ésta y también se pueden restringir los permisos para realizar transacciones.
- Híbridos: estos sistemas combinan los beneficios de privacidad de los sistemas autorizados, así como la seguridad y transparencia de los sistemas sin permiso. Esto brinda flexibilidad para elegir qué datos se desean hacer públicos y qué datos mantener en privado.

Los mecanismos de consenso son las reglas y procedimientos mediante los cuales los nodos acuerdan la forma de validar las transacciones. En los sistemas DLT, se debe determinar que usuario es el responsable de validar el siguiente bloque de información, ya que esto se implementa mediante alguno de los mecanismos de consenso.

Los mecanismos de consenso más comunes, señalados por la UIT (2019) son:

- Prueba de Trabajo (en lo sucesivo, "PoW" por sus siglas en inglés): en estos sistemas el nodo encargado de validar el siguiente bloque de información es el primero en resolver un problema computacional intensivo. La solución al problema, es la prueba de que han "realizado el trabajo". La probabilidad de validar un nuevo bloque de información depende de la capacidad computacional dedicada a la solución del rompecabezas. Un nodo recibirá cierta cantidad de "criptoactivos" o tarifas por transacción como recompensa por validar un bloque de información.
- Prueba de Participación (en lo sucesivo, "PoS" por sus siglas en inglés): es un proceso de consenso en el que se toma en cuenta la participación existente en el sistema como puede ser la cantidad de información almacenada. La participación suele ser una cantidad de activos criptográficos que los usuarios han invertido en un sistema DLT. Los nodos que participan en este mecanismo de consenso, son recompensados con tarifas por transacción, por cada bloque de información que es validado por primera vez.
- Tolerante a Fallas Bizantinas (en lo sucesivo, "BFT" por sus siglas en inglés): las fallas bizantinas ocurren cuando algunos nodos se comportan de manera anormal. El algoritmo de consenso BFT, ha sido diseñado para resolver este problema al garantizar que el sistema funcione con normalidad incluso cuando existan nodos anormales. Todos los nodos de la red deben participar en el consenso BFT, lo que implica realizar múltiples rondas de votación y comunicación para llegar a un consenso. Por lo tanto, es más adecuado para sistemas pequeños que tienen un número limitado de nodos.

Así mismo, existen cuatro aspectos del ecosistema DLT, que se deben tomar en cuenta: hardware, aspectos comerciales, desarrollo de software y desarrollo de protocolo.

Por su lado, el aspecto de hardware se refiere a los nodos que componen el ecosistema y donde éstos pueden ser una computadora, un servidor o un dispositivo de almacenamiento. Existen tres modalidades de nodos: nodos de validación que producen bloques de información, nodos de validación completos, que no producen bloques de información y nodos parciales o ligeros (UIT, 2019).

Un nodo de validación que produce bloques de información, participa en los procesos de consenso y contiene una réplica completa de la información, incluidas las transacciones que se han ejecutado. Un nodo de validación completa que no produce bloques de información, no participa en los procesos de consenso, pero contiene una réplica completa de la información incluidas las transacciones que se han realizado. Un nodo parcial o ligero, solo contiene una lista de transacciones parciales; sin embargo,

debe estar conectado a un nodo completo para asegurarse de que sus datos sean precisos.

El aspecto comercial se compone de los siguientes elementos según la UIT (2019):

- Usuarios: son entidades que interactúan con un sistema DLT, mediante el uso de aplicaciones, productos o servicios para lograr un propósito especifico como la transferencia de activos.
- Inversores: son las personas u organizaciones que aportan el capital para crear el ecosistema DLT. Los productores de bloques de información, son nodos de validación completos que participan activamente en el proceso de consenso de una red DLT.
- Corporaciones: utilizan los sistemas DLT, para crear espacios donde los usuarios puedan realizar transacciones más fácilmente mientras que la propia corporación se beneficia de una mayor seguridad e integridad de los datos.
- Desarrolladores: son las personas que crean aplicaciones, productos o servicios utilizando los protocolos y redes DLT.

El aspecto de software se refiere a las aplicaciones DLT, las cuales pueden ser escritas utilizando diversos lenguajes de programación. Sin embargo, éstas deben cumplir con los requisitos y especificaciones del software. Las aplicaciones DLT, se dividen generalmente en tres categorías: aplicaciones financieras, las cuales implican el uso y gestión del dinero; aplicaciones semi financieras, las cuales incluyen procesos comerciales que pueden involucrar dinero, pero se enfocan en la finalización de tareas o ejecución de contratos; y aplicaciones no financieras, las cuales incluyen una gran cantidad de actividades como votaciones electorales, almacenamiento de registros de datos y autenticación de identidad (UIT, 2019).

El aspecto de protocolo del ecosistema DLT, se refiere a los desarrolladores y a los académicos. Los desarrolladores están involucrados en la configuración del protocolo DLT, que utilizan las redes, distinguiéndose dos tipos: código de protocolo abierto, el cual permite que las personas descarguen, auditen y envíen cambios al protocolo; y el código de protocolo cerrado, el cual es empleado por entidades privadas y solamente es accesible para operaciones específicas. Por otra parte, los académicos y los investigadores proporcionan revisiones formales al software DLT (UIT, 2019).

La UIT (2019) ha indicado que los sistemas DLT, ofrecen múltiples ventajas respecto a la seguridad:

- Cifrado de datos.
- Control de acceso. A pesar de que los registros existen en muchos nodos de una red DLT, el acceso a éstos se puede restringir por usuario.
- Datos resistentes a la manipulación. Una vez que los datos se cargan en una red DLT, se requieren amplios recursos informáticos y/o una colusión masiva entre las partes interesadas para modificar los datos sin que otros lo noten.
- Gestión de la Identidad. Los participantes en un sistema DLT, pueden ser anónimos, semi anónimos o completamente identificables.
- Tolerancia a fallas. Los algoritmos de consenso del sistema DLT, ofrecen un medio de redundancia para mitigar el riesgo de que la red se vea comprometida si uno o más componentes fallan.

Por lo anterior, los sistemas DLT, han mostrado su potencial como herramientas para verificar la identidad. Sin embargo, una solución para la verificación de la identidad basada en DLT, tiene tres desafíos: la seguridad, la privacidad y la portabilidad (UIT, 2019).

Se puede crear una identificación digital al utilizar una red DLT, descentralizada de código abierto y combinarla con una herramienta de administración de identidades, por lo que tanto las personas como las empresas podrían almacenar y autenticar su identidad (UIT, 2019). Esta identificación digital podría usarse para verificar una identidad en cualquier transacción en tiempo real.

Los sistemas DLT, pueden asociar características y atributos a un individuo sin revelar la identidad de éste, por lo que se pueden utilizar para evitar el robo de identidad sin que exista el riego de filtraciones de información (UIT, 2019).

Se puede implementar la identidad digital como servicio mediante los sistemas DLT, ya que, a través de este servicio, los operadores móviles pueden verificar los datos personales de sus usuarios a petición de éstos. Los sistemas DLT, son una solución óptima para la verificación de la identidad digital conforme a la UIT (2019) debido a que:

- Se puede verificar la información de identidad entre todos los participantes de una plataforma descentralizada, sin revelar la información de identidad en sí.
- Los servicios de identidad digital se pueden proporcionar de manera estandarizada tanto por los operadores móviles como por otras organizaciones autorizadas.
- Los servicios de verificación de la identidad se encuentran disponibles para múltiples proveedores de servicio a través de la misma plataforma DLT.

Sin embargo, la UIT (2019) ha identificado barreras para la adopción de DLT, como son las siguientes:

- Infraestructura legada: el costo de reacondicionar o remplazar los sistemas heredados es alto. Además, se necesita una inversión significativa tanto de tiempo (capacitación) como de capital (equipo, software, aplicaciones) para crear una nueva infraestructura y capacitar al personal con las habilidades necesarias. La transición de los sistemas heredados a los sistemas DLT, será gradual y puede tardar años en completarse, ya que se requiere integrar las tecnologías legadas con las nuevas tecnologías.

- Dilema de compensación: los sistemas DLT, pueden ofrecer descentralización, escalabilidad y seguridad. Sin embargo, solamente dos de estos tres objetivos se pueden alcanzar de forma simultánea. Los problemas de seguridad en las redes DLT pueden causar un impacto significativo en los usuarios ya que, si bien las claves privadas otorgan al usuario el control sobre los datos, la pérdida de ésta puede resultar en la pérdida permanente del acceso a los datos almacenados. Los problemas de escalabilidad pueden crear cuellos de botella en el rendimiento y velocidad de procesamiento de los sistemas afectados por el mecanismo de consenso, la cantidad de nodos y el rendimiento de la red. La descentralización permite la operación autónoma de la red; sin embargo, la descentralización requiere un modelo de gobernanza a través de mecanismos de consenso estrictos y que consumen muchos recursos, además de que existe el riesgo de seguridad en los nodos que utilizan un código obsoleto o hackeado.

- Falta de estándares: no existen estándares aceptados de manera general ni requisitos de interoperabilidad entre distintas plataformas DLT. Las aplicaciones DLT, no siguen un enfoque unificado de arquitectura, diseño de software e interoperabilidad.

- Seguridad de los datos: los sistemas DLT públicos, plantean un problema de seguridad en los datos, ya que, dependiendo de la regulación, puede ser ilegal almacenar cierto tipo de datos sin cifrar. Por otro lado, almacenar datos privados cifrados en un sistema DLT público, es costoso y aún plantea problemas de seguridad.

- Ciclo de retorno de la inversión: los proyectos DLT suelen tener un ciclo de retorno de la inversión más lento en comparación con otras tecnologías emergentes, debido a la lenta adopción por parte de los usuarios. Invertir en nuevas

tecnologías puede ser costoso, por lo que la incertidumbre respecto al ciclo de retorno, es una barrera importante para su adopción masiva. Asimismo, los sistemas DLT, muestran un mayor retorno de la inversión cuando diferentes participantes cooperan en la creación de una plataforma compartida, ya que crear una plataforma para servir a una sola entidad o empresa, trae pocos beneficios comerciales y operativos.

- Posibles altos costos de implementación: los potenciales altos costos de la implementación inicial aunado a los riesgos asociados a la adopción temprana de los sistemas DLT, pueden plantear desafíos importantes.

- Riegos a la privacidad: aunque los sistemas DLT, pueden implementarse para compartir datos a través de redes públicas, todavía se debe garantizar que los métodos de encriptación actuales y futuros, sean lo suficientemente fuertes para conservar la privacidad del usuario. Además, tanto los gobiernos, como los reguladores, deben desarrollar leyes y reglamentos que aborden los beneficios y desafíos específicos que presentan los sistemas DLT.

PUNTOS CLAVE DE SOLUCIONES BASADAS EN *BLOCKCHAIN*

- *Blockchain* permite el almacenamiento de datos en grupos denominados bloques, los cuales son validados criptográficamente y vinculados al bloque anterior, formando de esta manera una cadena de datos en constante crecimiento.

- Los mecanismos de consenso son las reglas y procedimientos mediante los cuales los nodos acuerdan la forma de validar las transacciones.

- Se puede implementar la identidad digital como servicio mediante los sistemas DLT, ya que a través de este servicio los operadores pueden verificar los datos personales de sus usuarios.

- Los sistemas DLT han mostrado su potencial como herramientas para verificar la identidad, sin embargo, la adopción de *blockchain* para la autenticación de CLI en el ámbito de las telecomunicaciones aún no tiene un uso extendido.

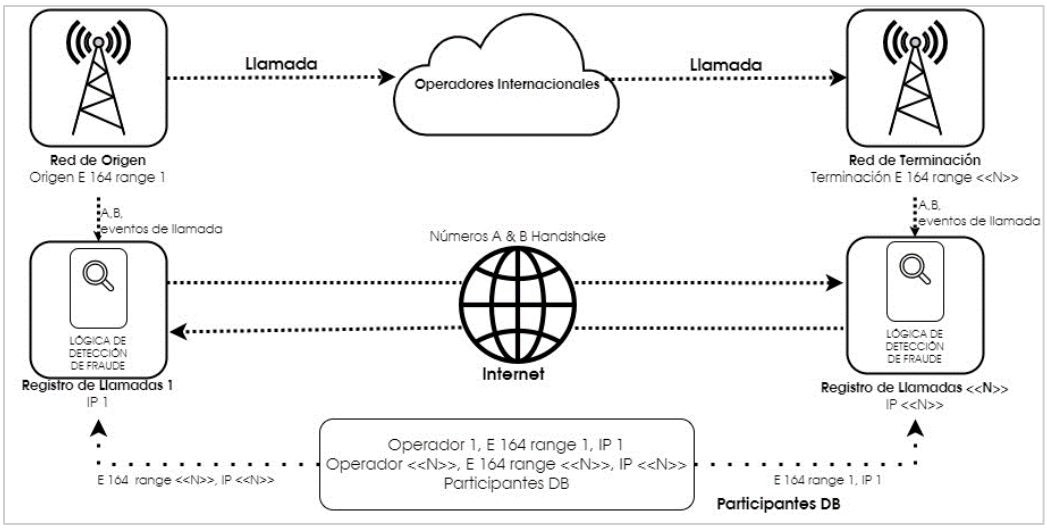
III. *AB Hanshake*

La solución *AB Handshake* es promovido por la *AB Handshake Corporation*, la cual utiliza un método de validación fuera de banda para no interferir con el proceso de establecimiento de una llamada telefónica. Esta arquitectura permite una integración tanto con redes IP, como legadas; asimismo, el flujo de llamadas locales e internacionales no se ve afectado por el método de validación de *AB Handshake* (Electronic Communications Committee, 2022).

Esta es una solución para detectar fraudes en tiempo real mediante la cooperación entre operadores que validan el tráfico enviado entre sus redes. Actualmente esta solución se utiliza para validar el tráfico intercambiado en tiempo real entre operadores ubicados en diferentes regiones geográficas.

La solución de *AB Handshake,* se encuentra en uso entre proveedores de servicio para mitigar los riesgos asociados al fraude en los servicios de voz internacional. La prestación del servicio de *AB Handshake* se realiza de la siguiente manera conforme al Foro Internacional de Interconexión (en lo sucesivo, "i3 Forum" por sus siglas en inglés) (2020):

Diagrama 7. Principio de funcionamiento de AB Handshake



Fuente: Elaboración propia con base en i3 Forum (2020).

- El operador que origina la llamada almacena el número llamante (número de A), el número al que se llama (número de B) y el estampado de tiempo en su base de datos denominada "registro de llamadas de origen" antes de pasar la llamada saliente a las centrales IP (en lo sucesivo, "IPX" por sus siglas en inglés).

- El operador que termina la llamada también almacena el número de A, el número de B y el estampado de tiempo en su base de datos denominada "registro de llamadas de terminación" al recibir la llamada entrante del IPX[9].
- Los registros de llamadas de ambos operadores verifican a través de una ruta paralela basada en el protocolo HTTP los detalles de la llamada para determinar su validez.

La solución de *AB Handshake,* requiere que todos los operadores que participan en este modelo presenten el rango de numeración que tienen asignado y la dirección IP, de su registro de llamadas, a la entidad que coordina el servicio (i3 Forum, 2020). La entidad coordinadora, pondrá a disposición de todos los participantes esta información, para facilitar el enrutamiento entre registros de llamadas.

Debido a que la información distribuida por la entidad coordinadora contiene el mapeo entre los números telefónicos y la dirección IP, de los registros de llamadas, ésta puede ser utilizada para comprobar el origen de una llamada. Asimismo, *AB Handshake,* puede bloquear las llamadas fraudulentas en tiempo real o emitir solamente una alerta sin que exista bloqueo.

Todos los detalles de las llamadas son guardados en un registro, para ser utilizados en caso de una investigación o disputas entre operadores. Además, en caso de que la validación de la llamada no sea posible debido a la falta de respuesta de cualquiera de las partes, la llamada se establece sin interrupción. La validación de las llamadas se realiza directamente, entre los registros de llamadas de los operadores involucrados.

Esta solución puede detectar y bloquear otros tipos de fraudes telefónicos, como la suplantación de identidad, ya que *AB Handshake,* valida todos los parámetros de una llamada telefónica (Electronic Communications Committee, 2022). Además, se contempla que esta solución también pueda aplicarse para la validación del tráfico de mensajes cortos "persona a persona", así como de "aplicación a persona".

Sin embargo, se necesita un conocimiento detallado en tiempo real sobre los números telefónicos asignados a cada operador, por lo que se requiere integrar la base de datos de portabilidad numérica dentro del ecosistema de *AB Handshake*.

[9] Servicio de interconexión ofrecido por operadores de telecomunicaciones.

PUNTOS CLAVE DE SOLUCIONES BASADAS EN *AB HANDSHAKE*

- La solución *AB Handshake*, utiliza un método de validación fuera de banda para no interferir con el proceso de establecimiento de una llamada telefónica. Esta arquitectura permite una integración tanto con redes IP, como legadas. Además, el flujo de llamadas locales e internacionales no se ve afectado por el método de validación de *AB Handshake.*

- La solución de *AB Handshake*, requiere que todos los operadores que participan en este modelo presenten el rango de numeración que tienen asignado y la dirección IP, de su registro de llamadas, a la entidad que coordina el servicio.

- *AB Handshake*, puede bloquear llamadas fraudulentas en tiempo real o emitir solamente una alerta sin que exista bloqueo. Todos los detalles de las llamadas son guardados en un registro de llamadas, para ser utilizados en caso de una investigación o disputas entre operadores.

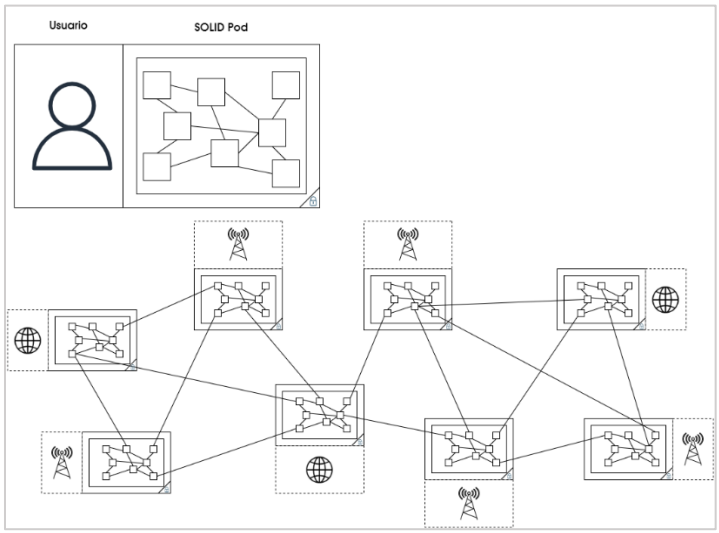
- Esta solución necesita un conocimiento detallado en tiempo real sobre los números telefónicos asignados a cada operador, por lo que se requiere integrar la base de datos de portabilidad numérica dentro del ecosistema de *AB Handshake.*

IV. *SEISMIC*

La solución de *SEISMIC* (*Stopping Exploitation Inter-Network Signal Fraud by Mitigating Illegitimate Communications*) es una iniciativa de la Asociación GSM (en lo sucesivo, "GSMA" por sus siglas en inglés) que busca eliminar varios tipos de fraude que se realizan en la interconexión entre operadores. Se basa en una infraestructura distribuida que utiliza estándares web abiertos para SOLID (*Social Linked Data*), con *pods*[10] individuales por proveedor de servicio, para garantizar la seguridad de extremo a extremo en el establecimiento de una llamada. Además, cada entidad individual controla los datos en su *pod* y elige con qué otras entidades los compartirá.

[10] Bases de datos descentralizadas

Diagrama 8. Arquitectura de SOLID



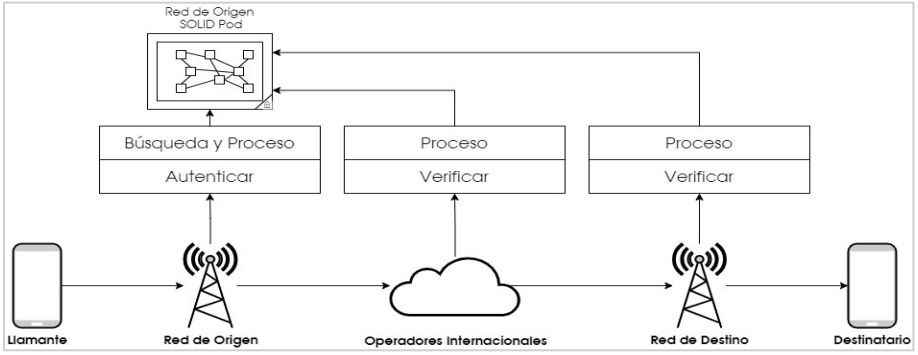
Fuente: Elaboración propia con base en i3 Forum (2019).

SOLID, es un conjunto de convenciones y herramientas para crear aplicaciones descentralizadas basadas en los principios de *Linked Data*[11]. El modelo de SOLID es modular y extensible, basándose principalmente en los estándares y protocolos W3C (*World Wide Web Consortium*) existentes.

Además SOLID, utiliza el protocolo HTTP, por lo que es compatible con una serie de estándares y protocolos abiertos. Asimismo, SOLID reutiliza la infraestructura usada para el tráfico de la *Web* por lo que no requiere nuevos protocolos o infraestructura adicional.

El modelo descentralizado de seguridad de SOLID permite la validación del número de A, debido a que cuenta con autenticación, autorización y cifrado punto a punto:

Diagrama 9. Proceso de Autenticación y Verificación



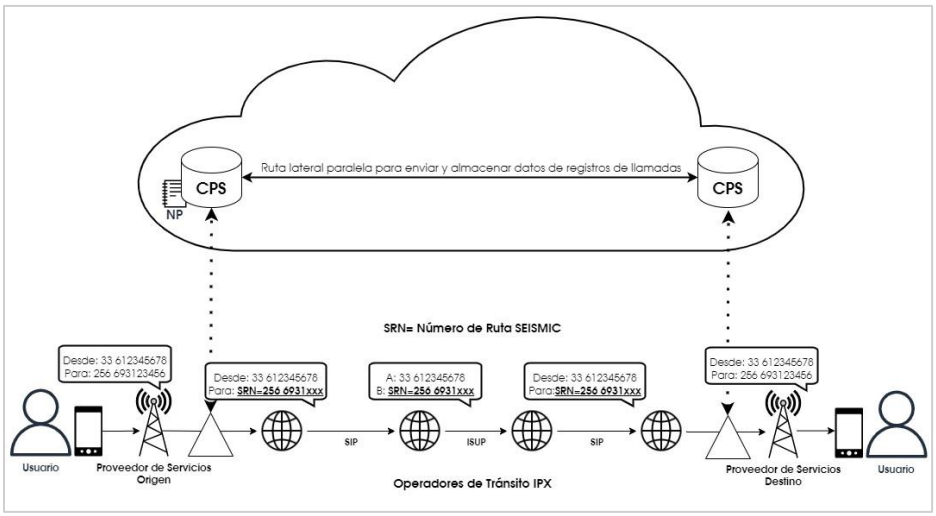
[11] Conjuntos de datos interrelacionados en la Web

Fuente: Elaboración propia con base en i3 Forum (2019).

SEISMIC asegura que el operador móvil encargado de terminar la llamada pueda detectar si se trata de una llamada fraudulenta y decidir si dejar que la llamada continúe, bloquear la llamada o determinar cualquier otra acción.

Una posible implementación es mediante el reemplazo del número de B, por el número de enrutamiento *SEISMIC* (en lo sucesivo, "SRN" por sus siglas en inglés), para entregar la llamada al proveedor de servicio encargado de terminarla:

Diagrama 10. Funcionamiento de SEISMIC



Fuente: Elaboración propia con base en i3 Forum (2020).

Este sigue el mismo principio de enrutamiento utilizado entre operadores móviles para la entrega de llamadas a usuarios itinerantes en el extranjero. La ocultación temporal del número de B y la transferencia de los datos del registro de llamadas por una ruta paralela, proporciona protección contra varios tipos de fraude como la modificación del CLI. Sin embargo, la ocultación temporal del número de B, ocasionará que las llamadas no se puedan establecer si se interrumpe el servicio de *SEISMIC* o si las llamadas son terminadas en redes que no lo soportan.

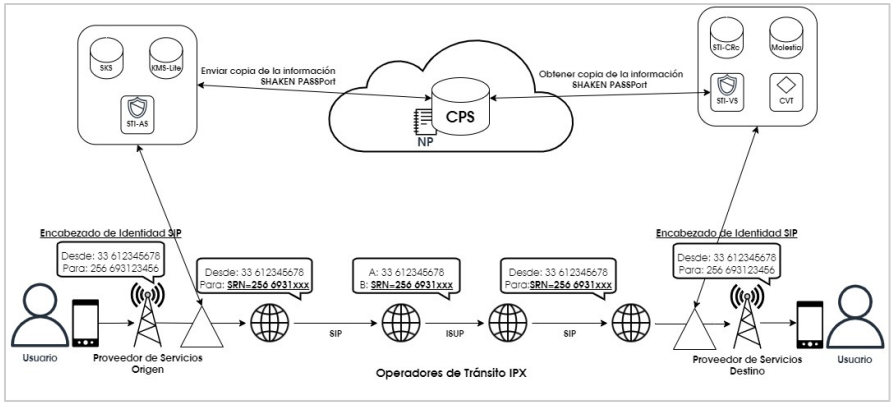
El i3 Forum (2020) ha identificado las siguientes ventajas de SEISMIC respecto al modelo de *STIR/SHAKEN*:

- Funciona independientemente del tipo de señalización por lo que se puede usar en redes basadas en SIP o TDM.
- No requiere que la señalización SIP sea soportada de extremo a extremo.

- No depende de una autoridad de gestión central ya que funciona de forma bilateral.

Por lo anterior, se contempla que soluciones como *SEISMIC* sean suplementarias de *STIR/SHAKEN* para la validación de llamadas entre redes ya que pueden conectar diferentes dominios (regionales o nacionales) de *STIR/SHAKEN*:

Diagrama 11. Potencial uso de SEISMIC con STIR/SHAKEN



Fuente: Elaboración propia con base en i3 Forum (2020).

Sin embargo, la GSMA está evaluando la interoperabilidad de *SEISMIC*, para la validación del CLI, por lo que el proceso de estandarización se encuentra detenido.

PUNTOS CLAVE DE SOLUCIONES BASADAS EN *SEISMIC*

- El modelo descentralizado de seguridad de SOLID permite la validación del número de A debido a que cuenta con autenticación, autorización y cifrado punto a punto.

- SEISMIC asegura que el operador encargado de terminar la llamada pueda detectar si se trata de una llamada fraudulenta y decidir si dejar que la llamada continúe, bloquear la llamada o determinar cualquier otra acción.

- SEISMIC funciona independientemente del tipo de señalización por lo que se puede usar en redes basadas en SIP o TDM, y no requiere que la señalización SIP, sea soportada de extremo a extremo.

- Se contempla que SEISMIC sea suplementaria de STIR/SHAKEN para la validación de llamadas entre redes.

V. Aplicaciones móviles

La identificación de llamadas por medio de aplicaciones para dispositivos móviles con el objeto de filtrar las llamadas no deseadas es una solución basada principalmente en la utilización de bases de datos y en el análisis comparativo de estas e involucra los siguientes elementos:

- Base de datos: La conformación de la base de datos a partir de diversas fuentes, principalmente a través de la contribución de los usuarios al compartir información de llamadas y lista de contactos, bases de datos que contienen directorios telefónicos públicos y de la información proporcionada por operadores de servicios de telecomunicaciones.

- Algoritmos: Las aplicaciones para combatir las llamadas no deseadas utilizan técnicas de coincidencia de patrones, aprendizaje automático, análisis de comportamientos y retroalimentación de los usuarios, para mejorar los algoritmos de detección de llamadas no deseadas.

En este sentido, los algoritmos utilizados son una combinación del aprendizaje automático, la minería de datos y el análisis de patrones llevado a cabo en la identificación de llamadas no deseadas.

Este tipo de aplicaciones pueden identificar al llamante y llevar a cabo la acción necesaria para combatir las llamadas no deseadas, la cual consiste no sólo en el bloqueo de la misma, sino también en no recibir de manera anticipada dichas comunicaciones, todo esto en tiempo real y previo análisis automático de la aplicación, o de forma manual por parte del usuario.

Una de las aplicaciones más utilizadas a nivel global es *TRUECALLER* (2022) , la cual es una aplicación que identifica de manera automática llamadas de acoso, fraudes, robocalls, etc. Dicha aplicación, cuenta con más de 350 millones de usuarios activos a nivel mundial y ha bloqueado e identificado más de 37 mil millones de llamadas (TRUECALLER, 2023).

A nivel internacional, algunos prestadores de servicios móviles ofrecen a sus usuarios aplicaciones de filtrado y bloqueo de llamadas no deseadas, como el caso de T-Mobile y su aplicación para teléfonos iOS y Android *Scam Shield* (2023), Uscellular y la aplicación *Call Guardian* (2023), y Verizon con la aplicación Call Filter (2023).

Cabe señalar que los operadores de telecomunicaciones, para poder ofrecer el servicio de identificar y bloquear las llamadas no deseadas, hacen uso de los servicios de proveedores de soluciones analíticas, como lo son *Hiya*, *TNS Call Guardian*, *Call Transparency*, entre otros (CTIA, 2019).

PUNTOS CLAVE DE SOLUCIONES BASADAS EN APLICACIONES MÓVILES

- Las aplicaciones para el filtrado y bloqueo de llamadas no deseas se basan en la conformación de la base de datos integradas con la información de usuarios, directorios telefónicos públicos y de la información proporcionada por operadores de servicios de telecomunicaciones.
- Utilizan técnicas de coincidencia de patrones, aprendizaje automático, análisis de comportamientos y retroalimentación de los usuarios, para la mejorara de los algoritmos de detección de llamadas no deseadas.

E. Comparativa de las alternativas de solución

Se deben de tomar en cuenta algunas consideraciones generales, para elegir la solución más adecuada al combatir las llamadas de suplantación de identidad según el i3 Forum (2020):

- Las soluciones estandarizadas, son más adecuadas debido a que se requiere la confianza mutua entre los operadores y apertura a las prácticas técnicas implementadas.
- No se deben *anonimizar* datos como el número de enrutamiento, ya que los proveedores de servicio mayoristas y los IPX, necesitan tener visibilidad de todos los datos para brindar sus servicios.
- Las soluciones que implican el cifrado de la información para la autenticación y validación del CLI como *STIR/SHAKEN* son aceptables.

Por lo anterior, aunque los únicos costos de hardware asociados para la implementación de la solución de *AB Handshake,* son los servidores para implementar los registros de llamadas (AB Hanshake), el seleccionar soluciones propietarias que no se encuentren debidamente estandarizadas, es discorde con las mejores prácticas internacionales.

Por otro lado, *SEISMIC* es una solución descentralizada que puede trabajar en redes de telecomunicaciones basadas en tecnología SIP, TDM o híbridas. Además, está diseñada para combatir los siguientes tipos de fraudes cometidos por los usuarios como ha indicado el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (en lo sucesivo, "BEREC" por sus siglas en inglés) (2019):

- Suplantación de identidad.
- *Bypass*.[12]
- *Wangiri*.[13]
- *Spam*.

Asimismo, BEREC (2019) ha señalado que *SEISMIC* puede combatir los siguientes tipos de fraudes cometidos por los operadores:

[12] Técnicas para la terminación de llamadas que buscan eludir las rutas de interconexión legales y desviar las llamadas entrantes internacionales.
[13] Llamadas de corta duración que buscan dejar una notificación de llamada perdida para incitar a que el usuario devuelva la llamada.

- Suplantación de identidad.
- *Bypass*.
- *Call Stretching*.[14]
- *Short Stopping*.[15]
- IRSF.[16] ("*International Revenue Share Fraud"*)

Además, se contempla que *SEISMIC,* sea complementaria de *SITR/SHAKEN*. Sin embargo, esta solución todavía se encuentra en proceso de estandarización.

La solución de *Blockchain* utiliza un modelo distribuido que puede trabajar en redes de telecomunicaciones basadas en tecnología SIP y TDM. *Blockchain* está diseñada para combatir los siguientes tipos de fraudes cometidos por los usuarios como ha indicado BEREC (2019):

- Suplantación de identidad.
- *Bypass*.
- *Wangiri*.
- *Spam*.

Además, puede combatir los siguientes tipos de fraudes cometidos por los operadores de telecomunicaciones como ha indicado BEREC (2019):

- Suplantación de identidad.
- *Bypass*.
- *Call Stretching*.
- *Short Stopping*.
- IRSF.

Sin embargo, todavía no existen estándares aceptados de manera general ni requisitos de interoperabilidad entre las distintas plataformas DLT. Asimismo, los operadores pueden enfrentar posibles altos costos de implementación inicial.

[14] Se produce cuando un operador desconecta al número de B de una llamada, mientras mantiene conectado al número de A, reproduciendo durante este tiempo un fragmento de la conversación, para mantenerlos conectados el mayor tiempo posible y así aumentar los cargos.
[15] Se produce cuando una llamada es desviada por un operador de tránsito a un call center o a una grabación destinada a mantener a la persona que llama conectada el mayor tiempo posible, para aumentar los cargos.
[16] Tipo de fraude que utiliza distintas técnicas para realizar llamadas no autorizadas a números premium.

STRI/SHAKEN sigue un modelo centralizado que solamente funciona en redes de telecomunicaciones basadas en tecnología SIP. BEREC (2019) ha señalado que esta solución puede combatir los siguientes tipos de fraudes cometidos por los usuarios:

- Suplantación de identidad.
- *Bypass*.
- *Wangiri*.
- *Spam*.

Sin embargo, *STIR/SHAKEN,* no está diseñada para combatir los fraudes cometidos por operadores (BEREC, 2019). Además, la implementación de esta solución puede ser costosa y compleja debido a que todo el tráfico que cursa por las redes de telecomunicaciones debe ser migrado a IP, ya que, *STIR/SHAKEN,* requiere que la señalización SIP, sea soportada de extremo a extremo.

Por otra parte, el i3 Forum (2020) ha señalado lo siguiente respecto a *STIR/SHAKEN*:

- *STIR/SHAKEN,* se considera la solución más favorable a largo plazo debido a que tiene menos impacto en las actividades de los operadores mayoristas y los IPX, ya que combina la autenticación y validación de extremo a extremo del CLI, mientras mantiene la visibilidad del número de A.
- *STIR/SHAKEN,* no será la única solución para resolver el problema de suplantación de identidad debido a los diferentes marcos regulatorios, la complejidad del problema y los distintos tipos de fraudes presentes en las diferentes regiones.
- Se deben considerar soluciones que sean interoperables con *STIR/SHAKEN*.
- Los IPX, internacionales deben aprovechar la experiencia de Estados Unidos de América respecto a la colaboración que tuvieron, tanto los operadores de telecomunicaciones entre sí como con su agencia reguladora, en la adopción e implementación de *STIR/SHAKEN*.
- Soluciones como *STIR/SHAKEN,* combaten efectivamente el problema de la suplantación de identidad; sin embargo, ésta no protege contra otros tipos de fraudes.

Por lo anterior, se resalta que existen visiones encontradas respecto a la adopción de *STIR/SHAKEN,* ya que mientras el i3 Forum, considera que esta es la solución más adecuada a largo plazo, la UIT ha señalado que las soluciones basadas en *Blockchain* deben ser consideradas más adecuadas en cuanto se definan y adopten ampliamente los estándares.

PUNTOS CLAVE COMPARATIVA DE LAS ALTERNATIVAS DE SOLUCIÓN

- Las soluciones estandarizadas son más adecuadas debido a que se requiere la confianza mutua entre los operadores y apertura a las prácticas técnicas implementadas.

- Las soluciones que implican el cifrado de la información para la autenticación y validación del CLI, como STIR/SHAKEN, son aceptables.

- No se considera adecuado el seleccionar la solución de AB *Handshake*, ya que las soluciones propietarias que no se encuentren debidamente estandarizadas no es acorde a las mejores prácticas internacionales.

- SEISMIC es una solución descentralizada que puede trabajar en redes de telecomunicaciones basadas en tecnología SIP, TDM o híbridas. SEISMIC puede ser una solución complementaria de STIR/SHAKEN. Sin embargo, esta solución todavía se encuentra en proceso de estandarización.

- Las soluciones basadas en *blockchain*, utilizan un modelo distribuido que puede trabajar en redes de telecomunicaciones basadas en tecnología SIP y TDM. Sin embargo, todavía no existen estándares aceptados de manera general ni requisitos de interoperabilidad entre las distintas plataformas DLT. Asimismo, los operadores pueden enfrentar posibles altos costos de implementación inicial.

- STIR/SHAKEN, sigue un modelo centralizado que solamente funciona en redes de telecomunicaciones basadas en tecnología SIP. La implementación de STIR/SHAKEN, puede ser costosa y compleja debido a que todo el tráfico que cursa por las redes de telecomunicaciones debe ser migrado a IP, ya que STIR/SHAKEN, requiere que la señalización SIP sea soportada de extremo a extremo.

- Existen visiones encontradas respecto a la adopción de STIR/SHAKEN, ya que, mientras el i3 Forum, considera que esta es la solución más adecuada a largo plazo, la UIT ha señalado que las soluciones basadas en blockchain, deben ser consideradas más adecuadas en cuanto se definan y adopten ampliamente estos estándares.

Referencias:

3GPP. (2014). *Recomendación TR 33.831.* Obtenido de https://www.3gpp.org/ftp/Specs/archive/33_series/33.831/33831-c00.zip

3GPP. (2022). *Recomendación TR 33.937.* Obtenido de https://www.3gpp.org/ftp/Specs/archive/33_series/33.937/33937-h00.zip

AB Hanshake. (s.f.). *AB Handshake Global Solution for Call Validation.* Obtenido de https://www.gsma.com/membership/wp-content/uploads/2021/04/AB-Handshake_whitepaper.pdf

ATIS. (2020). *ATIS-1000084.* Obtenido de https://access.atis.org/apps/group_public/download.php/55473/ATIS-1000084.v002.pdf

ATIS. (2021). *Robocalling and Communication ID Spoofing.* Obtenido de https://access.atis.org/apps/group_public/download.php/57909/ATIS-I-0000081.pdf

ATIS. (2022). *ATIS-1000080.* Obtenido de https://access.atis.org/apps/group_public/download.php/69428/ATIS-1000080.v005.pdf

ATIS. (2022). *Signature-based Handling of Asserted information using toKENS (SHAKEN).* Obtenido de https://access.atis.org/apps/group_public/download.php/67436/ATIS-1000074.v003.pdf

BEREC. (2019). *BoR (19) 241.* Obtenido de https://www.berec.europa.eu/sites/default/files/files/document_register_store/2019/12/BoR_%2819%29_241_-_Report_Fraud_Misuse_of_Numbers.pdf

BSNL DLT. (2022). *A Secured DLT platform.* Obtenido de https://www.ucc-bsnl.co.in/#features

CFCA. (2023). *Communications Fraud Control Association .* Obtenido de https://cfca.org/telecommunications-fraud-increased-12-in-2023-equating-to-an-estimated-38-95-billion-lost-to-fraud/

CRTC. (2016). *Compliance and Enforcement and Telecom Regulatory Policy CRTC 2016-442.* Obtenido de https://crtc.gc.ca/eng/archive/2016/2016-442.htm

CRTC. (2017). *Compliance and Enforcement and Telecom Notice of Consultation CRTC 2017-4.* Obtenido de https://crtc.gc.ca/eng/archive/2017/2017-4.htm

CRTC. (2019). *Compliance and Enforcement and Telecom Decision CRTC 2019-402.* Obtenido de https://crtc.gc.ca/eng/archive/2019/2019-402.htm

CRTC. (2019). *Compliance and Enforcement and Telecom Decision CRTC 2019-403.* Obtenido de https://crtc.gc.ca/eng/archive/2019/2019-403.htm

CRTC. (2020). *Compliance and Enforcement and Telecom Decision CRTC 2019-402-2.* Obtenido de https://crtc.gc.ca/eng/archive/2019/2019-402-2.htm

CRTC. (2021). *Compliance and Enforcement and Telecom Decision CRTC 2021-123.* Obtenido de https://crtc.gc.ca/eng/archive/2021/2021-123.htm

CRTC. (2023). *Caller ID Spoofing*. Obtenido de https://crtc.gc.ca/eng/phone/telemarketing/identit.htm

CST-GA. (2019). *Canadian Secure Token Governance Authority.* Obtenido de https://cstga.ca/

CST-GA. (2020). *CST-GA Selects Neustar as Secure Telephone Identity Policy Administrator and Certification Authority in Canada.* Obtenido de https://cstga.ca/news/cst-ga-selects-neustar-as-secure-telephone-identity-policy-administrator-and-certification-authority-in-canada/
CST-GA. (2021). *Canadian Secure Token Governance Authority.* Obtenido de https://cstga.ca/wp-content/uploads/2021/10/CST-GA-Policy-Guide_V1.2.pdf
CTIA. (2019). *HowtoStopRobocalls.* Obtenido de https://www.ctia.org/consumer-resources/how-to-stop-robocalls
Electronic Communications Committee. (2022). *ECC Report 338 CLI Spoofing.* Obtenido de https://docdb.cept.org/download/4027
Electronic Communications Committee. (2022). *ECC Report 338 CLI Spoofing.* Obtenido de https://docdb.cept.org/download/4027
Electronic Communications Committee. (2022). *ECC Report 338 CLI Spoofing.* Obtenido de https://docdb.cept.org/download/4027
FCC. (2003). *FCC 03-153.* Obtenido de https://docs.fcc.gov/public/attachments/FCC-03-153A1.pdf
FCC. (2018). *FCC Actions on Robocalls, Telemarketing*. Obtenido de https://www.fcc.gov/general/telemarketing-and-robocalls
FCC. (2020). *Call Authentication Trust Anchor Report and Order and Further Notice of Proposed Rulemaking.* Obtenido de https://docs.fcc.gov/public/attachments/FCC-20-42A1.pdf
FCC. (2020). *Call Authentication Trust Anchor Second Report and Order.* Obtenido de https://docs.fcc.gov/public/attachments/FCC-20-136A1.pdf
FCC. (2020). *Wireline Competition Bureau Caller ID Authentication Best Practices.* Obtenido de https://docs.fcc.gov/public/attachments/DA-20-1526A1.pdf
FCC. (2021). *Call Authentication Trust Anchor Third Report and Order.* Obtenido de https://docs.fcc.gov/public/attachments/FCC-21-93A1.pdf
FCC. (2021). *Call Blocking Tools Available to Consumers: Second Report on Call Blocking.* Obtenido de https://docs.fcc.gov/public/attachments/DA-21-772A1.pdf
FCC. (2022). *Advanced Methods to Target and Eliminate Unlawful Robocalls.* Obtenido de https://docs.fcc.gov/public/attachments/FCC-22-37A1.pdf
FTC. (2023). *Complying with the Telemarketing Sales Rule*. Obtenido de https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#Introduction
Hiya. (2023). *Informe Hiya sobre la amenaza mundial de las llamadas Q3 2023.* Obtenido de https://es.hiya.com/global-call-threat-report
i3 Forum. (2019). *OBC and A-Number validation.* Obtenido de https://i3forum.org/wp-content/uploads/2019/07/5-i3forum-AC-2019-OBC-and-A-Number-validation-def.pdf
i3 Forum. (2020). *Calling Line Identification (CLI) spoofing.* Obtenido de https://i3forum.org/public_html/wp-content/uploads/2020/11/i3f-Technical-Report-CLI-spoofing-Technical-Report-final.pdf
i3 Forum. (2020). *Calling Line Identification (CLI) spoofing.* Obtenido de https://i3forum.org/public_html/wp-content/uploads/2020/11/i3f-Technical-

Report-CLI-spoofing-Technical-Report-final.pdf
ICO. (2018). *Guide to the Privacy and Electronic Communications Regulations.* Obtenido de https://ico.org.uk/media/for-organisations/guide-to-pecr-2-4.pdf
ICO Ofcom. (2021). *Nuisance calls and messages Update to ICO/Ofcom joint plan.* Obtenido de https://www.ofcom.org.uk/__data/assets/pdf_file/0025/216439/nuisance-calls-joint-action-plan-2021.pdf
ICO Ofcom. (s.f.). *Tackling Nuisance Calls and Messages.* Obtenido de https://www.ofcom.org.uk/__data/assets/pdf_file/0033/49569/ico_ofcom_letter_200313.pdf
IFT. (2022). *Segunda Encuesta 2022 Usuarios de Servicios de Telecomunicaciones.* Obtenido de https://www.ift.org.mx/sites/default/files/contenidogeneral/usuarios-y-audiencias/segundaencuesta2022vf.pdf
INEGI. (2022). *Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública.* Obtenido de https://www.inegi.org.mx/contenidos/programas/envipe/2022/doc/envipe2022_presentacion_nacional.pdf
ITU. (2019). *FG DLT D2.1.* Obtenido de https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d21.pdf
ITU. (2019). *FG DLT D2.1 Digital Identity as a Service.* Obtenido de https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d21.zip
ITW GLF. (2023). *GLF Fraud Report and Code of Conduct Attestation 2023.* Obtenido de https://content.comms.euromoneyplc.com/GLF-activities_GLF-Fraud-Report-2023.html
OEA. (2019). *Estado de la Ciberseguridad en el Sistema Financiero Mexicano.* Obtenido de http://www.oas.org/es/sms/cicte/documents/informes/Estado-de-la-Ciberseguridad-en-el-Sistema-Financiero-Mexicano.pdf
Ofcom. (2010). *Tackling abandoned and silent calls Statement.* Obtenido de https://www.ofcom.org.uk/__data/assets/pdf_file/0025/46690/Tackling-abandoned-and-silent-calls-Statement.pdf
Ofcom. (2022). *Guidance on the provision of Calling Line Identification facilities and other related services.* Obtenido de https://www.ofcom.org.uk/__data/assets/pdf_file/0021/247503/CLI-guidance-annex.pdf
Ofcom. (2022). *Improving the accuracy of Calling Line Identification (CLI) data.* Obtenido de https://www.ofcom.org.uk/__data/assets/pdf_file/0031/247486/statement-improving-accuracy-CLI-data.pdf
PROFECO. (2023). *Informes de actividades.* Obtenido de https://www.gob.mx/profeco/documentos/informes-de-actividades-29444?state=published
SAMSUNG. (2023). *Smart Call.* Obtenido de https://www.samsung.com/mx/apps/smart-call/
T-Mobile. (2023). *Scam Shield APP.* Obtenido de https://es.t-mobile.com/benefits/scam-

shield-app
TRAI. (2018). *THE TELECOM COMMERCIAL COMMUNICATIONS CUSTOMER PREFERENCE REGULATIONS,.* Obtenido de https://trai.gov.in/sites/default/files/RegulationUcc19072018.pdf
TRAI. (2018). *TRAI issues Direction regarding implementation of Digital Consent Acquisition under TCCCPR, 2018.* Obtenido de https://www.trai.gov.in/notifications/press-release/trai-issues-direction-regarding-implementation-digital-consent
TRAI. (2022). *CurbingUCCthrough effective implementation of Telecom Commercial.* Obtenido de https://trai.gov.in/sites/default/files/PR_No.75of2022.pdf
Truecaller. (2022). *How Truecaller's Caller ID Works – Your Questions Answered.* Obtenido de https://www.truecaller.com/blog/features/how-truecallers-caller-id-works-your-questions-answered
TRUECALLER. (2023). *Bloqueo de Spam.* Obtenido de https://www.truecaller.com/es-la/spam-blocking
UIT. (2007). *Suplemento 1 de la Recomendación E.156.* Obtenido de https://www.itu.int/rec/T-REC-E.156/recommendation.asp?lang=es&parent=T-REC-E.156-200711-I!Sup1
UIT. (2008). *Recomendación X.1244.* Obtenido de https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1244-200809-I!!PDF-S&type=items
UIT. (2011). *Suplemento 2 de la Recomendación E.156.* Obtenido de https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-E.156-201106-I!Sup2!PDF-S&type=items
UIT. (2015). *Recomendación X.1246.* Obtenido de https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1246-201509-I!!PDF-S&type=items
UIT. (2019). *FG DLT D1.1.* Obtenido de https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf
UIT. (2019). *FG DLT D1.2.* Obtenido de https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d12.pdf
UIT. (2019). *FG DLT D2.1.* Obtenido de https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d21.pdf
UIT. (2020). *Recomendación M.3362.* Obtenido de https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-M.3362-202006-I!!PDF-E&type=items
UIT. (2021). *TR.spoofing Countering Spoofing.* Obtenido de https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-TRUST-2021-PDF-E.pdf
uscellular. (2023). *SILENCE THE SPAM CALLS WITH CALL GUARDIAN.* Obtenido de https://www.uscellular.com/support/help/fraud-prevention
Verizon. (2023). *Answer with confidence.* Obtenido de https://www.verizon.com/solutions-and-services/call-filter/

INSTITUTO FEDERAL DE
TELECOMUNICACIONES

Instituto Federal de Telecomunicaciones
Insurgentes Sur 1143, Col. Nochebuena,
Demarcación Territorial Benito Juárez, C.P. 03720
Ciudad de México, Tel: 55 5015 4000 / 800 2000 120

www.ift.org.mx