Diseño de un modelo de seguridad orientado a las redes de telefonía IP de Colombia basado en el protocolo STIR/SHAKEN para evitar la suplantación de identidad de números telefónicos por medio de herramientas de simulación.

Gabriel Fernando Anaya Blanco, Ivonne Andrea Duarte Forero

Trabajo de grado para optar el título de Magíster en Gestión y Consultoría en Tecnologías de la Información y la Comunicación

Director

Ricardo Andrés Medina Puentes

Magíster en Redes y Sistemas de Comunicación

Universidad Santo Tomás, Bucaramanga

División de Ingenierías y Arquitectura

Maestría en Gestión y Consultoría TIC

2023

Dedicatoria

A Dios, hacedor de todo lo que existe.

A nuestras familias, que son apoyo, fortaleza y nuestro motor.

Agradecimientos

A nuestro director de trabajo final de Maestría, Ingeniero Ricardo Medina, por su invaluable orientación y apoyo. Su dedicación y experiencia han sido pilares fundamentales para el desarrollo exitoso de este proyecto.

A nuestros compañeros y colegas, fue una experiencia enriquecedora y motivadora compartir este camino con ustedes.

Contenido

Lista de figuras

Lista de tablas

Lista de apéndices

Resumen

Este trabajo de grado plantea el diseño de un modelo de seguridad basado en el protocolo STIR/SHAKEN, orientado a evitar la suplantación de identidad de números telefónicos en las redes de telefonía IP en Colombia. A través de una estructura metodológica de cuatro fases principales, se realiza un análisis del panorama global actual relacionado con la implementación del protocolo STIR/SHAKEN, se identifican los modelos de seguridad actualmente implementados en las redes de telefonía IP específicamente en el contexto colombiano para adaptar el modelo propuesto a las condiciones y desafíos particulares del país y se realiza la validación del funcionamiento del protocolo en un entorno de simulación controlado, permitiendo evaluar su rendimiento. Por último, se presenta el análisis de los resultados obtenidos, con base en estos se genera una guía que para la implementación del protocolo STIR/SHAKEN en las redes de telefonía IP en Colombia. Las contribuciones fundamentales de este trabajo de grado incluyen proporcionar un mejor entendimiento de los requisitos específicos para la implementación del protocolo STIR/SHAKEN en el contexto colombiano. Al abordar la falta de regulación específica y la ausencia de mecanismos de seguridad robustos, este proyecto aspira a impulsar la protección contra la suplantación de identidad telefónica en las redes de telefonía IP en Colombia.

Palabras clave: Ciberseguridad, STIR/SHAKEN, Voz IP

Abstract

This thesis proposes the design of a security model based on the STIR/SHAKEN protocol, aimed at preventing the identity spoofing of telephone numbers in IP telephony networks in Colombia. Through a methodological framework consisting of four main phases, an analysis of the current global landscape related to the implementation of the STIR/SHAKEN protocol is conducted. The security models currently implemented in IP telephony networks, specifically within the Colombian context, are identified to tailor the proposed model to the country's specific conditions and challenges. The protocol's functionality is then validated in a controlled simulation environment, allowing for a comprehensive performance evaluation. Finally, an analysis of the obtained results is presented, based on which a guide for the implementation of the STIR/SHAKEN protocol in Colombian IP telephony networks is generated. The primary contributions of this thesis include providing a better understanding of the specific requirements for implementing the STIR/SHAKEN protocol in the Colombian context. By addressing the lack of specific regulations and the absence of robust security mechanisms, this project aims to enhance protection against telephone number identity spoofing in Colombian VOIP networks.

Keywords: Cybersecurity, STIR/SHAKEN, VoIP

Introducción

La expansión global de los ciberataques ha ocasionado un aumento tanto en su frecuencia como en la magnitud del impacto generado. Dentro de las distintas modalidades y técnicas de engaño, la suplantación de identidad de números telefónicos emerge como una técnica cibernética avanzada, denominada "Call ID spoofing". Esta técnica permite a los ciberdelincuentes falsificar identificadores de llamadas, engañando a los receptores con el propósito de hacerse pasar por personas conocidas, entidades gubernamentales o empresas de confianza, sin la posibilidad de que el usuario pueda verificar la autenticidad del número asociado al remitente de la llamada.

La creciente necesidad de abordar la problemática de la suplantación de identidad telefónica ha motivado la adopción de estrategias eficaces para fortalecer la seguridad en las redes de telefonía IP. A nivel internacional, la implementación exitosa del protocolo STIR/SHAKEN ha demostrado ser eficaz en la autenticación y verificación de identidad, proporcionando un marco sólido para combatir la suplantación de identidad por medio de llamadas telefónicas a través de las redes de telefonía IP.

El propósito fundamental de este proyecto es diseñar un modelo de seguridad adaptado a las redes de telefonía IP en Colombia, basado en el protocolo STIR/SHAKEN. Este modelo busca no solo mitigar la suplantación de identidad, sino también contribuir al cuerpo de conocimiento en seguridad de la información, adoptando un enfoque metodológico integral, que incluye un escenario de simulación.

Este trabajo de grado se sitúa en el contexto de la Maestría en Gestión y Consultoría TIC y se fundamenta en la necesidad existente de fortalecer la seguridad en las comunicaciones telefónicas en Colombia. La falta de normativas específicas y la ausencia de mecanismos de seguridad robustos por parte de los operadores de telefonía han permitido que la suplantación de identidad avance, afectando negativamente tanto a ciudadanos como a empresas. Este proyecto se posiciona como un facilitador fundamental para potenciar la implementación de mecanismos de seguridad altamente eficaces. Su impacto se extiende hacia la consolidación de la confianza en las comunicaciones telefónicas, desempeñando un papel crucial en la promoción de prácticas seguras en las infraestructuras de telefonía IP a nivel nacional.

1. Diseño de un modelo de seguridad orientado a las redes de telefonía IP de Colombia basado en el protocolo STIR/SHAKEN para evitar la suplantación de identidad de números telefónicos por medio de herramientas de simulación.

1.1 Planteamiento del problema

Durante los últimos 5 años se ha visto un aumento a nivel mundial de los ciberataques, tanto en la cantidad como en la repercusión de estos, el Centro Criptológico Nacional de España CCN–CERT en el resumen ejecutivo de Ciber Amenazas y Tendencias en su edición 2021 (CCN-CERT, 2021), señala que el año 2020 pasará a la historia como el año en el que hubo más incidentes de seguridad digital dado que los ciberdelincuentes cada vez perfeccionan sus técnicas y establecen vectores de ataque más sofisticados. Según el informe “Perspectivas de Ciberseguridad 2023” entregado por LATAM CISCO, señala que los ciberataques a nivel mundial han tenido un incremento exponencial y Latinoamérica es una de las regiones que recibe la mayor cantidad de ataques cibernéticos en el mundo. Se destaca que dentro de los ataques más comunes que afectan hoy en día a las empresas y a los ciudadanos del común se encuentran el secuestro de datos (Rasomware), denegación de servicio (DoS) y la suplantación de identidad (CISCO, 2023), como es el caso de la suplantación de identidad de números telefónicos denominada como "Caller ID spoofing", esta técnica tiene la capacidad de falsificar un identificador de llamada haciendo la suplantación por el de una persona conocida, un ente del gobierno o una empresa de la cual se es cliente, sin que el usuario receptor de la llamada pueda probar la legitimidad del número que le llama.

En países como Estados Unidos a través de la Comisión Federal de Comunicaciones (FCC) definieron un conjunto de reglas para que los proveedores de telefonía implementaran a partir del 30 de junio del 2021 en sus redes IP, protocolos de autenticación de identificación de llamadas para proteger a sus clientes de llamadas automáticas ilegales y de esta manera recuperar la confianza de los Estadounidenses en las llamadas telefónicas, luego esta medida se extendió a países como Canadá donde a través del Comité Canadiense de Radio, Televisión y Telecomunicaciones (CRTC) ordenó a los operadores de telefonía para ofrecer y proveer servicios de telecomunicaciones implementar en sus redes IP un protocolo para autenticar y verificar la identidad de la persona que llama (Commission, Compliance and Enforcement and Telecom Decision, 2021).

Sin embargo, en países como Colombia, actualmente no existe una normativa por parte del ente regulador de Telecomunicaciones, Comisión de Regulación de Comunicaciones (CRC) que estandarice las políticas de seguridad de la telefonía, lo que conlleva a que los operadores del país no implementen protocolos de cifrado para la autenticación de identificador, que permitan mitigar la suplantación de identidad de llamadas que cursan a través de la red de telefonía IP.

La ausencia de implementación por parte de los operadores de mecanismos técnicos de seguridad para contrarrestar este tipo de amenazas es un factor que contribuye a que se incrementen los delitos de estafa a través de esta modalidad la cual afecta tanto a los ciudadanos como a las mismas empresas y busca a través del engaño sustraer información personal y financiera. Teniendo en cuenta lo anterior es fundamental que los operadores de telefonía en Colombia adopten

mecanismos de seguridad robustos y eficaces que permitan establecer servicios de autenticación y con esto lograr que los delitos ejecutados a través de este medio se reduzcan considerablemente.

Pregunta de investigación

¿Cómo se puede evitar la suplantación de identidad de llamadas a través de un modelo de seguridad basado en el protocolo STIR/SHAKEN?

1.2 Justificación

En el escenario actual de las comunicaciones telefónicas existe una necesidad latente de abordar el creciente problema de seguridad, específicamente la suplantación de identidad de números telefónicos conocida como "Call ID spoofing", esta táctica perpetrada por ciberdelincuentes implica la manipulación fraudulenta del identificador de llamada para presentarse como personas o entidades legítimas, lo que conlleva a un aumento en los delitos de estafa y violación de la privacidad. La ausencia de implementación por parte de los operadores de telefonía de mecanismos técnicos de seguridad para contrarrestar este tipo de amenazas es un factor que contribuye a que se incrementen los delitos de estafa a través de esta modalidad la cual afecta tanto a los ciudadanos como a las mismas empresas con consecuencias que van más allá de la pérdida financiera, alcanzando la sustracción de información personal y financiera mediante engaños. Teniendo en cuenta lo anterior es fundamental que los operadores de telefonía del país adopten mecanismos de seguridad robustos y eficaces que permitan establecer servicios de autenticación y con esto lograr que los delitos ejecutados a través de este medio se reduzcan considerablemente.

La brecha regulatoria que existe entre naciones como Estados Unidos y Canadá, que han adoptado medidas proactivas basadas en el protocolo STIR/SHAKEN para autenticar y verificar identidades en llamadas telefónicas, y países como Colombia, donde la ausencia de una normativa específica en el tema ha dejado a los operadores de telefonía sin directrices claras, ha creado un vacío significativo en la protección de los usuarios. La falta de regulación específica y de implementación generalizada de mecanismos de seguridad por parte de los proveedores de telefonía IP expone a los ciudadanos colombianos a riesgos como fraudes y robos de identidad.

En este contexto, se presenta una oportunidad desde la línea profesional de la Maestría en Gestión y Consultoría TIC para abordar estas vulnerabilidades y contribuir a la generación de conocimiento y la promoción de buenas prácticas de seguridad en las redes de telefonía IP en el país, a través del diseño de un modelo de seguridad basado en el protocolo STIR/SHAKEN adaptado a las redes de telefonía IP de Colombia que permita autenticar y verificar la identidad de los números telefónicos, evitando así la suplantación de identidad y brindando mayor confianza y seguridad a los usuarios. Este trabajo de grado no solo se presenta como una respuesta a una necesidad imperativa de implementación de medidas de seguridad, sino también como una iniciativa proactiva que promueve un entorno más seguro y confiable en las comunicaciones a través de telefonía IP en Colombia.

1.3 Objetivos

1.3.1 Objetivo general

Diseñar un modelo de seguridad orientado a las redes de telefonía IP de Colombia basado en el protocolo STIR/SHAKEN para evitar la suplantación de identidad de números telefónicos por medio de herramientas de simulación.

1.3.2 Objetivos específicos

Caracterizar la estructura del protocolo STIR/SHAKEN a través de la revisión de literatura e implementaciones realizadas a nivel internacional a fin de establecer un marco de referencia.

Determinar el estado actual de modelos de seguridad en las redes de telefonía IP en Colombia para evitar la suplantación de identidad y fraude a través de la revisión de la regulación existente.

Evaluar el modelo del protocolo STIR/SHAKEN aplicado a redes de telefonía IP por medio de la utilización de software libre a fin de determinar la efectividad del protocolo.

Elaborar una guía de ruta para la implementación del modelo de seguridad STIR/SHAKEN sobre redes de telefonía IP que sirva como referencia para el ente regulador en Colombia.

2. Marco Referencial

2.1 Marco conceptual

IP: (RFC 791) (1981) *"The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks."* (Agency, September 1981)

VOIP: definido como Voz sobre Protocolo de Internet, se basa en un estándar IP que es capaz de transportar paquetes de voz y datos a través de la misma red. Las señales de voz se convierten en

paquetes que se envían a través de la red y se reensamblan en el orden correcto cuando llegan a su destino (Gartner, s.f.).

SIP: (RFC 3261) (2022) *"Session Initiation Protocol is an application-layer control protocol that can establish, modify and terminate multimedia sessions (conferences) such as Internet telephony calls."* (J. Rosenberg dynamicsoft, H. Schulzrinne Columbia U, G. Camarillo Ericsson, A. Johnston WorldCom, J. Peterson Neustar, R. Sparks dynamicsoft, M. Handley ICIR, E. Schooler AT&T, June 2022).

CALLER ID SPOOFING: *Suplantación del identificador de llamadas*. La suplantación del identificador de llamadas se define como el acto de alterar el identificador de llamadas que se muestra a la persona que recibe la llamada (Commission, https://crtc.gc.ca, s.f.).

STIR: *Secure Telephony Identity Revisited*. STIR es el nombre de un grupo de trabajo de estandarización y se usa comúnmente para etiquetar la tecnología que agrega firmas criptográficas a las solicitudes de señalización de llamadas. Esta tecnología evita que una persona que llama proporcione un número de llamada a la parte receptora que no está autorizada a utilizar.

SHAKEN: *Signature-based Handling of Asserted information using toKENs*. SHAKEN es un estándar de la industria que define cómo los proveedores de servicios de voz deben implementar la tecnología STIR para garantizar que los números de las partes que llaman no sean falsificados ilegalmente.

STIR/SHAKEN: Describe el conjunto de estándares técnicos y procedimientos operativos para implementar la autenticación de llamadas transportadas a través de una red IP (Filip ŘEZÁČ, January 2010).

2.2 Marco Teórico

La voz sobre protocolo de internet (VoIP) se ha convertido en una alternativa universal a las redes de telefonía pública conmutada (PSTN), ha revolucionado la industria de las comunicaciones al proporcionar una alternativa más flexible, económica y versátil y ha proporcionado ventajas como bajos costos, flexibilidad y características avanzadas. En lugar de utilizar redes telefónicas tradicionales basadas en circuitos, la VoIP utiliza paquetes de datos para transmitir la voz a través del protocolo IP e integra múltiples servicios en un modelo convergente mediante internet, VoIP utiliza el RTP (Real Time Transport Protocol) que define un formato de paquete estándar para entregar media sobre internet y SIP (Session Initiation Protocol), protocolo de señalización utilizado para establecer, mantener y finalizar una sesión entre dos o más participantes.

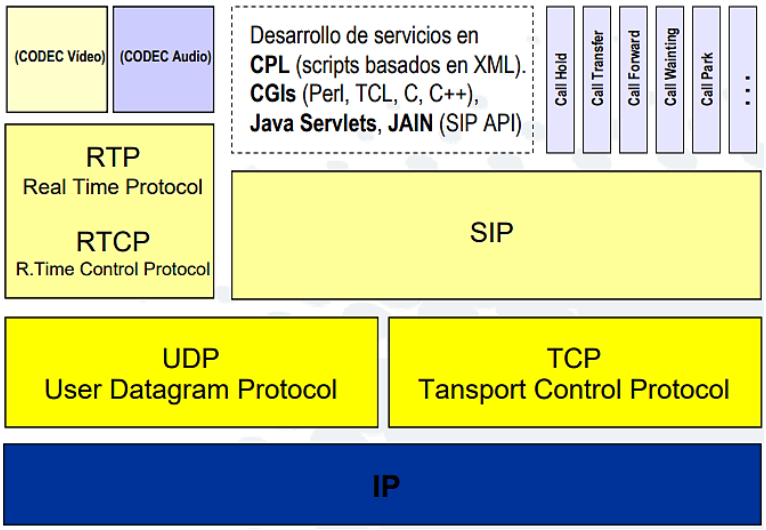
Sin embargo, la popularidad de la telefonía IP o Voz sobre IP (VoIP) también ha traído consigo riesgos de seguridad de la información, estos pueden incluir interceptación, modificación o incluso pérdida de datos durante el transporte (Filip ŘEZÁČ, January 2010). Los piratas informáticos han explotado técnicas como la suplantación de identificación de llamadas, utilizando el inicio de sesión (SIP) un atacante puede generar automáticamente llamadas con identificadores falsos (D. Butcher, 2007).

2.2.1 Protocolo SIP

El protocolo de inicio de sesión fue desarrollado por la IETF y especificado en la RFC 3261 en 2002, SIP trabaja en la creación, modificación, y finalización de sesiones que incluyen llamadas telefónicas de internet las cuales son transportadas dentro de los protocolos RTP/RTCP

(Real Time Transport Protocol) y SDP (Session Description Protocol) con uno o varios participantes (Handeley, Shulzrinne, & Schooler, 1999), como se describe en la figura 1.

Figura 1. *Pila de Protocolo de Inicio de Sesión*

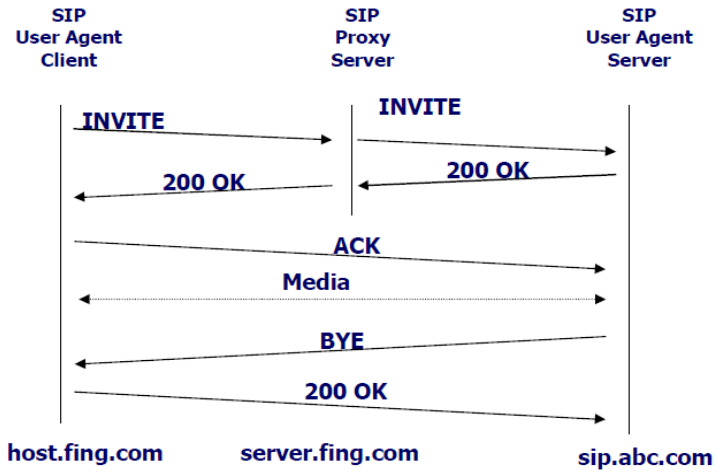


Adaptado de Arquitecturas Telefonía IP [12].

SIP está basado en un modelo cliente-servidor, los clientes SIP envían peticiones (Request Messages) a un servidor, una vez procesada el servidor contesta con una respuesta (Response Messages) como se muestra en la figura 2. Los terminales SIP pueden generar tanto peticiones como respuestas al estar formados por el denominado cliente del agente de usuario (User Agent Client- UAC) y servidor del agente de usuario (User Agent Server - UAS). Funcionan como UAC cuando generan una petición y funcionan como UAS cuando la reciben (Mendez & Valdez, 2013).

Los mensajes SIP comparten una directiva de servicio muy similar a la de las peticiones y respuestas HTTP y se intercambian entre los dispositivos y servidores SIP.

Figura 2. *Funcionamiento mensajes protocolo SIP*



Adaptado de (Johnston, 2004)

Los mensajes SIP están conformados por una estructura básica que incluye encabezados y cuerpo.

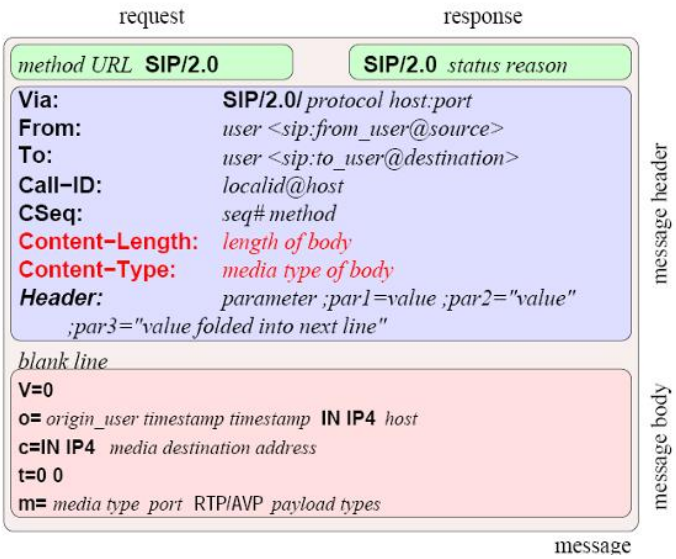
URI (Uniform Resource Identifier): es la primera línea del mensaje y contiene el método o la respuesta del mensaje, INVITE, REGISTER, ACK, CANCEL, BYE Y OPTIONS.

Encabezados (Header): el encabezado contiene la siguiente información adicional sobre la solicitud o respuesta:

- From: identifica quién envía el mensaje SIP, incluye el nombre y dirección SIP.
- To: identifica quién es el destinatario del mensaje SIP, incluye el nombre y dirección SIP.
- Vía: indica las rutas que el mensaje ha seguido a través de diferentes servidores proxy.
- Call-ID: identifica una llamada específica y se utiliza para correlacionar los mensajes SIP relacionados con esa llamada.
- Content-Type: define el tipo de contenido que se encuentra en el cuerpo del mensaje, como texto, audio, video, etc.
- Content-Length: indica la longitud del cuerpo del mensaje en bytes.

Cuerpo (body): es la parte del mensaje SIP que contiene información adicional asociada con la solicitud o respuesta (Benedini, 2013).

Figura 3. *Estructura Protocolo de Inicio de Sesión (SIP)*



Adaptado de (Terzoli, 2014)

La identidad de llamada es importante para garantizar la autenticidad y la integridad de la comunicación. La identificación del llamante "Call-ID" o "Caller Identification" se refiere a la información que se muestra en el teléfono receptor para identificar al llamante. Esta información generalmente incluye el número telefónico o el nombre asociado con la llamada entrante. La suplantación de Caller ID, también conocida como "Caller ID spoofing" o "suplantación de identidad de llamadas", es una técnica utilizada por los atacantes para falsificar la información de identificación del llamante. Esto les permite ocultar o cambiar el número telefónico del que proviene la llamada, haciendo que parezca que la llamada proviene de un número diferente al real (Kevin Daimi, 2021). Para combatir estos problemas, se ha desarrollado el marco de autenticación de llamadas STIR/SHAKEN.

2.2.2 STIR/SHAKEN

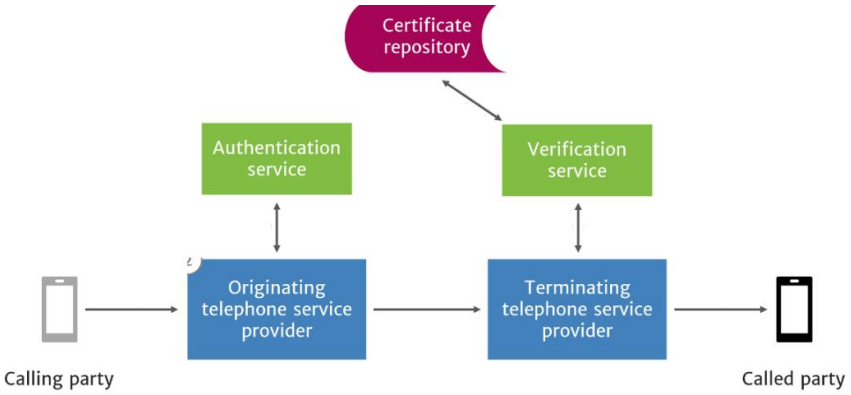
La IETF (Internet Engineering Task Force) desarrolló el marco de estándares interconectados denominado STIR/SHAKEN, acrónimo de los estándares “Secure Telephone Identity Revisited” (STIR) y “Signature-based Handling of Asserted Information Using Tokens” (SHAKEN), estos dos estándares trabajan en conjunto para autenticar las llamadas telefónicas y proporcionar información verificada sobre la identidad del llamante (Ustelecom, 2019).

STIR/SHAKEN permite la validación digital de las llamadas telefónicas a medida que atraviesan diferentes operadores en las redes telefónicas interconectadas. Los operadores de origen firman digitalmente el identificador de llamadas para certificar su legitimidad, y los operadores receptores validan esta firma antes de entregar la llamada a los consumidores. De esta manera, el protocolo garantiza que la compañía telefónica del consumidor pueda verificar que la llamada proviene del número que se muestra en el identificador de llamadas, brindando mayor confianza en la autenticidad de las llamadas entrantes (Commision).

2.2.2.1 Marco STIR/SHAKEN. El marco STIR/SHAKEN está compuesto por dos mecanismos que trabajan de forma articulada. El proceso de gobernanza de certificados que mantiene la confianza en la información de autenticación del identificador transmitida junto con una llamada y el componente técnico relacionado con la autenticación y verificación de la información del identificador de llamadas basado en criptografía de la llave pública, la cual permite asegurar la información transmitida y que será de conocimiento por parte del proveedor de autenticación sobre el usuario que realiza la llamada y su relación con el número telefónico utilizado, con el fin de que el proveedor de servicios de voz verifique la información, como se muestra en la figura 4. La información que es transmitida viaja de forma cifrada y se encuentra

inmersa en un tramo del mensaje SIP conocido como “campo de encabezado de identidad”, esta información es recibida y descifrada por el proveedor de servicios de terminación, quien a su vez valida la información de identificación del usuario que realiza la llamada y posteriormente utiliza esta información para proteger a sus usuarios de llamadas falsificadas o no deseadas (TransNexus, transnexus.com).

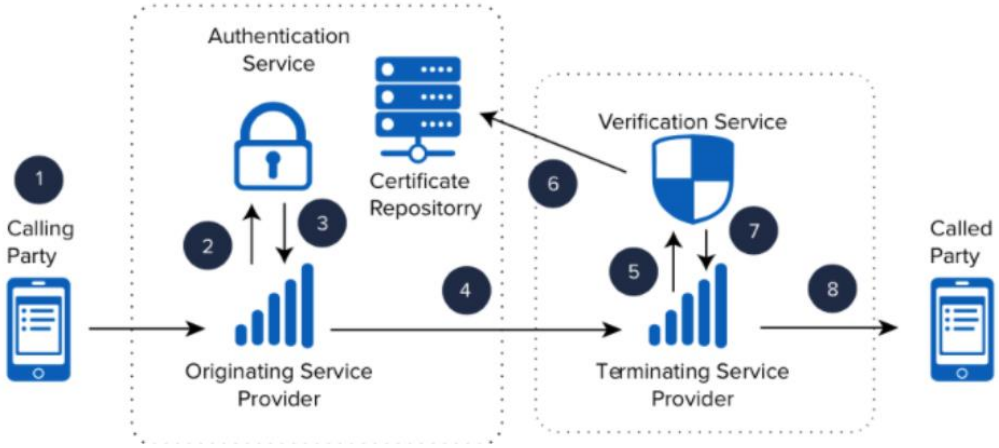
Figura 4. *Flujo de trabajo de STIR/SHAKEN*



Adaptado de (TransNexus, transnexus.com)

2.2.2.2 Funcionamiento STIR/SHAKEN. En la figura 5, se detalla el funcionamiento del protocolo STIR/SHAKEN, representando gráficamente el proceso de llamada inicial y la generación de la firma. Este esquema ilustra de manera clara y secuencial cómo se lleva a cabo la autenticación durante la llamada, desde la generación de la firma en el origen hasta el momento en que la llamada es entregada al receptor. Este proceso, destaca la integridad del protocolo STIR/SHAKEN al proporcionar una capa de seguridad que aborda la autenticación a lo largo de la cadena de transmisión, asegurando una comunicación telefónica confiable y auténtica desde su origen hasta su destino final (Edwards Gregory, 2020).

Figura 5. *Funcionamiento de STIR/SHAKEN*

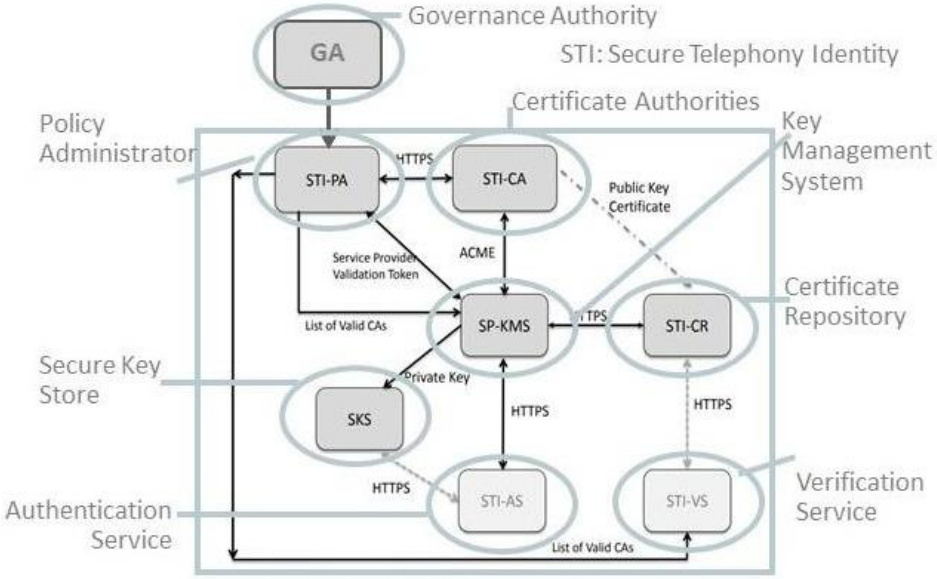


Adaptado de (Livevox, s.f.)

1. El proveedor de servicios telefónicos de origen recibe SIP INVITE
2. El proveedor origen verifica la fuente de la llamada y el número que llama para determinar la validez como dar fe de la validez del número que llama.
3. El proveedor de origen utiliza el servicio de autenticación para crear un encabezado de identidad SIP que contiene los siguientes datos (número que llama, número llamado, fecha y hora, nivel de atestación, identificador de origen).
4. El SIP INVITE con el encabezado SIP Identity se envía al proveedor de servicios telefónicos de destino.
5. El SIP INVITE con el encabezado Identity es enviado al servicio de verificación.
6. El servicio de verificación obtiene el certificado digital del proveedor de origen del repositorio público de certificados y comienza un proceso de verificación.
7. El servicio de verificación devuelve los resultados al proveedor del servicio de terminación.
8. La llamada se completa en la parte llamada.

2.2.2.3 Componentes de STIR/SHAKEN. El protocolo STIR/SHAKEN se compone de elementos fundamentales para su implementación los cuales se detallan en la figura 6.

Figura 6. *Componentes de STIR/SHAKEN*



Adaptado de Componentes de STIR/SHAKEN (Tejedor, 2020)

GA (Governance Authority Policies) Es el encargado de identificar las autoridades de certificación y a su vez de establecer quien será el encargado de formar digitalmente las llamadas.

STI-PA (Secure Telephony Identity - Policy Administrator) Su principal función es la de administrar las políticas establecidas por el GA y adicionalmente entrega los “token” al KMS “Proveedor de Servicios Servidor de Gestión de Claves” con el propósito de adquirir el certificado digital utilizado para la firma de las llamadas.

STI-CA (Secure Telephony Identity - Certificate Authority) Las autoridades de certificación son las encargadas de elaborar la infraestructura digital para establecer la firma de las

llamadas, de igual manera estas autoridades de certificación deberán ser aprobadas por el Administrador de Políticas (PA).

SP-KMS (Service Provider - Key Management Server) Su función principal es la de establecer la clave pública y privada para la generación de la firma digital y obtener los certificados STI de las Autoridades de Certificación STI-CA.

SKS (Secure Key Store) Este componente funciona como un repositorio de certificados, es el encargado de acoger y almacenar la clave privada generada por el SP-KMS.

STI-AS (Secure Telephony Identity - Authentication Service) Ejerce como un servicio de autenticación, su función principal es la de obtener la clave privada generada por el repositorio de certificados SKS, seguidamente efectúa la firma de certificación y posteriormente produce el token en la cabecera del mensaje SIP.

STI-CR (Secure Telephony Identity - Certificate Repository) Se encarga de guardar los certificados de la clave pública empleados por el servicio de verificación STI-VS con el fin de verificar las firmas obtenidas en las llamadas provenientes de otras operadoras.

STI-VS (Secure Telephony Identity - Verification Service) Este componente funciona como un servicio de verificación el cual se encarga de obtener del “token” desde la cabecera utilizando la URL adjunta en el mensaje SIP con el propósito de conseguir el certificado de clave pública que proporciona el STI-CR, para posteriormente deshacer el “token” y verificarlo.

SPR (Suscriber Profile Repository) Este componente no hace parte integral del protocolo Stir/Shaken pero es recomendable implementarlo en la solución ya que establece la base de datos para el proceso de las llamadas, el libro de contabilidad que contiene información de las llamadas certificadas, la preferencia visuales y de idioma, los números no deseados, entre otros aspectos (Tejedor, 2020).

2.2.3 Gestión de certificados digitales.

Dentro de la infraestructura de generación de claves públicas y privadas con base en el protocolo STIR/SHAKEN, los proveedores de servicios de telefonía IP gestionan las claves por medio de un servicio de gestión de certificados (CMS) que debe ser efectuado por los operadores de servicios de telefonía. Dentro del proceso de generación de certificados es necesario que los proveedores de servicios se encuentren autorizados por el Administrador de Políticas (PA), quien es el responsable de mantener la integridad de los certificados digitales ya que evalúan y autorizan a las entidades que quieran crear o emitir certificados. Este procedimiento impide que quienes no estén autorizados para firmar llamadas adquieran un certificado y evita que las autoridades certificadoras entreguen certificados incorrectos.

Dentro de este proceso el proveedor de telefonía emplea la clave privada con el propósito exclusivo de firmar las llamadas, posteriormente otro proveedor de servicios podría utilizar una clave pública para comprobar el propietario legítimo de la firma y así poder confirmar que esta firma fue establecida por dicha clave privada.

El administrador de Políticas (PA) ejerce como entidad de confianza dentro del proceso de STIR/SHAKEN. Para que un proveedor de servicios pueda ser aprobado, el Administrador de Políticas (PA) le debe generar un token con el Identificador de Proveedor de Servicios (SPID), una vez obtenido este token, el proveedor de servicios se encuentra autorizado para pedir los certificados. Con el fin de prevenir el uso no autorizado de la clave privada, el servicio de gestión de certificados (CMS) la cifra y la sitúa en un repositorio de certificados SKS (Secure Key Store), a su vez el CMS remite la clave pública a la entidad certificadora de confianza y esta devuelve el certificado firmado donde además de contener la clave incluye información de su propietario,

como se muestra en la figura 7. Posteriormente el CMS (servicio de gestión de certificados) almacena el certificado en el repositorio público del proveedor de servicios.

Figura 7. *Gestión de certificados digitales STIR/SHAKEN*

Adaptado de (Alliance for Telecommunications Industry Solutions, 2021)

El proveedor de servicios genera una solicitud de firma de certificado (CSR) y junto al token lo remite a la autoridad certificadora con el fin de adquirir el certificado, posteriormente la entidad de certificación deberá aprobar dicha solicitud y a su vez deberá crear y firmar el certificado para luego entregárselo al proveedor de servicios. El administrador de Políticas (PA) es quien define y custodia la lista de todas las autoridades autorizadas para emitir los certificados de STIR/SHAKEN, la cual deberá estar disponible para todos los proveedores de servicios.

En el transcurso del proceso de validación de STIR/SHAKEN el certificado emitido por el proveedor de servicios de origen debe ser validado previamente por el proveedor de servicios de terminación comprobante que el certificado haya sido generado por una autoridad certificadora autorizada por el administrador de Políticas (PA) (Alliance for Telecommunications Industry Solutions, 2021).

2.2.2.2 Generación de claves públicas y privadas. Las llaves públicas y privadas juegan un papel fundamental dentro de la seguridad utilizada por el protocolo STIR/SHAKEN ya que por medio de estas se verifican y autorizan los identificadores de las llamadas, pero a su vez, es necesario que se creen y administren adecuadamente estas llaves para que STIR/SHAKEN cumpla su objetivo.

El servicio de gestión de certificados (CMS) emplea un conjunto de algoritmos matemáticos para establecer las claves públicas y privadas, aun cuando estas claves están asociadas matemáticamente, los algoritmos se encuentran cuidadosamente elaborados para que la clave privada no se pueda derivar incluso por alguien que conozca la llave pública y los algoritmos matemáticos empleados para generarla (C. Wendt Comcast, J. Peterson Neustar Inc, 2018).

Figura 8. *Ejemplo de llave pública*

```
04:72:47:09:1B:62:3C:9F:A9:21:67:55:82:E9:01:92:3D:43:F5:8E:B3:2B:0E:0F:ED:
C0:C3:98:C4:31:C9:FE:C5:C3:79:4D:1B:F7:7E:7F:8C:B4:CC:46:42:F6:80:6F:BE:1E:
F7:B0:FC:9D:24:BC:4F:48:A1:69:C3:4F:46:D0:59
```

Adaptado de (Jaikaran, 2016)

2.2.4 Verificación en la autenticidad en las llamadas.

Existen tres posibles niveles de verificación de autenticidad dentro del protocolo STIR/SHAKEN con el propósito de identificar al usuario que realiza la llamada.

1. A o Full Attestation. Establece que el proveedor de servicio identifica que el número telefónico se encuentra registrado con el suscriptor de origen.
2. B o Partial Attestation. Señala que la llamada se originó desde un usuario conocido, pero a su vez no se puede comprobar la pertenencia del número del cliente.

3. C o Gateway Attestation. Muestra que se puede identificar que la llamada proviene se origina desde una puerta de enlace conocida, por ejemplo, una conexión a otro proveedor de servicios.

Los receptores de las llamadas verificadas por medio del protocolo STIR/SHAKEN presentarse de forma diferente, teniendo en cuenta el nivel de verificación de cada llamada. Lo anterior depende del dispositivo del destinatario y el proveedor de servicios. A continuación, se detallan tres posibles escenarios sobre la verificación de una llamada:

Las llamadas que cuentan con nivel de verificación (Full Attestation o A) pueden ir acompañadas de un calificador establecido como "Verified" y/o de un calificador visual, como una señal de verificación en el caller ID.

Las llamadas parcialmente verificadas (Partial Attestation o B) podrían ir acompañadas de un calificador "Unknown caller" o "Spam risk" en el caller ID.

Las llamadas que no hayan podido verificarse (Gateway Attestation o C) pueden ir acompañadas de un calificador "Unknown caller" o "Known spam caller" en el caller ID (ATIS).

2.3 Marco legal

El presente trabajo de investigación se enmarca dentro de los siguientes artículos, normativas y documentos de carácter público emitidos por el gobierno nacional de la República de Colombia. Estos instrumentos detallan aspectos normativos que deben considerarse al abordar la seguridad en las redes de telefonía IP.

Tabla 1. *Marco Legal*

Nombre	Descripción
Ley 1341 de 2009	Modificada por la Ley 1978 de 2019. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones
Resolución CRC 5050 de 2016	Por la cual se compilan las Resoluciones de Carácter General vigentes expedidas por la Comisión de Regulación Comunicaciones
Resolución CRC 6522 de 2022	Por la cual se modifican algunas disposiciones referidas al acceso, uso e interconexión de redes de telecomunicaciones contenidas en el Titulo IV de la Resolución CRC 5050 de 2016, y se dictan otras disposiciones.
Decreto 2870 de 2007	Por medio del cual se adoptan medidas para facilitar la Convergencia de los servicios y redes en materia de Telecomunicaciones.
CONPES 3995	Política nacional de confianza y seguridad digital
CONPES 3854	Política nacional de seguridad digital
CONPES 3701	Lineamientos de política para ciberseguridad y ciberdefensa
Modelo de seguridad y privacidad de la información	Define los lineamientos para la implementación de la estrategia de seguridad digital

Elaborada por los autores.

3. Método

Para el desarrollo del presente objeto de estudio y en función de las líneas temáticas sobre las cuales se basa, se adopta un enfoque metodológico híbrido o mixto que combina elementos

cualitativos y cuantitativos para abordar la investigación de manera holística, obtener una comprensión integral del problema de suplantación de identidad en las redes de telefonía IP de Colombia y definir una estrategia efectiva que resuelva la situación problemática planteada. Desde el enfoque cuantitativo, para recopilar y analizar los datos de las simulaciones en entorno controlado y desde el enfoque cualitativo a través de la revisión y análisis de contenido de documentos relevantes, como normativas y políticas relacionadas con la ciberseguridad y la telefonía IP.

Con base en la metodología de investigación propuesto, se presentan a continuación, cuatro fases definidas que se han estructurado para llevar a cabo el cumplimiento de los objetivos definidos en este trabajo, los cuales se sintetizan la tabla 2.

Tabla 2. *Fases Metodológicas*

Nombre	Descripción
Fase 1	Análisis y verificación de la documentación existente a nivel internacional
Fase 2	Dimensionamiento del estado actual de modelos de seguridad en Colombia para redes de telefonía IP
Fase 3	Elaboración de un ambiente simulado
Fase 4	Construcción de la guía de implementación.

Elaborada por los autores.

3.1 Fase 1. Análisis y verificación de la documentación existente a nivel internacional

- *Actividad 3.1.1* Búsqueda de material bibliográfico con el propósito de investigar y analizar artículos y publicaciones académicas en revistas y conferencias especializadas en el campo

de las telecomunicaciones y la seguridad de la información que puedan proporcionar análisis técnicos y casos de estudio sobre el protocolo STIR/SHAKEN.

- *Actividad 3.1.2* Validación de la existencia de actualizaciones o revisiones en los estándares y regulaciones relacionadas con STIR/SHAKEN.
- *Actividad 3.1.3* Clasificación y evaluación la documentación recolectada.

3.2 Fase 2. Dimensionamiento del estado actual de modelos de seguridad en Colombia para redes de telefonía IP

- *Actividad 3.2.1* Validación de los protocolos existentes de seguridad aplicados a telefonía IP en Colombia.
- *Actividad 3.2.2* Análisis y diagnóstico de la regulación actual aplicada a la telefonía IP en Colombia.

3.3 Fase 3. Elaboración de un ambiente simulado

- *Actividad 3.3.1* Elaboración del esquema general del escenario de simulación.
- *Actividad 3.3.2* Configuración de un escenario de simulación para validar la implementación y eficacia del protocolo STIR/SHAKEN a través de un entorno de simulación de software libre y código abierto.
- *Actividad 3.3.3* Ejecución de pruebas de simulación y documentación de los resultados obtenidos con el fin de validar si las firmas digitales se generan adecuadamente y si la información de identificación se transmite correctamente durante la simulación.
- *Actividad 3.3.4* Evaluación de los resultados obtenidos de la simulación con el fin de validar la efectividad del protocolo.

3.4 Fase 4. Construcción de la guía de implementación.

- *Actividad 3.4.1* Validación de los resultados y avances obtenidos durante las fases anteriores.
- *Actividad 3.4.2* Elaboración de un documento guía para la implementación del modelo de seguridad orientado a las redes de telefonía IP basado en el protocolo STIR/SHAKEN que sirva como material de estudio para el ente regulador en Colombia.

4. Resultados

En esta sección, se exponen los resultados obtenidos durante cada fase del desarrollo de la investigación, conforme a la metodología híbrida definida. Se destacan los aportes más significativos que han surgido a lo largo de este proceso que estructuran la integración de los resultados. Estos hallazgos, de manera general, constituyen elementos clave que preparan el terreno para el análisis posterior, proporcionando así una base sólida para la evaluación detallada y la formulación de conclusiones pertinentes.

4.1 Análisis técnico y casos de estudio sobre el protocolo STIR/SHAKEN a nivel internacional.

Con base en el análisis realizado en diversos repositorios de información y fuentes bibliográficas, se ha constatado un progreso notable en la implementación y despliegue del protocolo STIR/SHAKEN a nivel internacional. Este avance se destaca por la colaboración coordinada entre los diferentes actores involucrados, entre los que se incluyen los entes reguladores, los operadores de servicios de telefonía IP y los usuarios en general. Es crucial resaltar el papel pionero desempeñado por países como Estados Unidos y Canadá, quienes se han

posicionado como líderes a nivel mundial en la adopción de estos estándares de seguridad para las redes de voz sobre el protocolo IP.

La adopción y despliegue de STIR/SHAKEN en países como Estados Unidos y Canadá forman parte de una estrategia integral para combatir el fraude telefónico y las molestas llamadas no deseadas. Los proveedores de servicios de telefonía están dedicando esfuerzos significativos para implementar y cumplir con las regulaciones que exigen la integración de STIR/SHAKEN en sus redes. Este enfoque proactivo demuestra el compromiso de la industria en garantizar la integridad y seguridad de las comunicaciones telefónicas, proporcionando a los usuarios una experiencia más confiable y libre de fraudes.

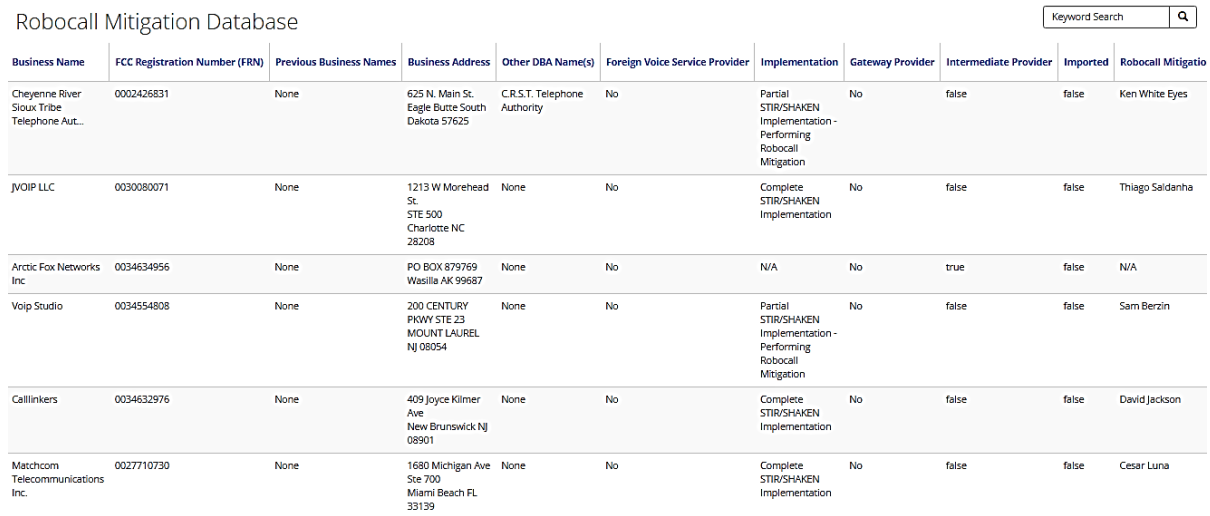
4.1.1 Implementación del protocolo STIR/SHAKEN en Estados Unidos.

Un punto de partida ha sido el Congreso de los Estados Unidos, el cual aprobó el proyecto de ley TRACED “Telephone Robocall Abuse Criminal Enforcement and Deterrence”, que luego se convirtió en ley a fines de 2019, Las normas de la Comisión que implementan la Ley TRACED exigía que los proveedores de servicios de voz implementaran completamente STIR/SHAKEN en sus redes antes del 30 de junio de 2021. La Comisión Federal de Comunicaciones de Estados Unidos (FCC) es el ente regulador a cargo de hacer seguimiento de la ley y ordenó a todas las compañías telefónicas del país implementar la autenticación de identificación de llamadas utilizando el estándar técnico STIR/SHAKEN para proteger a los consumidores de telefonía IP del país contra la suplantación de identidad de identificadores de llamadas que a menudo se usan durante las campañas de estafa de llamadas automáticas (Communications, 2020).

Las directrices establecidas por la FCC imponen la obligación a la mayoría de los proveedores de servicios de comunicación de implementar y emplear el Protocolo STIR/SHAKEN en las secciones de Protocolo de Internet (IP) de sus infraestructuras. Este requisito tiene como objetivo permitir que los ciudadanos estadounidenses se beneficien plenamente de esta tecnología crucial, restaurando así la confianza en sus llamadas telefónicas.

En conformidad con las normativas de la FCC, se requiere que todos los proveedores de servicios de voz certifiquen en la base de datos de mitigación de llamadas automáticas que han implementado integralmente STIR/SHAKEN o han establecido un programa dedicado a mitigar las llamadas automáticas ilegales. Esta medida busca garantizar la transparencia y el compromiso de la industria en la lucha contra este tipo de actividades fraudulentas (Koilada, 2019).

Figura 9. *Base de datos mitigación de llamadas automáticas*



Robocall Mitigation Database

Keyword Search

Business Name	FCC Registration Number (FRN)	Previous Business Names	Business Address	Other DBA Name(s)	Foreign Voice Service Provider	Implementation	Gateway Provider	Intermediate Provider	Imported	Robocall Mitigatio
Cheyenne River Sioux Tribe Telephone Aut...	0002426831	None	625 N. Main St. Eagle Butte South Dakota 57625	C.R.S.T. Telephone Authority	No	Partial STIR/SHAKEN Implementation - Performing Robocall Mitigation	No	false	false	Ken White Eyes
JVOIP LLC	0030080071	None	1213 W Morehead St. STE 500 Charlotte NC 28208	None	No	Complete STIR/SHAKEN Implementation	No	false	false	Thiago Saldanha
Arctic Fox Networks Inc	0034634956	None	PO BOX 879769 Wasilla AK 99687	None	No	N/A	No	true	false	N/A
Voip Studio	0034554808	None	200 CENTURY PKWY STE 23 MOUNT LAUREL NJ 08054	None	No	Partial STIR/SHAKEN Implementation - Performing Robocall Mitigation	No	false	false	Sam Berzin
Calllinkers	0034632976	None	409 Joyce Kilmer Ave New Brunswick NJ 08901	None	No	Complete STIR/SHAKEN Implementation	No	false	false	David Jackson
Matchcom Telecommunications Inc.	0027710730	None	1680 Michigan Ave Ste 700 Miami Beach FL 33139	None	No	Complete STIR/SHAKEN Implementation	No	false	false	Cesar Luna

Adaptado de (Federal Communications Commission, 2023)

Como se muestra en la figura 9, en la base de mitigación de llamadas automáticas disponible en la página web de la Comisión Federal de Comunicaciones se encuentran los

proveedores de servicios de voz y proveedores de puerta acceso, se puede encontrar una lista activa de todos los proveedores que han presentado certificación y está disponibles para que el público puede descargarlas (Federal Communications Commission, 2023).

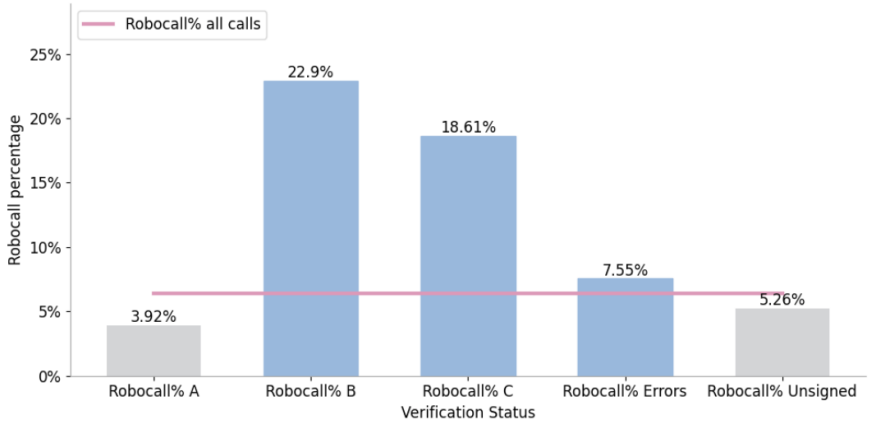
Aquellos proveedores que certifiquen la implementación de un programa de mitigación de llamadas automáticas deben detallar las medidas razonables que están adoptando para evitar la generación de tráfico ilegal de llamadas automáticas.

Es importante destacar que, dado que el marco STIR/SHAKEN opera exclusivamente en redes IP, las reglas de la Comisión también exigen que los proveedores que utilizan formas más antiguas de tecnología de red actualicen sus sistemas a IP o se embarquen activamente en el desarrollo de una solución de autenticación de identificación de llamadas que sea compatible con redes no IP. Esto refleja el compromiso de la FCC con la modernización y la seguridad en las comunicaciones, independientemente de la tecnología subyacente (Commision).

Como referencia del uso del protocolo STIR/SHAKEN en Estados Unidos, se revisó el informe mensual de STIR/SHAKEN publicado por TransNexus, con base en las cifras que recopilan de más de cien proveedores de servicios de voz que utilizan sus soluciones de STIR/SHAKEN y de prevención de llamadas automáticas. Las estadísticas las publican mensualmente desde abril de 2021 y los datos describen las llamadas que recibieron de otros 738 proveedores de servicios de voz que originaron llamadas, incluidas algunas llamadas automáticas, firmadas con STIR/SHAKEN. En la figura 10, compara el porcentaje de llamadas automáticas por nivel de certificación, para llamadas no firmadas y para todas las llamadas en junio de 2023. Las llamadas firmadas con certificación de nivel B o C incluyen un alto porcentaje de llamadas

automáticas. Las llamadas firmadas con certificación de nivel B tenían 4,4 veces más probabilidades de ser llamadas automáticas no firmadas.

Figura 10. *Porcentaje de llamadas automáticas por estado de verificación*



Adaptado de (TransNexus, 2023).

Los cambios en la participación de STIR/SHAKEN los miden mensualmente de tres formas:

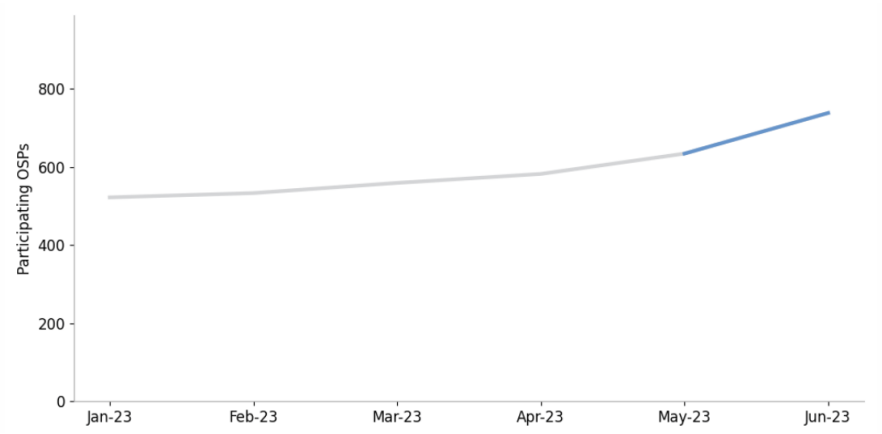
Proveedores de servicios de origen (OSP) que firman llamadas recibidas por sus clientes.

Proveedores de servicios autorizados para hacer SHAKEN por el Administrador de Políticas de STI (STI-PA).

Nuevas presentaciones de certificación en Robocall Mitigation Database (RMD).

La Figura 11 muestra la cantidad de llamadas firmadas por proveedores de servicios de origen (OSP). Esto había aumentado en aproximadamente 10 por mes en los meses anteriores. Se observan 104 nuevos firmantes de SHAKEN en junio, el mayor aumento mensual que se ha registrado.

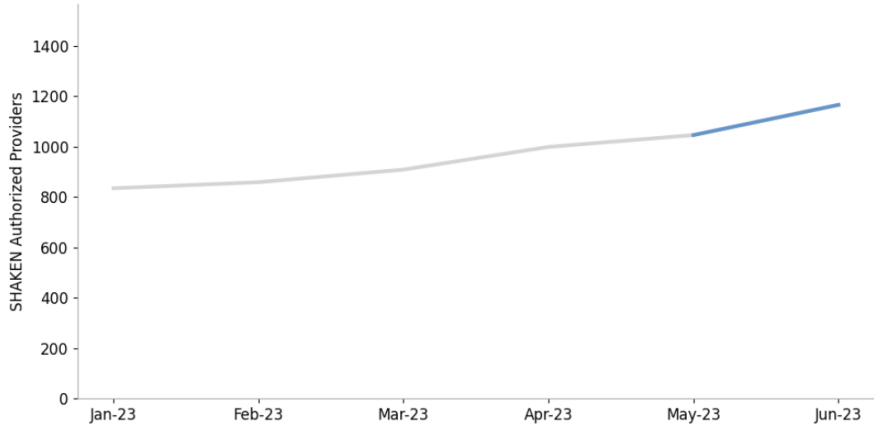
Figura 11. *Número de proveedores de servicios de origen (OSP) que envían llamadas firmadas*



Adaptado de (TransNexus, 2023).

La figura 12 muestra el número de proveedores autorizados de SHAKEN. Al igual que ocurre con los firmantes de OSP, este número tiene una tendencia ascendente que ha ido aumentando en los últimos meses. Hubo 120 nuevos proveedores autorizados de SHAKEN en junio.

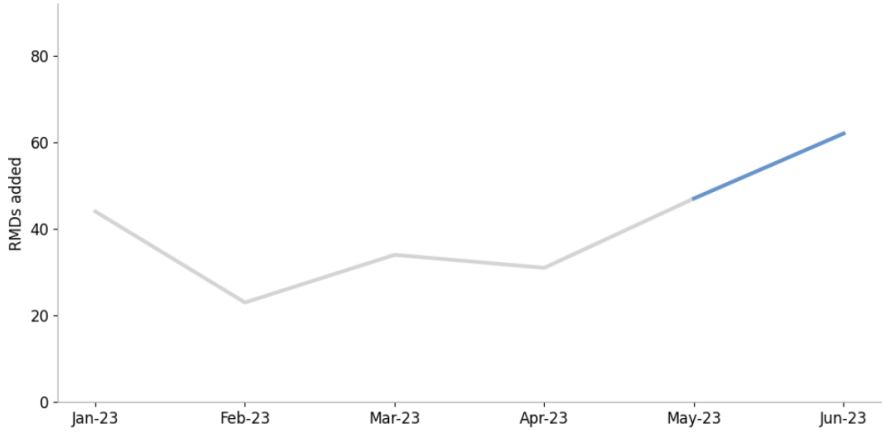
Figura 12. *Proveedores autorizados para STIR/SHAKEN por mes*



Adaptado de (TransNexus, 2023).

En la figura 13 muestra que las nuevas solicitudes de certificación en la base de datos de mitigación de llamadas automáticas aumentaron en 62 en junio. Se trata del mayor aumento desde junio de 2022, cuando se presentaron 108 nuevas certificaciones RMD.

Figura 13. *Nuevas solicitudes de bases de datos de mitigación de llamadas automáticas por mes*



Adaptado de (TransNexus, 2023).

Estas tres medidas muestran que la participación STIR/SHAKEN en Estados Unidos está cobrando impulso.

En el Informe trienal sobre la eficacia de las tecnologías utilizadas en el marco de autenticación de identificación de llamadas STIR/SHAKEN de la FCC, presentado al Comité Senatorial de Comercio, Ciencia y Transporte Comité de Energía y Comercio de la Cámara de Representantes de Estados Unidos, concluyen que la tecnología utilizada en el marco es eficaz para autenticar la información del identificador de llamadas e identificar llamadas falsificadas ilegalmente y anticipan que su eficacia aumentará a medida que la implementación de STIR/SHAKEN se generaliza. El marco cuenta con un apoyo significativo entre las partes interesadas, incluidos los proveedores de servicios de voz que han invertido recursos sustanciales en la implementación de STIR/SHAKEN en el transcurso de los últimos tres años y continúan haciéndolo (Wireline Competition Bureau, FCC, 2022).

4.1.2 Implementación del protocolo STIR/SHAKEN en Canadá.

La Comisión Canadiense de Radio, Televisión y Telecomunicaciones (CRTC) es el ente regulador de televisión y telecomunicaciones en Canadá. Esta institución estatal es la encargada de impartir lineamientos y ejercer control sobre aspectos relacionados con la prestación de servicio de transmisión de televisión por cable, regulación de los servicios de internet y telefonía, entre otros aspectos.

Con respecto a las redes de telefonía IP la CRTC estableció un marco técnico y operativo para la implementación del protocolo STIR/SHAKEN en todas las llamadas de voz fundamentadas en el Protocolo de Internet (IP). La CRTC como ente regulador de las telecomunicaciones determinó en su momento que a partir del 30 de noviembre de 2021 todos los operadores de telecomunicaciones (TSP) implementen el Protocolo STIR/SHAKEN con el propósito de autenticar y validar la información perteneciente a la identificación de llamadas (ID) para todas las llamadas de voz sobre redes de telefonía IP. En ese orden de ideas y con el propósito de establecer criterios y trabajar articuladamente con los distintos operadores en el país, la CRTC emitió una convocatoria de comentarios donde se recibieron aportes y sugerencias por parte de los distintos operadores de telecomunicaciones (TSP) (Commission, Compliance and Enforcement and Telecom Decision, 2021).

Algunas de las grandes compañías de telecomunicaciones como Bell Canada, CNOC, Cogeco, SaskTel, entre otros, realizaron observaciones como por ejemplo que a los pequeños operadores no se les exija la inmediata implementación de la solución STIR/SHAKEN debido a los costos económicos de su implementación, manifestaron que la implementación se debería realizar de manera gradual para algunos proveedores de servicio teniendo en cuenta algunos

criterios técnicos y de infraestructura tecnológica. A su vez algunos operadores manifestaron no estar de acuerdo con establecer como una condición de servicio la implementación del protocolo STIR/SHAKEN.

En conclusión, a las peticiones realizadas por los distintos operadores de telecomunicaciones la CRTC resolvió de manera concluyente varios aspectos como se describe a continuación:

- Ordenar a todos los operadores de servicios de telecomunicaciones (TSP) implementar el Protocolo STIR/SHAKEN en todas las redes basadas en el protocolo IP, esta medida se extiende a todos los operadores del país indistintamente de su tamaño, ubicación o cualquier otro de componente. La Comisión Canadiense de Radio, Televisión y Telecomunicaciones CRTC estableció que posponer su implementación erosionaría la eficacia de la solución, adicionalmente impediría tener un avance significativo de lograr impedir que los usuarios y en general todas las autoridades cuenten con las herramientas adecuadas para verificar la autenticidad de las llamadas y combatir la suplantación de estas.
- Se estableció la Autoridad Canadiense de Gobernanza de Tokens Seguros (CSTGA) dentro del proceso de despliegue e implementación del Protocolo STIR/SHAKEN. Esta autoridad es la encargada de escoger el Administrador de Políticas (PA) y la Autoridad Certificadora (AC) los cuales son ejes fundamentales dentro de la solución STIR/SHAKEN.
- La comisión determinó que es oportuno exigir a los operadores implementar el protocolo STIR/SHAKEN como condición para suministrar servicios de telecomunicaciones.

4.1.3 Avances implementación en Brasil.

Desde el año 2020, la Agencia Nacional de Telecomunicaciones de Brasil (ANATEL) ha adelantado eventos con expertos de la industria y proveedores de servicios abordando los orígenes y evolución de la tecnología STIR/SHAKEN, las experiencias internacionales de países donde esta tecnología ya es usada y los principales desafíos para la implementación de STIR/SHAKEN en las redes nacionales (DPL NEWS, 2021).

En agosto de 2023, la Agencia Nacional de Telecomunicaciones de Brasil (ANATEL) informó sobre el progreso logrado en la reducción de llamadas abusivas, destacando las acciones implementadas hasta la fecha y delineando el plan de acciones futuras diseñado para mitigar este problema de manera efectiva.

- Creó un código de conducta para las telecomunicaciones.
- Se implementó el código telefónico 0303 para ser utilizado por teleoperadores.
- Lanzó una serie de “medidas cautelares”:

  La Primera Medida Cautelar se dirigió a 26 proveedores de telecomunicaciones con el mandato de limitar las llamadas cortas (llamadas con una duración inferior a tres segundos) a 100 por día, por número.

  La Segunda Medida Cautelar amplió la Primera Medida Cautelar con medidas de eficiencia, transparencia y un ranking de principales infractores.

  La Tercera Medida Cautelar amplió la Primera y Segunda Medidas Cautelares a todas las empresas de telecomunicaciones.

Hasta finales del 2023 comenzará la implementación del protocolo de autenticación e identificación de llamadas STIR/SHAKEN en las redes telefónicas brasileñas. Se trata de una solución en la que las llamadas se presentarán a los consumidores con el número del marcador y también con su identificación, nombre y logotipo, así como el motivo de la llamada y el sello que acredita al emisor de la llamada. Con esta información será posible que el consumidor identifique empresas y decida si está interesado en atender la llamada. También será posible reconocer conexiones que constituyan conductas abusivas, para que el consumidor pueda adoptar las medidas que considere oportunas. El Grupo de Implementación del mecanismo de autenticación e identificación de llamadas ya contrató una solución centralizada, con la expectativa de que las primeras llamadas identificadas y autenticadas ocurran en enero de 2024 (Ministério das Comunicações - Agência Nacional de Telecomunicações, 2023).

4.1.4 Avances implementación en Europa.

En Europa, la lucha contra las llamadas automáticas y la suplantación se enfoca en fortalecer el Reglamento General de Protección de Datos (GDPR) y reforzar las regulaciones de privacidad de datos personales. Al prohibir la venta de números de teléfono e información personal sin el permiso explícito del propietario, se busca reducir el acceso de los generadores de llamadas automáticas a información personal. Estas medidas buscan otorgar a las personas un mayor control sobre su información, permitiéndoles decidir si desean compartir datos personales, como números de teléfono, lo que podría disminuir la inclusión de estos datos en bases almacenadas y utilizadas con fines fraudulentos (Unión Europea, s.f.).

4.2 Modelos de seguridad en Colombia para redes de telefonía IP.

En el marco de la revisión de los modelos de seguridad para las redes de telefonía IP en Colombia, se realizó validación de los marcos normativos relacionados con el Modelo de Seguridad y Ciberseguridad expedidos por las entidades gubernamentales, Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC) y el Departamento Nacional de Planeación (DNP), así como el marco regulatorio expedido por la Comisión de Regulación de Comunicaciones (CRC).

Se destaca la revisión de documentos clave como el CONPES 3995 que establece la Política Nacional de Confianza y Seguridad Digital (Departamento Nacional de Planeación, 2020); el CONPES 3854, que establece la Política Nacional de Seguridad Digital (Departamento Nacional de Planeación, 2016) y el CONPES 3701, que define las directrices de la Política para la Ciberseguridad y Ciberdefensa (Departamento Nacional de Planeación, 2011), todos emitidos por el DNP. Así como el Modelo de Seguridad y Privacidad de la Información (MSPI) definido por el MinTIC, el cual establece un marco integral para la implementación de medidas técnicas y administrativas y relacionadas con el talento humano para la seguridad de la información, focalizadas en preservar la confidencialidad, integridad y disponibilidad de los diversos activos de información y componentes tecnológicos en Colombia (Ministerio de Tecnologías de la Información y las Comunicaciones, 2021). En el curso de la revisión normativa, se observa que las directrices y lineamientos impartidos por estos entes gubernamentales en Colombia no contemplan mecanismos específicos de seguridad orientados a redes de telefonía IP. Asimismo, no se sugiere la alineación con marcos o estándares internacionales que aborden esta situación específica.

Por otra parte, se realizó contacto con la Comisión de Regulación Comunicaciones (CRC), organismo encargado de regular y supervisar los mercados y servicios de Telecomunicaciones del país y garantizar la protección de los derechos de los usuarios, con el objetivo de conocer el marco regulatorio que rige a los operadores de telefonía IP en Colombia. Se solicitó al ente de control información en relación al marco diferencial o categorización específica para los servicios de telecomunicaciones, particularmente aquellos que operan a través de la tecnología de voz sobre Protocolo de Internet (VoIP) y las regulaciones vigentes que supervisan y controlan la prestación, calidad y seguridad de la información en los servicios de telefonía IP en aspectos tales como la interoperabilidad, los requisitos de calidad de servicio, la protección de la privacidad y seguridad de los datos transmitidos a través de estos servicios.

A la solicitud, el ente regulador informa que de acuerdo a la Ley 1341 de 2009 modificada por la Ley 1978 de 2019, en Colombia se aplica el principio de neutralidad tecnológica. *"Artículo 6. Neutralidad Tecnológica. El Estado garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible".* Para la adopción y despliegue de redes para prestar servicios con tecnología de Voz IP (VoIP) bien sea para los servicios de telecomunicaciones fijos o móviles, la CRC no establece marcos diferenciales con condiciones únicas y específicas que apliquen a una tecnología especial. La regulación que expide la CRC aplica para todos los servicios de telecomunicaciones independiente de la tecnología usada para ofrecerlos al usuario final (CONGRESO DE COLOMBIA, 2009).

Para la adopción y despliegue de redes para prestar servicios con tecnología de Voz IP (VoIP) bien sea para los servicios de telecomunicaciones fijos o móviles, la CRC no establece marcos diferenciales con condiciones únicas y específicas que apliquen a una tecnología especial. A partir de la expedición de la ley 1341 de 2009, no existe una diferencia o categorización de los servicios de Telecomunicaciones, de manera que la provisión de redes y servicios de telecomunicaciones se habilita sin consideración al tipo de tecnología que se emplee para el efecto. En otras palabras, la regulación que expide la CRC aplica para todos los servicios de telecomunicaciones independiente de la tecnología usada para ofrecerlos al usuario final.

En cuanto a las condiciones de acceso, uso e interconexión de las diferentes redes de telecomunicaciones, en el Título IV de la Resolución CRC 5050 de 2016, la CRC estableció el Régimen de acceso, uso e interconexión de las redes de telecomunicaciones en un ambiente de convergencia tecnológica. Este régimen aplica para todas las redes de telecomunicaciones, independiente de la tecnología usada para prestar los servicios de telecomunicaciones a través de estas y, debe cumplirse por parte de todos los Proveedores de Redes y Servicios (PRST) que hagan uso de esta tecnología. Ahora bien, dentro del régimen si se establecen algunas condiciones técnicas que por la naturaleza de las tecnologías si son únicas para cada una de ellas y estas deben tenerse en consideración y cumplirse cuando se implementen interconexiones que involucren dichas tecnologías. Del mismo modo, en el Título V de la mencionada resolución, la CRC estableció el Régimen de calidad para los servicios de telecomunicaciones, incluido el servicio de voz fijo y móvil. Igualmente, y como sucede con el régimen de acceso, uso e interconexión, para los servicios de telecomunicaciones prestados a través de redes IP pueden establecerse condiciones técnicas que solo apliquen a esta tecnología debido a la diferencia existente con las demás. No

obstante, el régimen de calidad es único y aplica para todos los PRST que presten servicios de telecomunicaciones al público y debe ser cumplido, independiente de la tecnología usada para proveer los servicios (Comisión de Regulación de Comunicaciones, 2016).

En ese sentido, las regulaciones en el ámbito de las telecomunicaciones en Colombia se centran principalmente en aspectos generales de la prestación de servicios de comunicaciones, pero no abordan detalladamente las cuestiones específicas en las redes de telefonía IP, actualmente no existe una normativa por parte del ente regulador de Telecomunicaciones, que estandarice las políticas de seguridad de la telefonía IP, lo que conlleva a que los operadores del país no implementen mecanismos técnicos de cifrado para la autenticación de identificador, que permitan mitigar la suplantación de identidad de llamadas que cursan a través de la red de telefonía IP.

La ausencia de mecanismos normativos y legales que regulen los aspectos técnicos y de funcionamiento de las redes de telefonía IP, así como la prestación de servicios sobre ellas, presenta un desafío significativo en términos de seguridad, especialmente en la prevención de la suplantación de identidad en llamadas telefónicas. Dada la falta de directrices específicas por parte de la Comisión de Regulación de Comunicaciones (CRC) u otros entes reguladores, es esencial abordar esta problemática considerando diversos enfoques.

Este análisis pone de manifiesto la necesidad de considerar medidas específicas de seguridad para las redes de telefonía IP, así como la posibilidad de explorar estándares y mejores prácticas internacionales para abordar esta área crítica de la infraestructura tecnológica. Este

enfoque permitirá fortalecer aún más la seguridad digital en consonancia con las tendencias y desafíos emergentes en el panorama de la ciberseguridad.

El vacío frente a un marco regulatorio conlleva a abordar esta problemática desde un aspecto mucho más amplio y que incluya aspectos tales como examinar las normas técnicas y de calidad que se aplican a los servicios de telefonía IP, evaluar las disposiciones de seguridad implementadas para proteger la integridad de las comunicaciones, revisar las disposiciones que protegen los derechos de los usuarios, analizar cómo se alinea la regulación colombiana con los estándares internacionales en telefonía IP, analizar desafíos emergentes entre otros aspectos.

En el marco de la revisión de los modelos de seguridad para las redes de telefonía IP en Colombia, se aplicaron encuestas dirigidas a personal especializado del Centro Cibernético de la Policía Nacional y a un representante de los operadores de telefonía IP en el territorio nacional. El objetivo prinicipal de este sondeo ha sido determinar el nivel de conocimiento y familiarización con el protocolo STIR/SHAKEN, así como identificar las estrategias y procedimientos vigentes en el país destinados a la prevención y mitigación de la suplantación de identidad en las comunicaciones a través de la red de telefonía IP, ver apéndices C y D para un análisis detallado.

Los resultados obtenidos de estas entrevistas revelan una brecha significativa en la implementación de mecanismos técnicos avanzados para contrarrestar la suplantación de identidad en las redes de telefonía IP. Además, se evidencia una notable falta de conocimiento acerca de STIR/SHAKEN, lo que subraya la necesidad de adoptar medidas de divulgación del protocolo.

4.3 Escenario de simulación para validar la implementación y eficacia del protocolo STIR/SHAKEN.

4.3.1 Firma y verificación de la llamada.

En esta actividad se realizó la validación de la implementación y funcionamiento del protocolo STIR/SHAKEN sobre un ambiente de simulación de software libre, para esto se utilizó como herramienta de simulación el lenguaje de programación Phyton para demostrar el concepto principal de STIR/SHAKEN de firmar y verificar las llamadas. En esta simulación, se hace foco sobre dos componentes clave del sistema STIR/SHAKEN: el Servidor de Firma (STI-AS) y el Servidor de Verificación (STI-VS). El primero se encarga de firmar las llamadas salientes, mientras que el segundo verifica esas firmas en las llamadas entrantes.

Como se muestra en la figura 14, se genera una llave privada RSA de 2048 bits que simula la llave privada del Servidor de Firma (STI-AS). Se define el número de teléfono del llamante, que para efectos de simulación es el "6076817387", se realiza la creación del Token JWT (JSON Web Token) utilizando la biblioteca JWT que incluye la identidad del emisor (ISS), la marca de tiempo de emisión (IAT), y el número de teléfono del llamante (ORIG). Este token se firma con la llave privada del servidor de firma usando el algoritmo de firma RS256, el token firmado se imprime en la consola.

Figura 14. *Simulación firma de la llamada.*

```python
from cryptography.hazmat.backends import default_backend
from cryptography.hazmat.primitives import hashes, serialization
from cryptography.hazmat.primitives.asymmetric import rsa
import jwt
import datetime

# Llave privada del Servidor de Firma (STI-AS)
private_key = rsa.generate_private_key(
    public_exponent=65537,
    key_size=2048,
    backend=default_backend()
)

# Número de teléfono del llamante
caller_number = "6076817387"

# Crear el token JWT
token = jwt.encode(
    {
        "iss": "servidor_firma",
        "iat": datetime.datetime.utcnow(),
        "orig": caller_number,
    },
    private_key,
    algorithm='RS256'
)

print(f"Llamada firmada: {token}")
```

Nota. En la simulación se importan las librerías de Python correspondientes al paquete "cryptography" las cuales permiten generar claves y realizar operaciones criptográficas como la firma digital, cálculos criptográficos necesarios para implementar el concepto de autenticación de STIR/SHAKEN.

- cryptography.hazmat.backends.default_backend, proporciona acceso a un backend criptográfico predeterminado. Es responsable de seleccionar y gestionar la implementación específica de los algoritmos criptográficos subyacentes.

- cryptography.hazmat.primitives.hashes, contiene implementaciones de funciones hash. En la simulación, se utiliza para calcular el hash de los datos antes de firmarlos.
- cryptography.hazmat.primitives.serialization, se utiliza para serializar y deserializar claves públicas y privadas.
- cryptography.hazmat.primitives.asymmetric.rsa, se utiliza para generar un par de claves (pública y privada) y realizar operaciones de firma y verificación digitales.

Seguido de la firma de la llamada se simula la verificación de la firma, se obtiene la llave pública correspondiente a la llave privada del servidor de firma, que simula la llave pública del Servidor de Verificación (STI-VS), se define nuevamente el número de teléfono del llamante y se simula la recepción de un token firmado, en un escenario real, el token sería recibido de la red telefónica después de que la llamada ha sido firmada por el servidor de firma, para esto se utiliza la biblioteca JWT. Se verifica que el número de teléfono del originador en el token sea igual al número de teléfono esperado. Si es así, la llamada se considera auténtica, de lo contrario será marcada como no válida.

Para efectos de validación de la efectividad de la verificación de la firma, se simularon dos escenarios. En el primer escenario que se muestra en la figura 15, en el “signed token” se utilizó el mismo token que se generó en el paso anterior, al hacerlo, la verificación del número de teléfono ('orig') en el token pasará correctamente, y la llamada será considerada auténtica como se muestra en la figura 16.

Figura 15. *Simulación verificación de la firma - Llamada auténtica*

```
# Llave pública del Servidor de Verificación (STI-VS)
public_key = private_key.public_key()

# Token firmado (simulado)
signed_token = token  # Simulación: Utilizar el mismo token generado
anteriormente

try:
    # Verificar el token JWT
    decoded_payload = jwt.decode(signed_token, public_key, algorithms=['RS256'])

    if decoded_payload['orig'] == caller_number:
        print("Firma válida, la llamada es auténtica.")
    else:
        print("Número de teléfono falsificado. La llamada no es auténtica.")
except jwt.ExpiredSignatureError:
```

Figura 16. *Resultado simulación llamada firma válida.*

```
Llamada firmada:
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJzZXJ2aWRvcl9maXJtYSIsImlhdCI6MTcw
MDkyMjgwMiwib3JpZyI6IjEyMzQ1Njc4OTAifQ.I7fvpk6skLq9QrlxrbRqA9p8btNDmShqJIlk7QECx8
i9Az4d0xTRMVdN15IoFvHVl3P7vLitZWPIIpolKt0_b3-
4jozoWivBSUOQCVfdrUom87BoMQDsR52l5N2m7EifZHxwBOpfNf5L3DHbci5hw_gXUq2q74G07DY9nw4C
IBARnnpvebmMf6NfqPFhrGBurQ7T2BmTaaiTxpMWDrfBvsDAwUVEnVOIjG2agy-
DzvxuNMcl3X2aK9_AZEn2nfoNvknuxXvOfVrgQZDJVL80xAxlipApCrx6936duHChE8o1dzqTWB24f6Bu
sYMdyi0qtSC5okzDr2WXfTwHxd-SAw
Firma v◆lida, la llamada es aut◆ntica.

[Done] exited with code=0 in 0.634 seconds
```

En el segundo escenario de simulación, que se muestra en la figura 17, en el “signed token” se utilizó un token diferente al declarado, al hacerlo, la verificación del número de teléfono ('orig') en el token es diferente, por lo tanto, la verificación de la firma fallará y se imprimirá el mensaje indicando que la llamada no es auténtica como se muestra en la figura 18.

Figura 17. *Simulación verificación de la firma de llamada no auténtica*

```python
# Llave pública del Servidor de Verificación (STI-VS)
public_key = private_key.public_key()

# Número de teléfono del llamante
caller_number = "6076817387"

# Token firmado (simulado)
signed_token = "TOKEN_FIRMADO_AQUI"

try:
    # Verificar el token JWT
    decoded_payload = jwt.decode(signed_token, public_key, algorithms=['RS256'])

    if decoded_payload['orig'] == caller_number:
        print("Firma válida, la llamada es auténtica.")
    else:
        print("Número de teléfono falsificado. La llamada no es auténtica.")
except jwt.ExpiredSignatureError:
    print("Firma expirada. La llamada no es auténtica.")
except jwt.InvalidTokenError:
    print("Firma no válida. La llamada no es auténtica.")
```

Figura 18. *Resultado simulación llamada firma no válida.*

```
[Running] python -u "c:\Users\iadf0\OneDrive\Documentos\STIR
SHAKEN\llamada_no_valida.py"
Llamada firmada:
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJzZXJ2aWRvcl9maXJtYSIsImlhdCI6MTcw
MDkyMTY5NSwib3JpZyI6IjEyMzQ1Njc4OTAifQ.FZE4ILh49AiXruPEtjufENLq35bEeVfu5boPU1xh2V
rjy84B7tIoScb2BaXSn9Sw5t40sPwpwnpTS67ZPgMW9M05361tfqg4yjZLI6PZ4PyHtwM1xgLAWuKVJB6
80kX7sA3sqeoS90TkjzM1IYIvIBegwSdXibAN330wGZztfHInkMluNeJBSyyBYDtZxf1OSdZu_UJAE3-
roTfTVvSyqfbaNxzEAji3DvOBjYlz9JPNEMBXMVowrKiiC5a8R5y8hvzPihdkeS83uIyXOP8xfqxSf9lp
xJtRND1OL3d32ECb1--MK6Ngenp8DVNe8hwHbpx-Cg1Uc1DC2CN2kheB_w
Firma no v□lida. La llamada no es aut□ntica.

[Done] exited with code=0 in 0.927 seconds
```

Estas simulaciones proporcionan una visión simplificada de los procesos de firma y verificación en el protocolo STIR/SHAKEN. El proceso de firma de llamadas mediante la generación de tokens JWT y su firma digital con una llave privada proporciona una capa de

seguridad robusta, La inclusión de información como el emisor, la marca de tiempo y el número de teléfono del llamante en el token refuerza la autenticidad de la llamada saliente. El uso de llaves en este proceso refleja la aplicación de principios criptográficos sólidos para asegurar la integridad de la información.

4.3.2 Esquema básico para trabajar STIR/SHAKEN con PASSporT.

STIR/SHAKEN utiliza PASSporT (Personal ASSertion Token) también conocido como token de identidad, el contiene la información que STIR/SHAKEN necesita para la autenticación y verificación de llamadas. Los PASSporT tienen el formato de tokens web JSON. Contienen un encabezado, una carga útil y una firma. El encabezado define el tipo de PASSporT. La carga útil incluye la información de identidad de una llamada, la firma se genera mediante técnicas criptográficas asimétricas (TransNexus, transnexus.com).

En esta simulación, se hizo la implementación de un esquema básico para trabajar con PASSporT STIR/SHAKEN. Como se muestra en el código de la figura 19, se definieron tres clases: StirShakenHeader, StirShakenPayload, y StirShakenPassport. Cada una representa una parte específica del Personal ASSertion Token: encabezado, carga útil y la estructura general del token de identidad. Se utilizan funciones Codificar y Decodificar, *encode_passport* y *decode_passport*; así como funciones firmar y verificar la firma, *sign_passport* (simula el proceso de firma utilizando SHA-256) y *verify_signature* (simula el proceso de verificación de la firma, compara la firma almacenada con una firma calculada). Se crea un objeto *StirShakenPassport* con un encabezado y una carga útil y se simula el proceso de firma del pasaporte y la verificación de la firma.

Figura 19. *Simulación PASSporT STIR/SHAKEN*

```
import json
import time
import hashlib

# Define a class for the Passport Header
class StirShakenHeader:
    def __init__(self, alg, ppt, typ, x5u):
        self.alg = alg
        self.ppt = ppt
        self.typ = typ
        self.x5u = x5u

# Define a class for the Passport Payload
class StirShakenPayload:
    def __init__(self, attest, dest, iat, orig, origid):
        self.attest = attest
        self.dest = dest
        self.iat = iat
        self.orig = orig
        self.origid = origid
# Define a class for the Passport, containing the Header, Payload, and Signature
class StirShakenPassport:
    def __init__(self, header, payload, signature):
        self.header = header
        self.payload = payload
        self.signature = signature

# Function to encode Passport to JSON format
def encode_passport(passport):
    passport_dict = {
        "header": {
            "alg": passport.header.alg,
            "ppt": passport.header.ppt,
            "typ": passport.header.typ,
            "x5u": passport.header.x5u
        },
        "payload": {
            "attest": passport.payload.attest,
            "dest": passport.payload.dest,
            "iat": passport.payload.iat,
            "orig": passport.payload.orig,
            "origid": passport.payload.origid
        },
```

```
        "signature": passport.signature
    }
    return json.dumps(passport_dict, indent=2)

# Function to decode Passport from JSON format
def decode_passport(encoded_passport):
    passport_dict = json.loads(encoded_passport)
    header = StirShakenHeader(**passport_dict["header"])
    payload = StirShakenPayload(**passport_dict["payload"])
    signature = passport_dict["signature"]
    return StirShakenPassport(header, payload, signature)

# Function to simulate signing the Passport (generating a simple signature)
def sign_passport(passport):
    data_to_sign = passport.header.alg + passport.payload.attest
    passport.signature = hashlib.sha256(data_to_sign.encode()).hexdigest()

# Function to simulate verifying the Passport signature
def verify_signature(passport):
    data_to_verify = passport.header.alg + passport.payload.attest
    calculated_signature = hashlib.sha256(data_to_verify.encode()).hexdigest()
    return passport.signature == calculated_signature

# Create and initialize StirShakenPassport object with a Header and Payload
header = StirShakenHeader("ES256", "shaken", "passport",
"https://shaken.signalwire.cloud/sp.pem")
payload = StirShakenPayload("B", {"tn": ["01256700800"]}, int(time.time()),
{"tn": "01256500600"}, "e32f4189-cb86-460f-bb92-bd3acb89f29c")
passport = StirShakenPassport(header, payload, None)

# Encode the Passport to JSON format and print it
encoded_passport = encode_passport(passport)
print("\n1. Passport encoded:")
print(encoded_passport)

# Decode the Passport from JSON format and print the decoded Header and Payload
decoded_passport = decode_passport(encoded_passport)
print("\n2. Passport decoded:")
print(f"Header: {decoded_passport.header._dict_}")
print(f"Payload: {decoded_passport.payload._dict_}")

# Sign the Passport (simulate the signing process)
sign_passport(passport)
print("\n3. Passport signed.")

# Verify the Passport signature (simulate the verification process)
if verify_signature(passport):
    print("Passport signature is valid.")
else:
    print("Passport signature is invalid.")
```

El resultado que se muestra al ejecutar el código en la figura 20, incluye la información sobre el token de identidad creado, codificado, decodificado, firmado y verificado.

Figura 20. *Resultado simulación PASSporT STIR/SHAKEN*

4.4 Construcción de la guía de implementación.

Con base en la validación de los resultados y avances obtenidos durante las fases anteriores, se desarrolló una guía de recomendaciones que sirve como material de estudio para el ente regulador y que establece los aspectos más relevantes para la adopción del modelo de seguridad basado en el protocolo STIR/SHAKEN para las redes de telefonía IP en Colombia.

Dentro de los aspectos destacados que proporciona esta guía se establecen recomendaciones relacionadas con el desarrollo de buenas prácticas, mecanismos que deben tener en cuenta los proveedores de servicios de voz IP, aspectos relacionados con la autenticación de llamadas mediante proveedores intermedios, desarrollo de un marco regulatorio, monitoreo y evaluación continua, entre otros aspectos. Ver Anexo 1.

5. Conclusiones

Se ha comprobado que la tecnología incorporada en el marco de STIR/SHAKEN es efectiva para autenticar la información del identificador de llamadas y detectar llamadas falsificadas ilegítimas, este avanzado sistema se encuentra en uso en varios países, en los cuales, gracias a una colaboración coordinada entre los proveedores de servicios, los entes reguladores y los usuarios en general, se han logrado avances significativos tanto en la implementación como en el despliegue exitoso de la tecnología.

Existe una falta de marcos normativos y legales que supervisen los aspectos técnicos y operativos de las redes de telefonía IP en Colombia, así como la implementación de mecanismos de seguridad sobre estas plataformas, los cuales son esenciales para hacer frente al creciente aumento de delitos informáticos, específicamente aquellos que involucran herramientas tecnológicas, como es el caso de las llamadas realizadas a través de la telefonía IP.

Los resultados obtenidos en la evaluación del modelo del protocolo STIR/SHAKEN a través de un ejercicio de simulación por medio de la utilización de software libre destacan no solo la viabilidad técnica de su implementación, sino también su capacidad para autenticar la información del identificador de llamadas y contrarrestar la suplantación de identidad de manera eficaz.

La guía elaborada entrega lineamientos que pueden ser consideradas por el ente regulador para su análisis. Asimismo, se proporcionan sugerencias con respecto a las acciones que deben

tenerse en cuenta para la implementación exitosa del protocolo STIR/SHAKEN por parte de los proveedores de servicios de telecomunicaciones en Colombia.

6. Trabajos a futuro

Este trabajo de grado se constituye como un recurso y un punto de referencia para futuros esfuerzos tanto en la investigación académica como en la formulación de políticas regulatorias enmarcados en el robustecimiento de la seguridad en las telecomunicaciones. El estudio y la simulación del protocolo STIR/SHAKEN realizado en este trabajo de grado han demostrado la viabilidad y efectividad del protocolo en la autenticación de las llamadas y en la lucha contra la suplantación de identidad, esto lo convierte en una referencia clave en el ámbito académico y sienta las bases para investigaciones más especializadas con ambientes de simulación que involucren una mayor cantidad de variables operativas, el desarrollo de investigaciones sobre la integración de STIR/SHAKEN con tecnologías emergentes como las redes 5G, así como la promoción de proyectos de colaboración interdisciplinaria entre departamentos académicos de tecnología y derecho para abordar la implementación de STIR/SHAKEN desde una perspectiva holística.

Para el ente regulador del país, este trabajo proporciona un base para el establecimiento de lineamientos que rijan la autenticación de llamadas como medida de prevención del fraude y la formulación de políticas que orienten la implementación efectiva de STIR/SHAKEN en Colombia. Además, promueve la colaboración con los operadores de telecomunicaciones para incentivar la adopción de medidas de seguridad adicionales en las redes de telefonía IP para prevenir delitos informáticos, complementando la implementación de STIR/SHAKEN.

Referencias

Agency, D. A. (September 1981). *Internet Protocol Specification.* Arlington, Virginia.

Alliance for Telecommunications Industry Solutions. (2021). *Signature-based Handling of Asserted information using toKENs (SHAKEN):*. Washington, DC.

ATIS. (n.d.). *Improper Authentication and Attestation.*

Benedini, I. (2013). *Ataque de man in the middle para protocolo sip mediante análisis de.* Buenos Aires.

C. Wendt Comcast, J. Peterson Neustar Inc. (2018). *PASSporT: Personal Assertion Token.* Internet Engineering Task Force (IETF).

CCN-CERT. (2021). *Nacional, C. C. (2021). Ciber_Amenazas y Tendencias.*

CISCO, L. (2023). *Perspectivas de Ciberseguridad de los líderes de la industria.*

Comisión de Regulación de Comunicaciones. (2016, 11 10). Resolución - 5050. *Resolución - 5050*. Colombia.

Commision, F. C. (n.d.). *Combating Spoofed Robocalls with Caller ID Authentication.* Retrieved from www.fcc.gov: https://www.fcc.gov/call-authentication

Commission, C. R.-t. (2021). *Compliance and Enforcement and Telecom Decision.* Ottawa.

Commission, C. R.-t. (n.d.). *https://crtc.gc.ca*. Retrieved from https://crtc.gc.ca: https://crtc.gc.ca/eng/phone/telemarketing/identit.htm

Communications, C. F. (2020). *FCC Mandates that Phone Companies implement Caller ID authentication to combat spoofed robocalls.* Washington.

CONGRESO DE COLOMBIA. (2009). LEY 1341 DE 2009. *LEY 1341 DE 2009*.

D. Butcher, X. L. (2007). Security Challenge and Defense in VoIP Infrastructures. *IEEE Transactions on Systems Man and Cybernetics Part C (Applications and Reviews)*.

Departamento Nacional de Planeación. (2011). *CONPES 3701*. Bogotá.

Departamento Nacional de Planeación. (2016). *CONPES 3854*. Bogotá.

Departamento Nacional de Planeación. (2020). *CONPES 3995*. Bogotá.

DPL NEWS. (2021, Diciembre 22). Brasil | Anatel podría implementar tecnología para acabar con llamadas no deseadas. *Brasil | Anatel podría implementar tecnología para acabar con llamadas no deseadas*.

Edwards Gregory, G. M. (2020). Robocalling: STIRRED and SHAKEN! - An Investigation of Calling Displays on Trust and Answer Rates.

Federal Communications Commission. (2023, 12 01). *Robocall Mitigation Database*. Retrieved from Robocall Mitigation Database: https://fccprod.servicenowservices.com/rmd?id=rmd_welcome

Filip ŘEZÁČ, M. V. (January 2010). Security Risks in IP Telephony. *Advances in Electrical and Electronic Engineering*.

Gartner. (n.d.). *www.gartner.com*. Retrieved from https://www.gartner.com/en/information-technology/glossary/voice-over-internet-protocol-voip

Handeley, M., Shulzrinne, H., & Schooler, E. (1999). *SIP: Session Initiation Protocol.* The Internet Society.

J. Rosenberg dynamicsoft, H. Schulzrinne Columbia U, G. Camarillo Ericsson, A. Johnston WorldCom, J. Peterson Neustar, R. Sparks dynamicsoft, M. Handley ICIR, E. Schooler AT&T. (June 2022). *SIP: Session Initiation Protocol.* Internet Society.

Jaikaran, C. (2016). Encryption: Frequently Asked Questions. *Congressional Research Service.*

Johnston, A. B. (2004). *Understanding the Session Initiation Protocol.* Artech House, Inc.

Kevin Daimi, H. R.-S. (2021). Advances in Security, Networks, and Internet of Things. *Springer*.

Koilada, D. V. (2019). Strategic Spam Call Control and Fraud Management: Transforming Global Communications. *IEEE Engineering Management Review*.

Livevox. (n.d.). *https://livevox.com/*. Retrieved from https://livevox.com/what-is-stir-shaken-and-how-does-it-work/

Mendez, F., & Valdez, J. &. (2013). Performance analysis of SIP and IAX VOIP signaling protocols in a dual stack enviroment network. *Revista Gerencia Tecnológica Informática*, pp. 47-61.

Ministério das Comunicações - Agência Nacional de Telecomunicações. (2023, Agosto 22). *www.gov.br*. Retrieved from www.gov.br: https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-apresenta-balanco-do-combate-as-chamadas-abusivas

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). *Modelo de Seguridad y Privacidad de la Información.*

Tejedor, R. J. (2020). www.ramonmillan.com. *Conectrónica No 232, GM2 Publicaciones Técnicas*. Retrieved from www.ramonmillan.com: https://www.ramonmillan.com/tutoriales/stirshaken.php#caracteristicasstirshaken

Terzoli, A. &. (2014). *An Investigation into the Provision of Video Capabilities in iLanga.*

TransNexus. (2023). *STIR/SHAKEN statistics from June 2023.*

TransNexus. (n.d.). *transnexus.com.* Retrieved from transnexus.com: https://transnexus.com/whitepapers/stir-and-shaken-overview/

TransNexus. (n.d.). *transnexus.com.* Retrieved from transnexus.com: https://transnexus.com/whitepapers/stir-shaken-cms-solutions/

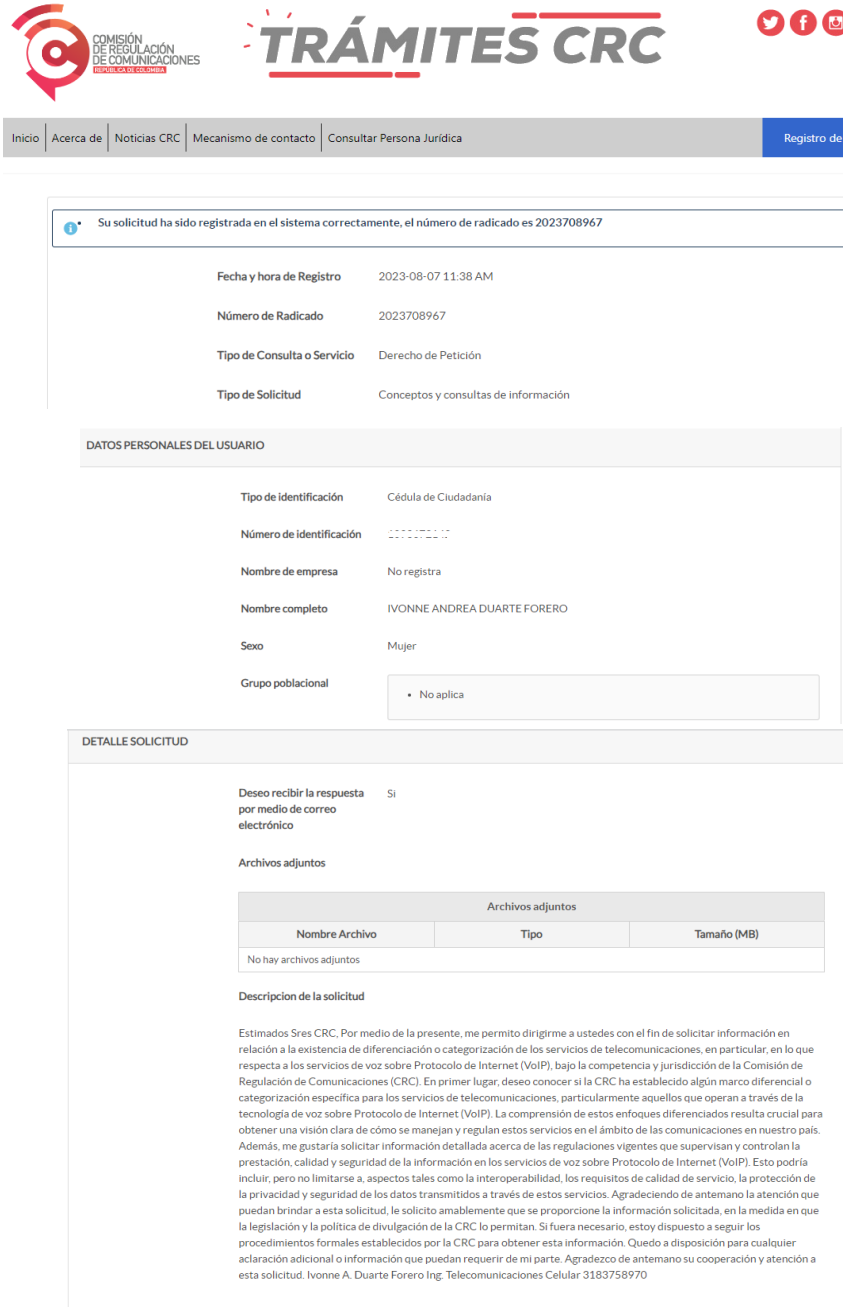
Unión Europea. (n.d.). *https://europa.eu/*. Retrieved from https://europa.eu/: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm

Ustelecom. (2019). *Anti-Robocall principles.* Retrieved from Anti-Robocall principles: https://www.ustelecom.org/wp-content/uploads/2019/08/State-AGs-ProvidersAntiRobocall-Principles-With-Signatories.pdf

Wireline Competition Bureau, FCC. (2022). *Triennial report on the efficacy of the Technologies used.*

Apéndices

Apéndice A. *Derecho de Petición Trámites CRC. Radicado 2023708967*



COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

TRÁMITES CRC

Inicio | Acerca de | Noticias CRC | Mecanismo de contacto | Consultar Persona Jurídica | Registro de

Su solicitud ha sido registrada en el sistema correctamente, el número de radicado es 2023708967

Fecha y hora de Registro	2023-08-07 11:38 AM
Número de Radicado	2023708967
Tipo de Consulta o Servicio	Derecho de Petición
Tipo de Solicitud	Conceptos y consultas de información

DATOS PERSONALES DEL USUARIO

Tipo de identificación	Cédula de Ciudadanía
Número de identificación	[redacted]
Nombre de empresa	No registra
Nombre completo	IVONNE ANDREA DUARTE FORERO
Sexo	Mujer
Grupo poblacional	• No aplica

DETALLE SOLICITUD

Deseo recibir la respuesta por medio de correo electrónico Si

Archivos adjuntos

Archivos adjuntos		
Nombre Archivo	**Tipo**	**Tamaño (MB)**
No hay archivos adjuntos		

Descripcion de la solicitud

Estimados Sres CRC, Por medio de la presente, me permito dirigirme a ustedes con el fin de solicitar información en relación a la existencia de diferenciación o categorización de los servicios de telecomunicaciones, en particular, en lo que respecta a los servicios de voz sobre Protocolo de Internet (VoIP), bajo la competencia y jurisdicción de la Comisión de Regulación de Comunicaciones (CRC). En primer lugar, deseo conocer si la CRC ha establecido algún marco diferencial o categorización específica para los servicios de telecomunicaciones, particularmente aquellos que operan a través de la tecnología de voz sobre Protocolo de Internet (VoIP). La comprensión de estos enfoques diferenciados resulta crucial para obtener una visión clara de cómo se manejan y regulan estos servicios en el ámbito de las comunicaciones en nuestro país. Además, me gustaría solicitar información detallada acerca de las regulaciones vigentes que supervisan y controlan la prestación, calidad y seguridad de la información en los servicios de voz sobre Protocolo de Internet (VoIP). Esto podría incluir, pero no limitarse a, aspectos tales como la interoperabilidad, los requisitos de calidad de servicio, la protección de la privacidad y seguridad de los datos transmitidos a través de estos servicios. Agradeciendo de antemano la atención que puedan brindar a esta solicitud, le solicito amablemente que se proporcione la información solicitada, en la medida en que la legislación y la política de divulgación de la CRC lo permitan. Si fuera necesario, estoy dispuesto a seguir los procedimientos formales establecidos por la CRC para obtener esta información. Quedo a disposición para cualquier aclaración adicional o información que puedan requerir de mi parte. Agradezco de antemano su cooperación y atención a esta solicitud. Ivonne A. Duarte Forero Ing. Telecomunicaciones Celular 3183758970

Apéndice B. *Derecho de Petición Trámites CRC. Respuesta a radicado 2023708967*

RADICACION DE SALIDA No.

Rad. 2023708967
Cod. 2000

Señora
IVONNE ANDREA DUARTE FORERO
Cel: 3217731689
Correo: iadf0302@gmail.com
Bucaramanga, Santander.

REF: Información sobre diferenciación o categorización de los servicios de telecomunicaciones prestados a través del protocolo IP, especialmente sobre la Voz IP (VoIP).

Respetada Señora Duarte,

La Comisión de Regulación de Comunicaciones (CRC) recibió su comunicación, por medio del radicado arriba anunciado, mediante la cual nos solicita información relacionada con diferenciación o categorización de los servicios de telecomunicaciones prestados a través del protocolo IP en la regulación expedida por la CRC.

Para dar respuesta, es importante señalar que, para poder proveer cualquier servicio de telecomunicaciones en el país, el interesado debe contar con la respectiva Habilitación General de la que habla el Artículo 10 de la Ley 1341 de 2009 modificada por la Ley 1978 de 2019.

En esta misma norma, también se establecen los principios orientadores que rigen al sector de la Tecnologías y las Comunicaciones, dentro de los que se encuentra el de Neutralidad Tecnológica, que dice lo siguiente:

"6. Neutralidad Tecnológica. El Estado garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible."

Sumado a lo anterior, es de aclarar que la Comisión de Regulación de Comunicaciones, es el órgano encargado de promover la competencia en los mercados, promover el pluralismo informativo, evitar el abuso de posición dominante, regular los mercados de las redes y los servicios de comunicaciones y garantizar la protección de los derechos de los usuarios; con el fin que la prestación de los servicios sea económicamente eficiente, y refleje altos niveles de calidad, de las redes y los servicios de comunicaciones, incluidos los servicios de televisión abierta radiodifundida y de radiodifusión sonora,? de conformidad con el artículo 19 de la Ley 1341 de 2009, modificado por el artículo 15 de la Ley 1978 de 2019.?

Por lo expuesto, para la adopción y despliegue de redes para prestar servicios con tecnología de Voz IP (VoIP) bien sea para los servicios de telecomunicaciones fijos o móviles, la CRC no establece marcos diferenciales con condiciones únicas y específicas que apliquen a una tecnología especial. En otras palabras, la regulación que expide la CRC aplica para todos los servicios de telecomunicaciones independiente de la tecnología usada para ofrecerlos al usuario final.

Por otro lado, en cuanto a las condiciones de acceso, uso e interconexión de las diferentes redes de telecomunicaciones, en el Título IV de la Resolución CRC 5050 de 2016, esta Entidad estableció el Régimen de acceso, uso e interconexión de las redes de telecomunicaciones en un ambiente de convergencia tecnológica. Como se indicó, este régimen aplica para todas las redes de telecomunicaciones, independiente de la tecnología usada para prestar los servicios de telecomunicaciones a través de estas y, debe cumplirse por parte de todos los Proveedores de Redes y Servicios (PRST) que hagan uso de esta tecnología. Ahora bien, dentro del régimen si se establecen algunas condiciones técnicas que por la naturaleza de las tecnologías si son únicas para cada una de ellas y estas deben tenerse en consideración y cumplirse cuando se implementen interconexiones que involucren dichas tecnologías.

Del mismo modo, en el Título V de la mencionada resolución, la CRC estableció el Régimen de calidad para los servicios de telecomunicaciones, incluido el servicio de voz fijo y móvil. Igualmente, y como sucede con el régimen de acceso, uso e interconexión, para los servicios de telecomunicaciones prestados a través de redes IP pueden establecerse condiciones técnicas que solo apliquen a está tecnología debido a la diferencia existente con las demás. No obstante, el régimen de calidad es único y aplica para todos los PRST que presten servicios de telecomunicaciones al público y debe ser cumplido, independiente de la tecnología usada para proveer los servicios.

En los anteriores términos, damos respuesta a su comunicación y quedamos atentos a cualquier aclaración adicional que requieran.

Proyectó: David Alberto Murillo N.
Revisó: Alejandra Arenas Pinto.

Finalmente, le solicitamos amablemente se sirvan diligenciar la encuesta haciendo click en el siguiente enlace: https://www.pnn.gov.co/EncuestaCARE?radicado=2023708967. La información es muy valiosa para la CRC ya que nos permite mejorar la calidad de nuestra atención.

NOTA: Este mensaje fue enviado por el sistema de Gestión Documental de la Comisión de Regulación de Comunicaciones . Por favor no intente responder a este mensaje, dado que este buzón de correo no es revisado por ningún funcionario de esta Entidad.
En caso de requerir información adicional, por favor acceda al siguiente formulario.

Cordial saludo,

Mariana Sarmiento Argüello
Coordinadora de Relacionamiento con Agentes
atencioncliente@crcom.gov.co
@CRCCol /CRCCol /CRCCol CRCCOL
Calle 59a Bis No. 5 - 53 Piso 9 Ed. Link Siete Sesenta
Código Postal: 110231 - Tel. +57 601 3198300
Bogotá - Colombia

Apéndice C. *Encuesta a proveedor de Telefónica Telecomunicaciones*

MAESTRÍA EN GESTIÓN Y CONSULTORÍA EN TIC

1. DATOS DE IDENTIFICACIÓN DEL ENTREVISTADO

1	Nombre y cargo del entrevistado:	Pedro Jose Rueda Gutiérrez Profesional Conmutación
2	Ciudad:	Bucaramanga
3	Nombre y tipo de Institución a la que pertenencia:	Telefónica Movistar - Telecomunicaciones
4	Campo en el que trabaja	Conmutación Fija

2. CUESTIONARIO

1) ¿Conoce o ha oído hablar del Protocolo Stir/Shaken para mitigar la suplantación de llamadas telefónicas sobre redes de VoIP?

1. X Nunca
2. ☐ Algo ha escuchado
3. ☐ Si

¿Qué conoce de esta tecnología?

_____

2) ¿Tiene conocimiento de casos relacionados con la suplantación de identidad de números telefónicos?

1. X No
2. ☐ SI

¿Cuáles? ¿Cómo funcionan?

_____

3) ¿Conoce si existe algún marco normativo en Colombia que regule la implementación de técnicas o mecanismos para prevenir la suplantación de llamadas telefónicas a través de redes VoIP?

   1. X No
   2. ☐ SI

   ¿Cuáles?

   _____

4) En su actual labor profesional, ¿Qué mecanismos conoce o recomienda para prevenir la suplantación de llamadas telefónicas mediante redes de telefonía IP en Colombia?

   ¿Cuáles? _
   No Conozco

5) ¿Cuál es su opinión sobre la posibilidad de que los operadores en Colombia adopten tecnologías para prevenir la suplantación de números telefónicos en redes VoIP?

   Describa con sus palabras:

   Creo que estamos demorados en que los operadores aseguren su red mediante dichas tecnologías, considerando que las redes PSTN se están reemplazando por redes sobre Voip. En pocos años, toda la telefonía fija funcionará sobre redes IP, lo cual se hace urgente adaptar medidas que prevengan dicha suplantación.

Apéndice D. *Encuesta a proveedor de Telefónica Telecomunicaciones*

MAESTRÍA EN GESTIÓN Y CONSULTORÍA

EN TIC

1. DATOS DE IDENTIFICACIÓN DEL ENTREVISTADO

1	Nombre y cargo del entrevistado:	JOSE LOPEZ MARROQUIN
2	Ciudad:	BOGOTÁ D.C
3	Nombre y tipo de Institución a la que pertenencia:	POLICIA NACIONAL
4	Campo en el que trabaja	CIBERSEGURIDAD

2. CUESTIONARIO

1) ¿Conoce o ha oído hablar del Protocolo Stir/Shaken para mitigar la suplantación de llamadas telefónicas sobre redes de VoIP?

1. Nunca _X
2. Algo ha escuchado _
3. Si _

¿Qué conoce de esta tecnología?

_____

2) ¿Tiene conocimiento de casos relacionados con la suplantación de identidad de números telefónicos?

1. No _
2. SI _X
¿Cuáles? ¿Cómo funcionan?

Este tipo de técnicas en algunos casos son tan especializadas que la eventual víctima aporta su información personal y financiera y siquiera genera una sospecha de que se trata de una modalidad de fraude; el problema con este tipo de casos es que no se realiza una denuncia ante la Fiscalía General de la Nación, situación que deja a las autoridades sin un contexto claro para establecer una línea investigativa

3) ¿Conoce si existe algún marco normativo en Colombia que regule la implementación de técnicas o mecanismos para prevenir la suplantación de llamadas telefónicas a través de redes VoIP?
1. No _
2. SI _X
¿Cuáles?

Con la materialización de este tipo de técnicas podríamos estar frente a conductas típicas en la norma como lo puede ser:

Artículo 269F. Violación de datos personales, el que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y

en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

Nota: sin embargo, la conducta por sí sola no está tipificada los delitos antes mencionados puede derivarse de la técnica implementada.

4) En su actual labor profesional, ¿Qué mecanismos conoce o recomienda para prevenir la suplantación de llamadas telefónicas mediante redes de telefonía IP en Colombia?

¿Cuáles?

- No proporcione información personal, información bancaria o contraseñas a través de llamadas.
- Realizar configuración de bloque de llamadas del proveedor de servicios ISP´s.
- Si recibe llamadas de alguien que afirma ser de una institución financiera u organización, verifica su identidad llamando directamente al número oficial de la empresa o banco.
- Ignora llamadas de números desconocidos

5) ¿Cuál es su opinión sobre la posibilidad de que los operadores en Colombia adopten tecnologías para prevenir la suplantación de números telefónicos en redes VoIP?

Describa con sus palabras:
Es una buena posibilidad que permitiría mitigar los riesgos a los que se ven expuestos los usuarios de las empresas prestadoras de servicios móviles en nuestro país; de igual forma permitiría reducir la conducta de forma significativa.