Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

MAESTRÍA EN CIBERDEFENSA y CIBERSEGURIDAD

Trabajo final de tesis

Vulnerabilidades y mitigación de riesgos en el ámbito de la ciberdefensa y ciberseguridad para la telefonía privada basada en la nube

Autor: Licenciado Daniel Perles

Director de Tesis: Ingeniero Aníbal Luis Intini

Fecha: 5 de diciembre 2019

i. RESUMEN.

En los últimos años, el mundo se enfrenta a una nueva amenaza: la guerra cibernética asimétrica, donde empresas y entes gubernamentales con grandes centros de datos, redes propias y usuarios individuales y hogareños de tecnología, están expuestos a constantes ataques informáticos, electrónicos y físicos a sus sistemas y equipos. Las actuales velocidades de transmisión, procesamiento y almacenamiento de la información están migrando el modelo actual de los centros de datos a infraestructuras basadas en la nube (del inglés: "*Cloud Computing*").

Esta tesis se enfoca en el estudio de uno de los tantos factores a contemplar a la hora de migrar un centro de datos a la nube, en particular analiza las singularidades de los aspectos fundamentales del problema de la ciberseguridad de la telefonía privada en las nuevas condiciones de servicio.

Muchas empresas y organismos públicos están adoptando servicios de telefonía privada basados en centros de datos localizados fuera de su propia infraestructura ofrecidos por nuevas compañías proveedoras de servicios tales como *Amazon Web Services, Google, Oracle, Microsoft Azure e IBM* entre otros.

Los motivos de este cambio tecnológico son varios, incluyendo la reducción de costos de infraestructura y de recursos humanos especializados para el mantenimiento de los centros de datos, la seguridad informática y la implementación de software seguro, pero principalmente en la necesidad de concentrase en su negocio principal (del inglés "*Core Business*"). Esta acción permite dejar el manejo y cuidado del centro de datos en manos de organizaciones especializadas, focalizando sus esfuerzos en el propio negocio dando lugar a que las organizaciones, ya sean privadas o estatales requieran un servicio y se independicen de esfuerzos como los de actualizaciones de hardware, software y dispositivos de red, que ahora recaen en el proveedor de servicios en la nube.

Recientes reportes especializados indican que un gran número de empresas y entes de gobierno están trabajando en proyectos, planes e implementaciones de migración, de su infraestructura de procesamiento, almacenamiento de información y servicios de telefonía, generando un cambio de paradigma en la gestión de la ciberseguridad para asegurar el servicio telefónico en servidores ubicados geográficamente en sitios remotos.

El objeto de esta tesis es el estudio y análisis de los aspectos mencionados anteriormente para la elaboración de un cuadro de vulnerabilidades y mitigación de riesgos en ciberdefensa y ciberseguridad en este nuevo escenario, que pueda ser utilizado por la comunidad técnica, científica y académica a la hora de evaluar el impacto de un plan de migración de los servicios de telefonía hacia la nube.

ii. ABSTRACT.

The world is experiencing a new threat. An asymmetric war where companies and government offices having data centers and networks deployed on premise sites are now exposed to constant cyberattacks to their systems and devices. These many times are part of the critical infrastructure of a nation.

This great technology offers much better data transmission speeds, higher CPU process times and bigger digital data storage capacities, which are changing the current model from on premise data centers to a Cloud based data centers model.

This document focuses on the specific case of moving the on-premise private IP Telephony infrastructure into a Cloud based data center solution. The public Cloud Computing based solution is being offered by many global providers such as Amazon Web Services, Google, Oracle, Microsoft Azure and IBM.

There are many reasons why a company decides to move into a Cloud based solution, from cost reduction (moving the current infrastructure as a capital expense into an operation expense model) to the need to have specialized human resources for data center maintenance, information security, secure software implementation and more. But mainly the need to dedicate their efforts in the core business, which could be finance, sales, factories or even technology. And leave the Data Center, infrastructure and Telephony services in hands of a third-party provider. Which can do it in a professional way and following the best practices for security policies, software patching and general cybersecurity standards.

This new scenario brings a new paradigm about the cybersecurity for the private telephony services, a change of managing and storing the phone calls in new servers and devices located geographically out of the company´s premises and open to many cybersecurity threads such DDOS attacks, phishing, spoofing and voice over IP and call recordings thefts.

These topics are the case study of this thesis with the objective to elaborate a cyber-defense and cybersecurity risk mitigation and vulnerability matrix for the scenario of an IP Telephony in the cloud. Expecting that this document could be useful even for companies or government offices planning a migration for their telephony infrastructure to the cloud, as well to academic and scientific community who wants to take any of the specific topics included into this work to be part of a new research.

iii. DEDICATORIAS.

A mi toda mi familia que siempre me acompaña y me espera en estas largas jornadas de estudio.

iv. AGRADECIMIENTOS.

A mi Director de Tesis, Ing. Aníbal Intini por su guía en el armado de tesis, las largas jornadas de revisión y tiempo dedicado, por enseñarme cada detalle importante en la redacción de una tesis y por las buenas ideas compartidas.

A los profesores y directivos que me acompañaron durante la maestría y el desarrollo del presente trabajo, Dr. Roberto Uzal, Ing. Carlos Amaya, Adriana Baravalle, Daniel Piorun y Christian Borghello.

A mis colegas de trabajo de quienes aprendí muchos detalles sobre el tema de la tesis Greg Hill, Chris Khoshaba, Don Ryan, Sam Somchana

A todos mis compañeros de la cohorte 2018 de la Maestría en Ciberdefensa y Ciberseguridad y en especial Dr. Nicolas Tato por su invalorable ayuda a todo el curso durante estos 2 años.

v. ÍNDICE

vi. ÍNDICE DE TABLAS

vii. ÍNDICE DE FIGURAS

viii. ABREVIATURAS Y ACRÓNIMOS

ISP	Internet Service Provider
GSIBA	Sistema Global Inteligente de base de datos de direcciones *IP* de atacantes DDOS
DDOS	Distributed Denial of Services
SBC	Session Border Controller
VOIP	Voice Over IP
APT	Advanced Persistent Tread
RTP	Real Time Protocol
SRTP	Secure Real Time Protocol
IP	Internet Protocol
TCP	Transmission Control Protocol
SMS	Short Message Service
SIP	Session Initiation Protocol
SDP	Session Description Protocol
DDOS	Distributed Denial of Service
DNS	Domain Name System
DMZ	Demilitarized Zone
ISDN	Integrated Service Digital Network
UTP	Unshielded Twisted Pair
OSI	Open System Interconnection
PABX	Private Branch Exchange
ISP	Internet Service Provider

VPN	Virtual Private Network
IaaS	Infrastructure as a Service
TI	Tecnología de la Información
RFC	Request for comment

1) INTRODUCCIÓN.

1.1) OBJETIVO.

Este trabajo de tesis tiene como principal objetivo, abordar la problemática relacionada con la ciberdefensa y ciberseguridad para la migración de la telefonía *IP* hacia sistemas basados en la nube, analizar detalladamente las vulnerabilidades y riesgos, concientizar a la comunidad tecnológica, científica y académica, y a los principales actores de la actividad privada y gubernamental que diseñan, lideran, implementan y mantienen proyectos y soluciones de telefonía *IP* basada en la nube, proponiendo soluciones y recomendaciones en cada uno de los puntos mencionados.

La **Figura 1**, esquematiza el cambio de modelo y el nuevo paradigma de uso compartido de recursos tanto materiales como humanos.

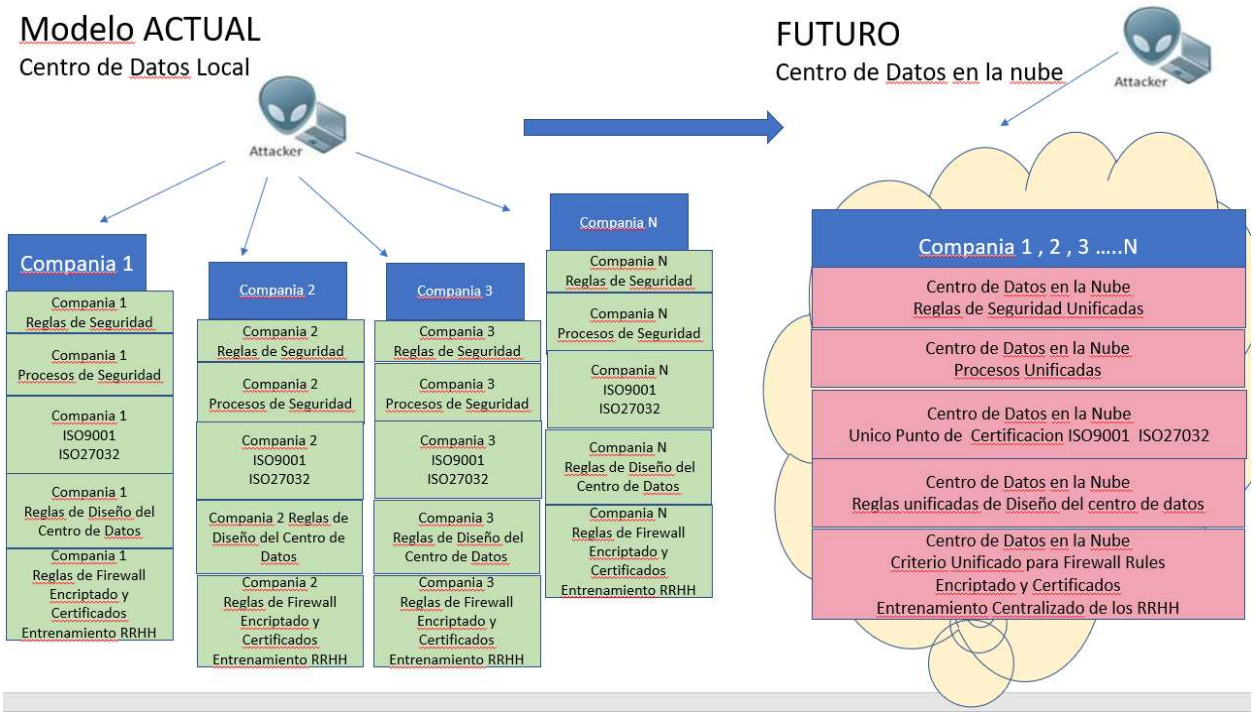


Figura 1. Del modelo actual basado en centros de datos propios a centros de datos en la nube

1.2) METODOLOGÍA.

La metodología de desarrollo del trabajo (Bunge, 1967) se basa en un enfoque mixto con mayor preponderancia de un enfoque cualitativo en cuanto al desarrollo general del trabajo y la investigación del estado del arte apoyado en la experiencia actual en migraciones de sistemas de telefonía privada *IP* hacia la Centros de datos basados en la nube.

El trabajo de investigación consiste en un diseño no experimental enfocado en el análisis de las vulnerabilidades conocidas y/o posibles para cada caso específico de estudio. Luego se analizan las pruebas de concepto en laboratorio técnico de telefonía *IP*, donde se aborda un enfoque cualitativo, comenzando con una recolección de datos, con observación no estructurada, entrevistas abiertas, revisión de documentos, evaluación de experiencias y registro de historias sobre el tema. (Sampieri, 2014).El proceso de indagación es holístico, porque se precia de considerar el todo además de los escenarios particulares.

Esta tesis consta de un desarrollo de marco teórico, el cual comienza con una reseña histórica de la evolución de la telefonía privada desde los sistemas analógicos, pasando por los sistemas digitales hasta llegar a los sistemas *IP*, todos ellos basados en centros de datos localizados en el sitio del usuario hasta la evolución tecnológica que permite migrar toda la infraestructura de telefonía *IP* hacia centros de datos basados en la nube, esto es ubicados geográficamente afuera del sitio del usuario, y permitiendo el crecimiento y adopción de mayores usuarios fuera de ese sitio.

1.3) PROBLEMA DE INVESTIGACIÓN - HIPÓTESIS

Se analizan los riesgos y vulnerabilidades principales, y la situación actual del parque instalado y las predicciones de adopción y crecimiento de esta arquitectura basada en informes recientes para la región de Latinoamérica. El marco teórico incluye una sección dedicada al análisis de los conceptos de quinto dominio, ciberguerra, cibercrimen, y el impacto actual en el tema tratado.

Finalmente, se presenta un detallado análisis de cada uno de los puntos propuestos respecto a los riesgos y las vulnerabilidades que hacen al espacio del problema, la propuesta de solución y la elaboración de la hipótesis que intenta responder los siguientes interrogantes:

¿Cuáles son las nuevas hipótesis de conflicto ante advenimiento de las Telefonía en la nube?

¿Cuáles son los riesgos en ciberdefensa y ciberseguridad, así como las vulnerabilidades de la Telefonía *IP* en la nube y qué medidas preventivas se deben tomar?

¿Cuáles son los riesgos al sumar nuevos servicios (video, chat, almacenamiento, en la nube)?

¿Cuáles son los riesgos de que todas las llamadas telefónicas se desarrollen dentro de la nube y puedan ser grabadas o escuchadas por el proveedor de servicios en la nube?

¿Qué medidas de seguridad son necesarias para prevenir y resguardar la información y contenido de las llamadas?

¿Cuál es el riego de que los paquetes de audio de las llamadas en la nube sean interferidos y capturados en internet?

¿Cuáles son los tipos de cifrado necesarios para voz en modo seguro?

¿Quién es el propietario legal de esa información ante un evento judicial?

¿Qué ocurre en sistemas de entidades públicas y de Gobierno?

¿Cuáles son los tipos de fraude que pueden ocurrir?

La contrastación de dicha hipótesis constituye un capítulo sensitivo de este documento, con pruebas y registros de llamadas telefónicas *IP* basadas en la nube detallando las partes de la información expuestas a riesgos en ciberseguridad, y cuyos resultados constituyen el fundamento esencial de las conclusiones de la tesis y de las recomendaciones para futuros trabajo de investigación relacionados

2) MARCO TEÓRICO.

La creciente utilización del concepto y herramientas asociadas al “quinto dominio”, el mayor número de ciber agresiones entre agente estatales y no estales concretados en dicho espacio y el incremento de requerimientos en materia de ciberdefensa y ciberseguridad que se le adjudica a la generalización del uso de la computación basada en la nube, constituyen el marco general de referencia de este trabajo.

Para el caso específico de la telefonía privada, las empresas y organismos del estado tienen planes para migrar parte de sus telecomunicaciones privadas hacia la nube, y esto se traduce en millones de puertos de Telefonía *IP* funcionando en centros de datos basados en la nube. Estos usuarios irán agregando otros servicios tales como Video, Chat, mail, *SMS* y redes sociales a un único marco de multicanalidad, aumentando así los puertos lógicos de red abiertos en la nube y las vulnerabilidades expuestas.

2.1) LA TELEFONÍA PRIVADA VERSUS LA TELEFONÍA PÚBLICA.

La telefonía privada es aquella que se desarrolla puertas adentro del sitio de la empresa, oficina u organismo. Esto incluye su propia red interna, cableado, dispositivos y equipamiento. Es administrada y mantenida por el dueño de la red. La telefonía pública es aquella que es provista por las empresas proveedores de telecomunicaciones que desarrollan la red pública que permite interconectar la red telefónica nacional, incluyendo su propio cableado y equipamiento hasta la entrada de cada usuario, ya sea particular o empresa. La **Figura 2** detalla esta división conceptual.

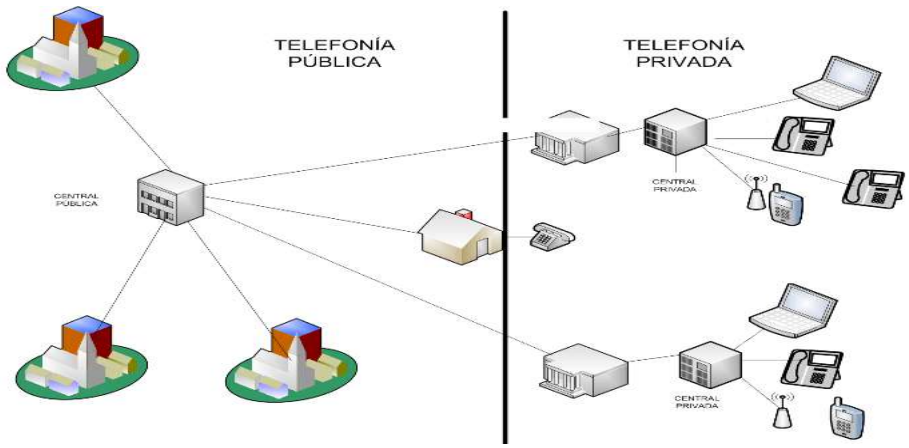


Figura 2. Telefonía Pública – Telefonía Privada

2.2) TELEFONÍA PRIVADA EN SITIO.

La telefonía privada en sitio refiere a la infraestructura telefónica de un organismo donde la conectividad de la red y el procesamiento se realizan íntegramente con equipamiento, dispositivos, servidores y cableado alojados dentro del mismo lugar geográfico donde se desarrollan las actividades del mismo. Su única conexión con el exterior es a través de las líneas telefónicas troncales públicas.

Algunos de los servicios adicionales ofrecidos en la telefonía privada son, la mensajería (correo de voz), conferencias (audio y video), sistemas de reportes, sistemas de grabación, servidores de ruteo y sistemas de respuesta automática e interactiva de voz. La **Figura 3** detalla un sistema básico de telefonía privada desarrollada íntegramente dentro de las instalaciones y sitio de la empresa.

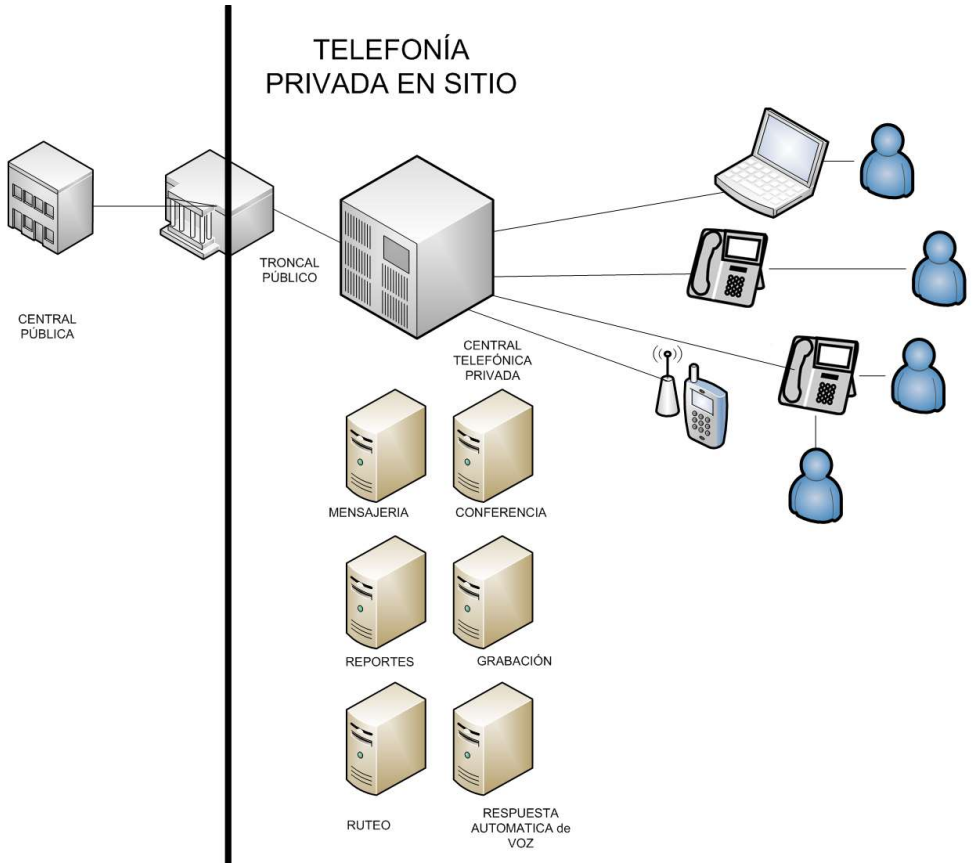


Figura 3 . Telefonía Privada en Sitio.

2.3) EVOLUCIÓN DE LA TELEFONÍA PRIVADA DESE LOS SISTEMAS ANALÓGICOS HASTA LOS SISTEMAS IP.

2.3.1) TELEFONÍA PRIVADA ANALÓGICA / DIGITAL.

Se refiere a la telefonía privada donde los internos telefónicos y/o los troncales públicos se basan en sistemas con señalización analógica (Singer., 2014) y/o digital (Stalling, 2000), estas señales pueden ser enviadas usando cable de par telefónico estándar o cable Coaxial. (Stalling, 2000)

Su particularidad, es que en ambos casos las conexiones van siempre desde el dispositivo hasta la interfase correspondiente en la central telefónica, la cual realizará la conmutación para conectar las llamadas entre las partes que correspondan. Estos teléfonos internos digitales utilizan señalización propietaria para el caso de cada fabricante de telefonía privada.

Los troncales públicos digitales utilizan distintos tipos de tramas digitales y señalizaciones tales como, *T1 ISDN* (usado en EEUU y CANADA), *E1 R2MFC* o *ISDN* (más usados en el resto del mundo). Tanto los troncales analógicos como los internos analógicos utilizan señalización *t*ip *and ring* (Stalling, 2000). La **Figura 4** detallas esta conectividad.

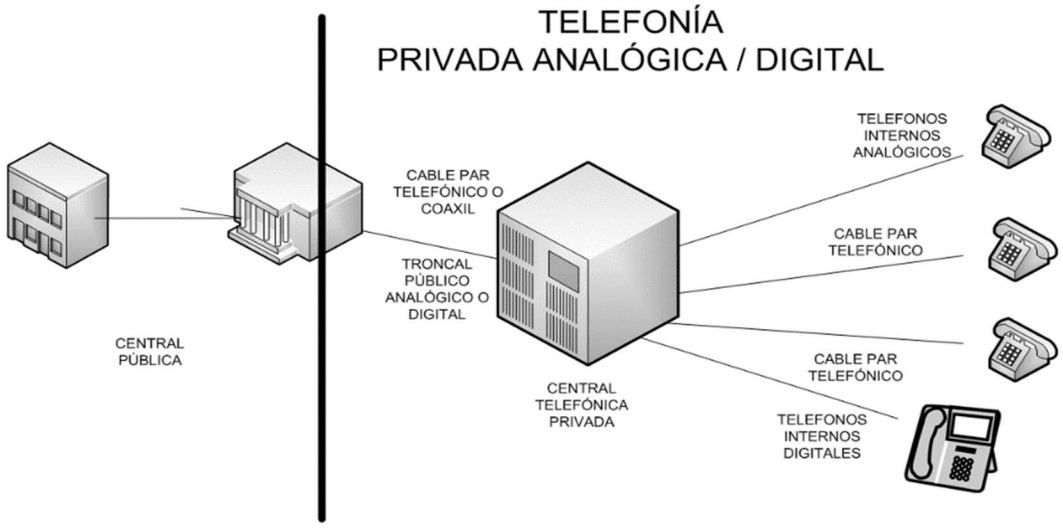


Figura 4. Telefonía privada analógica y Digital

2.3.2) TELEFONÍA PRIVADA *IP.*

A partir del año 1995, junto con el advenimiento del servicio de internet público, las empresas comenzaron a migrar y/o adoptar sus redes internas de datos a redes basadas en el protocolo *TCP /IP*. Este cambio tecnológico fue produciendo una convergencia de las redes de datos y telefonía hacia una única red, en este caso la red telefónica privada tradicional fue migrando a la red de datos *IP*. Esto permitió poder cursar tanto el tráfico de datos y voz por un mismo canal físico.

Para que esto sea posible, se adopta el concepto de telefonía *IP* tanto para líneas troncales como para teléfonos internos. La telefonía *IP* puede cursar el servicio telefónico sobre un canal *TCP / IP*, y esto incluye tanto la señalización necesaria para que el teléfono pueda establecer llamadas, así como la transmisión de la voz, conocida como *Voz sobre IP*.

El medio físico, puede ser cualquiera de los usados para transmisión de datos, en la mayoría de los casos a través de cable de cobre *UTP* o redes inalámbricas. La infraestructura necesaria de transmisión incluye dispositivos tales como *Routers* y *Switches*, que son ahora compartidos por la misma red de datos y telefonía *IP*. La **Figura 5** Detalla una red de Telefonía privada *IP* y sus componentes.

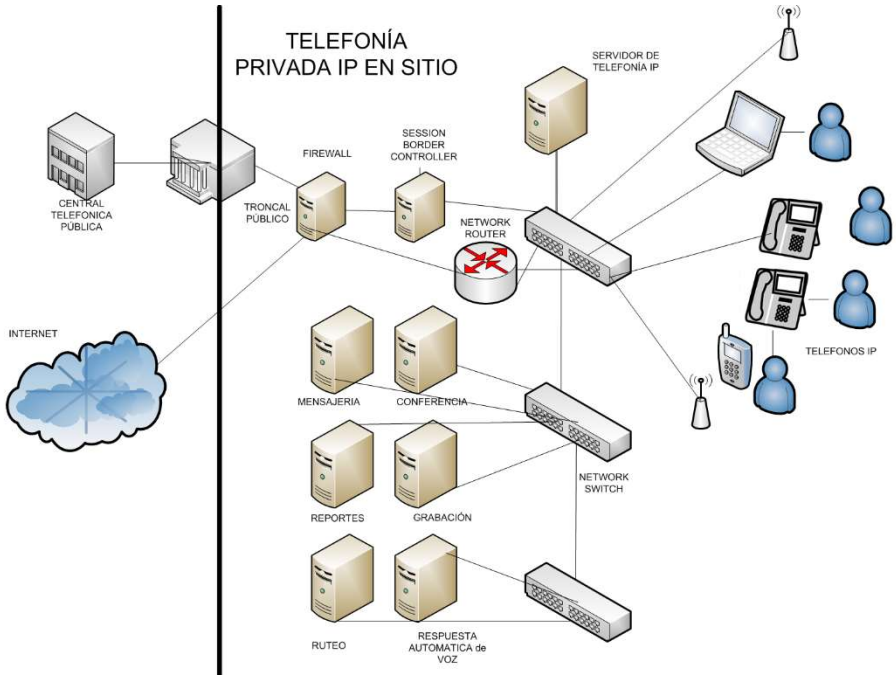


Figura 5. Telefonía privada IP en sitio.

2.3.3) LA TELEFONÍA PRIVADA *IP* EN LA NUBE.

Los avances mencionados anteriormente han hecho posible que los servicios de telefonía *IP* puedan ser ofrecidos desde un Centro de Datos ubicado fuera del sitio y conectado a través de internet. debido al aumento de las velocidades, capacidades y reducción de costos para la transmisión de datos, el aumento de la capacidad de procesamiento de los servidores y del almacenamiento de información. La **Figura 6** detalla el esquema del nuevo escenario de Telefonía *IP* basada en la nube.

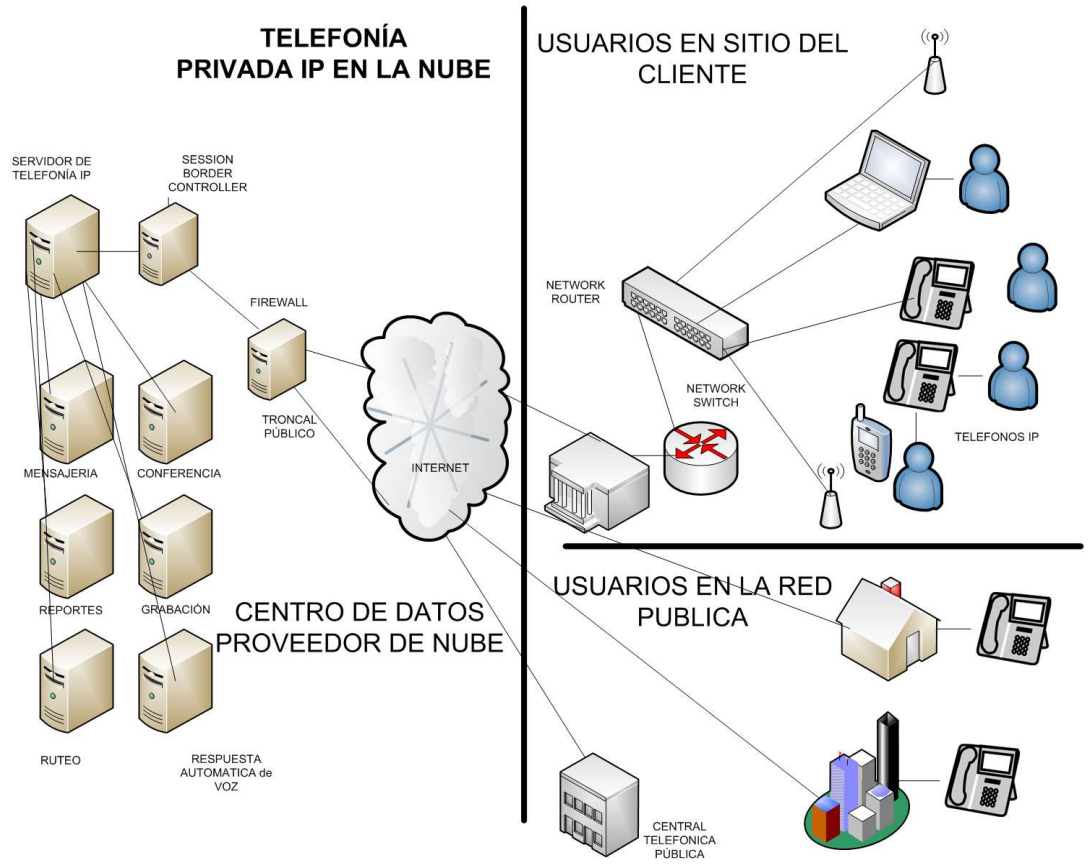


Figura 6. Telefonía Privada IP basada en la Nube

Bajo esta arquitectura de red aparece un nuevo escenario de vulnerabilidades donde cada uno de los teléfonos del organismo debe registrarse en un servidor en la nube, y cada una de las llamadas telefónicas será cursada a través de ese servidor conectado a la red de internet pública. La **Figura 7** detalla los componentes y el flujo de una comunicación de audio de voz sobre la red *IP* en el que se analiza en detalle cada una de las partes de ese recorrido, los riesgos, vulnerabilidades, ventajas, desventajas y oportunidades en lo que respecta a Ciberdefensa y Ciberseguridad.

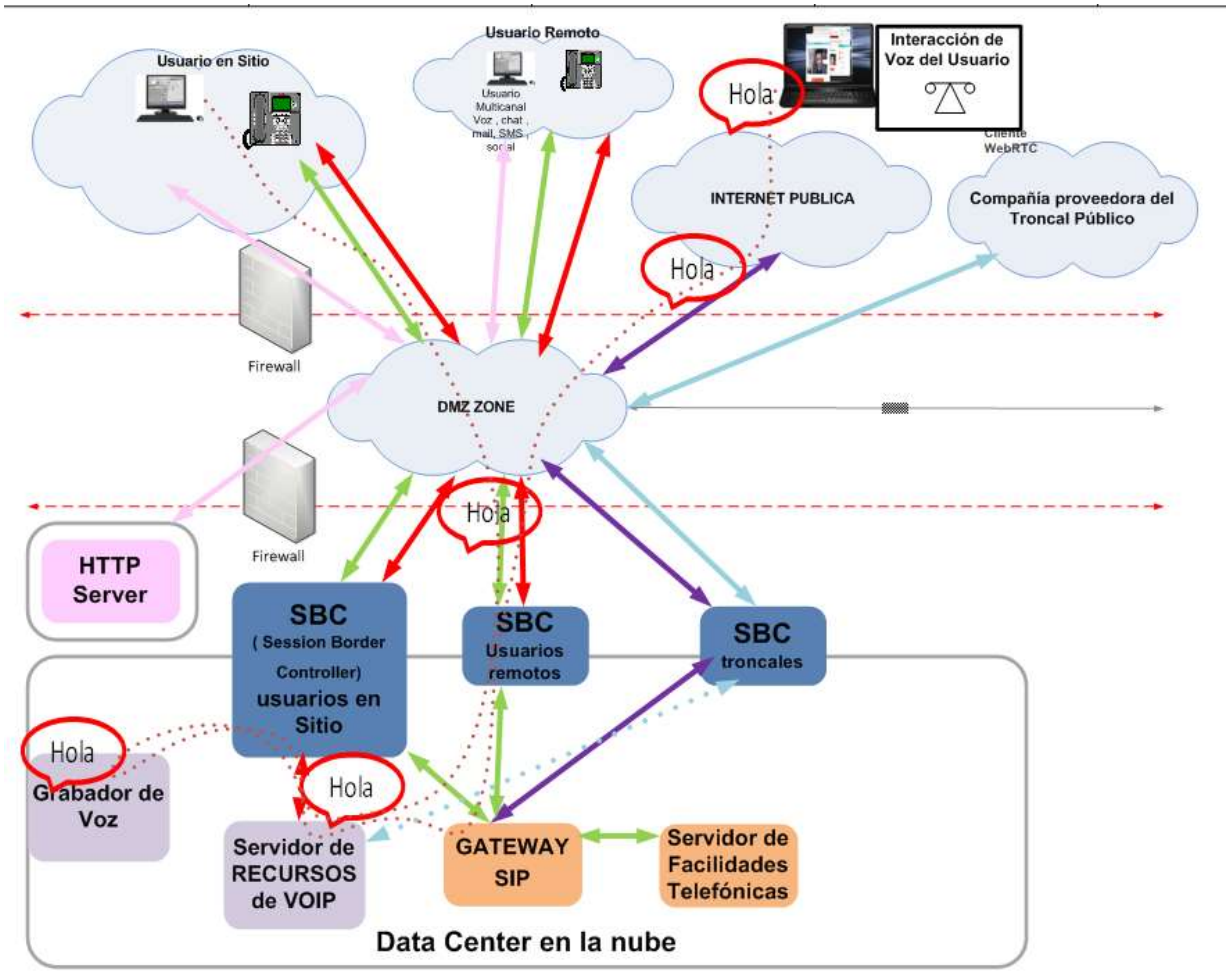


Figura 7. Flujo de la señalización y voz sobre IP para telefonía privada basada en la nube

2.3.3.1) COMPONENTES DE LA TELEFONÍA PRIVADA EN LA NUBE.

- *Teléfonos IP de usuarios fuera de la oficina (Hardphones[1] / Softphones[2] / Móviles)*: Usuarios telefónicos del organismo que están físicamente fuera del sitio y registran sus internos a través de una *IP* pública en Internet.
- *Teléfonos IP de usuarios dentro de la oficina (Hardphones / Softphones / Móviles)*: Usuarios telefónicos del organismo que están físicamente dentro del sitio y registran sus internos a través de una *IP* pública en Internet o una *IP* Privada en el caso de existir una conexión de red privada desde la empresa hacia el proveedor de la nube.
- *Firewalls de Red*: Dispositivos para filtrar el tráfico de red según parámetros configurables tales como puertos, direcciones *IP,* subredes, carga (Payload)[3], contenido, protocolo y tráfico. Además, separa las redes externa e Interna y resulta un dispositivo clave para la ciberseguridad de la telefonía en la nube.
- *SBC para Protocolo SIP (IETF, RFC3261 SIP Session Initiation Protocol, 2019):* Los *Session Border Controllers*, son los dispositivos que reciben todas las registraciones y llamadas de los teléfonos internos y troncales públicos. Luego de los firewalls, son la puerta de entrada para la telefonía *y* esencialmente dividen la red entre la parte pública y la parte privada utilizando diferentes interfaces de red.

  Los SBC manejan:

  - la señalización de teléfonos y llamadas por protocolo *SIP*.
  - las facilidades telefónicas por protocolo HTTP / HTTPs, (IETF, RFC2616 Hypertext Transfer Protocol -- HTTP/1.1, 2019).
  - los paquetes de Voz sobre *IP* por protocolos RTP (IETF, RFC3550 RTP: A Transport Protocol for Real-Time Applications, 2019) / SRTP (IETF, RFC 3711 The Secure Real-time Transport Protoco SRTP, 2019).
  - El protocolo WebRTC (IETF, RFC 7478 Web Real-Time Communication Use Cases and Requirements, 2019) en caso de cursar los paquetes de Voz a través de un Web Browser en tiempo real.

[1] HardPhone es el nombre como se denomina al dispositivo Telefónico físico IP.
[2] Softphone es el nombre genérico de los emuladores de Teléfono IP por software
[3] Payload es el nombre como se conoce al contenido de la información que lleva un paquete de Datos transmitido.

- *HTTP/s file Servers:* Son servidores que contienen los archivos necesarios para que los teléfonos que se conectan a la red puedan bajar sus actualizaciones de software, permisos, certificados y parámetros internos. Como su nombre lo indica, usan protocolo *HTTP/s.*
- *SIP Gateways*: son dispositivos que llevan el control de la registración de cada uno de los usuarios telefónicos, su localización (dirección IP), permisos, validación de certificados de seguridad, configuración, y especialmente el ruteo de llamadas. Es conocido como un servidor "proxy" esto es, que recibe mensajes *SIP* y los renvía al destino solicitado.
- *Servidores de Recursos de VOIP*: Estos dispositivos proveen de los Recursos necesarios para codificar, comprimir y decodificar los paquetes de voz y video sobre *IP* con distintos tipos de compresión según la calidad de voz deseada y el ancho de banda disponible y configurado para ser utilizado en cada llamada telefónica. También llamados *Codecs*[4] de *RTP* / *SRTP*. Maneja el encriptado y desencriptado de paquetes utilizando certificados de seguridad.
- *Servidores de Facilidades*: En la telefonía privada existen múltiples facilidades y servicios que pueden ofrecerse a los usuarios telefónicos tales como la transferencia de llamadas, establecimiento de conferencias de varias partes, grupos de atención aleatorios, permisos y bloqueos de llamadas, ruteo de llamadas a troncales públicas, ruteo de llamadas al sistema de contestador automático general y casillas de correo de voz entre otras funciones que históricamente las realizaba una *PABX*.
- *Troncales IP – SIP desde los Proveedores de Servicios*: Las empresas proveedoras de telefonía ofrecen el servicio de conexión a la red pública a los organismos usuarios de telefonía privada según el tráfico y necesidad del mismo. Para el caso de estudio de la telefonía en la nube, debido a que la conexión será siempre a través de internet, será necesario el uso de troncales *IP* con protocolo *SIP*, que es un estándar mundial descripto en las normas del IEEE (IEEE, 2019) , RFC 3261 (IETF, RFC3261 SIP Session Initiation Protocol, 2019).

[4] Codec: codificadores -decodificadores, que generalmente se usan para pasar convertir paquetes de datos de voz en tiempo real de analógico a digital utilizando distintos tipos de compresión de datos y de la información para poder ser transmitida en el canal disponible.

2.3.3.2) ARQUITECTURA CONSOLIDADA PARA LOS SERVICIOS DE TELEFONÍA BASADOS EN LA NUBE.

Cada uno de los componentes descriptos tiene sus particularidades respecto a vulnerabilidades y riesgos. La **Figura 8**, consolida el diseño de la arquitectura de ciberseguridad de la telefonía basada en la nube y esquematiza los protocolos y puertos expuestos a atacantes en internet.

Este es el punto fundamental y de partida para el análisis en los siguientes capítulos en relación con la ciberdefensa y ciberseguridad de la telefonía desde distintos aspectos posibles, considerando el componente técnico (puertos, protocolos, etc.), las vulnerabilidades de software, las reglas, normas y políticas de seguridad y los ataques cibernéticos.

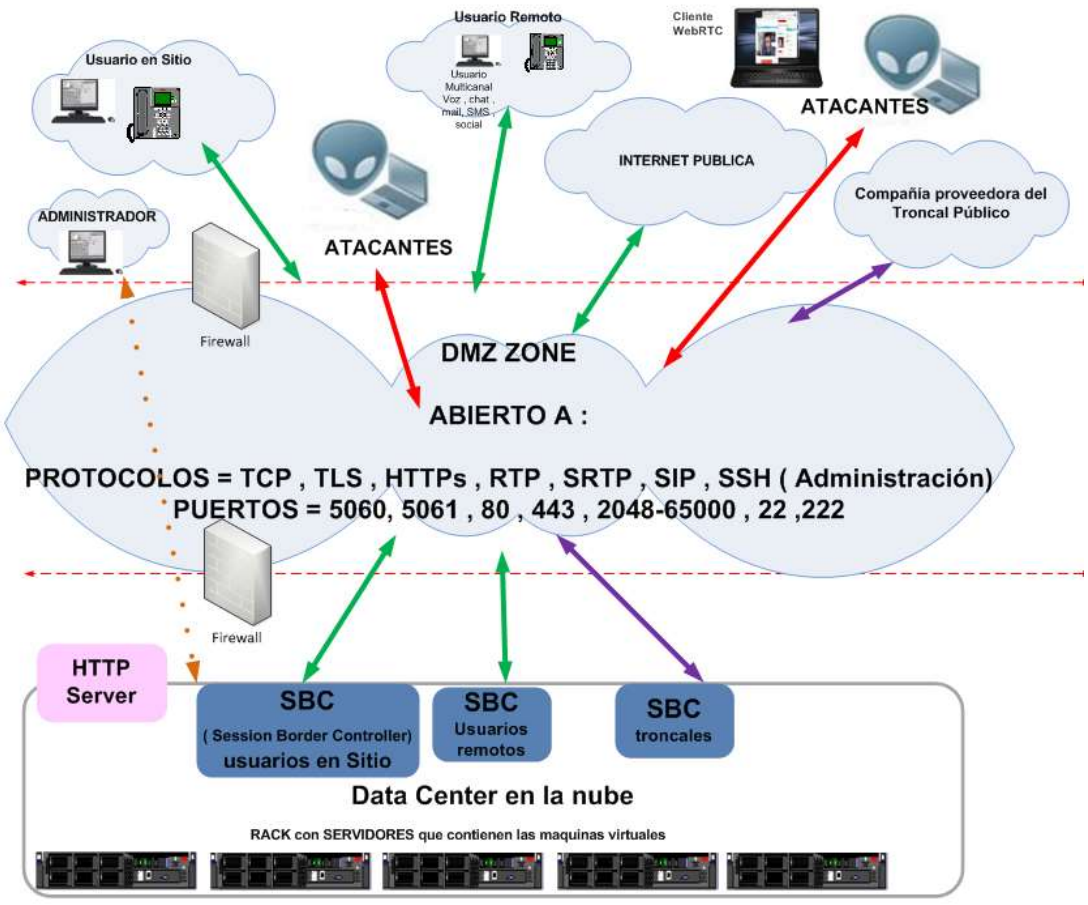


Figura 8. Protocolos y Puertos Abiertos en la arquitectura de Telefonía basada en la nube

2.3.3.3) ARQUITECTURA CONSOLIDADA DE LA TELEFONÍA BASADA EN LA NUBE PARA N CLIENTES EN UN MISMO CENTRO DE DATOS.

Este nuevo escenario de múltiples empresas migrando sus soluciones de telefonía a la nube irá consolidando un esquema con N clientes funcionando en un mismo centro de datos. La hipótesis de riesgo considerando que un ataque a un solo centro de datos puede causar daño a múltiples clientes al mismo tiempo. Este puede ser un ataque tanto al sitio físico como a la red del centro de datos.

En este sentido, dada la importancia que adoptan esos sitios y las redes involucradas deberían ser considerados parte de la infraestructura crítica de un país. La **Figura 9** detalla conceptualmente este escenario donde eventualmente muchos clientes pueden compartir no solo el mismo Centro de Datos , sino también el hardware asociado (servidores, firewalls, etc.).

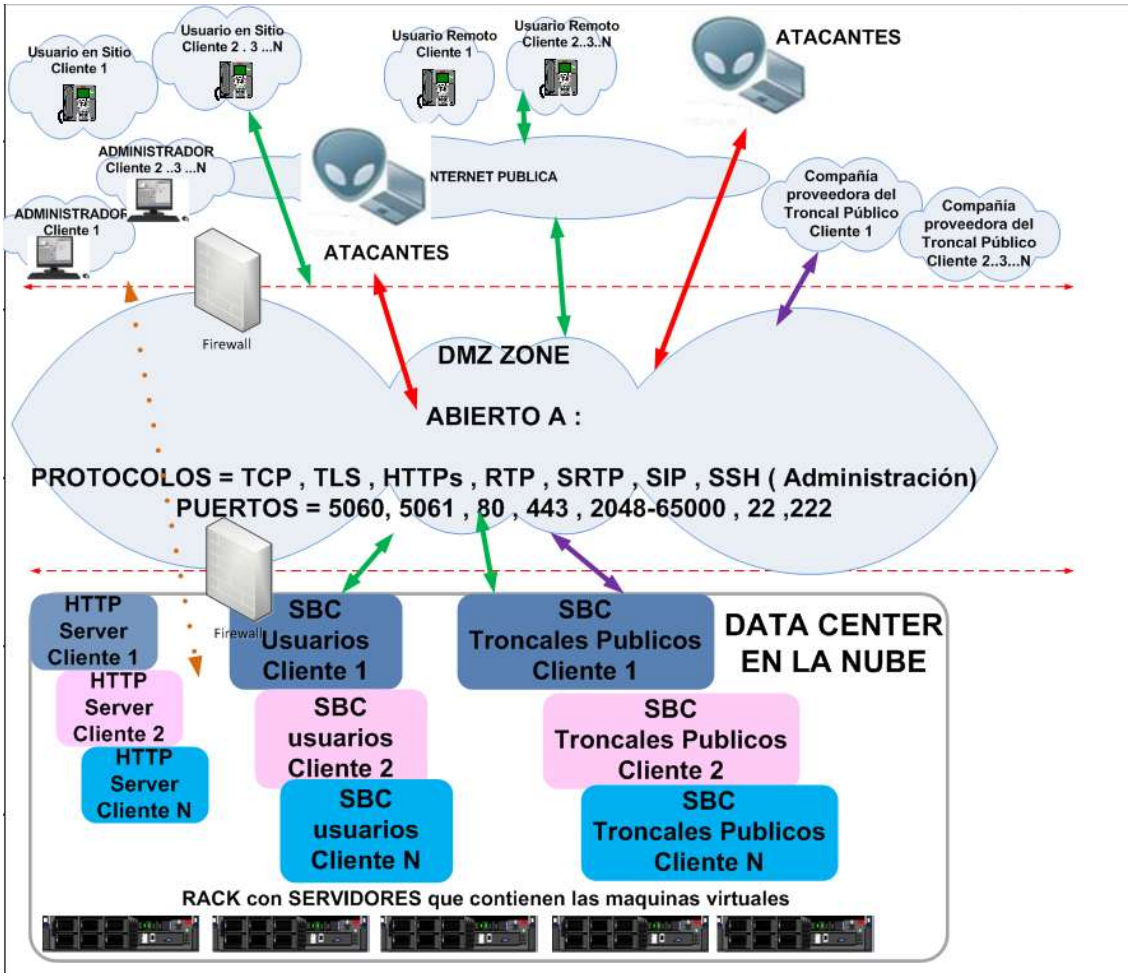


Figura 9. Arquitectura de Telefonía basada en la nube para N Clientes en un mismo Centro

2.3.3.4) ARQUITECTURA CONSOLIDADA DE LA TELEFONÍA BASADA EN LA NUBE PARA N CLIENTES EN UN MISMO CENTRO DE DATOS CON REDUNDANCIA GEOGRÁFICA.

Como parte de la arquitectura de telefonía basada en la nube, los sistemas cumplen con las capacidades de redundancia y alta disponibilidad para poder dar continuidad al servicio en caso de caída del sistema debido a desastres naturales, pérdida de conexión con el sitio, ataques al sitio físico, ataques de denegación de servicio, defecto de alguno de sus componentes principales y otras causas. La **Figura 10** sintetiza esta arquitectura detallando los dos centros de datos ubicados en sitios geográficos distantes y donde los usuarios pueden conectarse a cualquiera de ellos según la disponibilidad requerida.

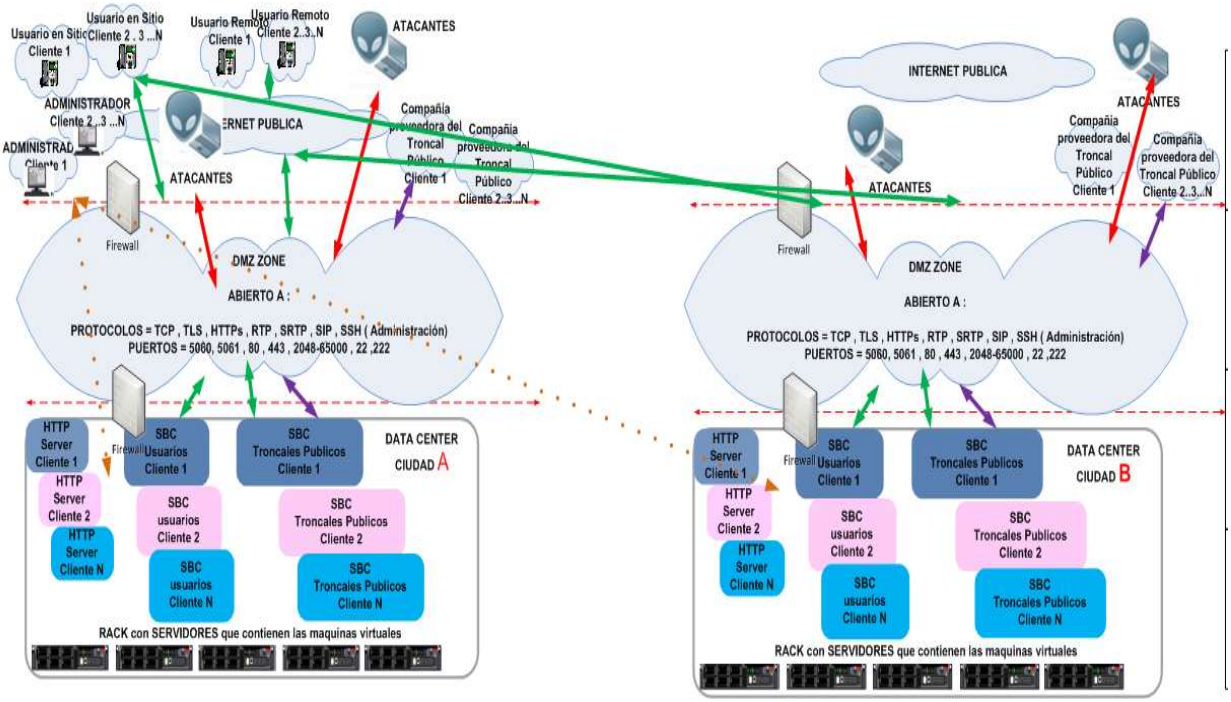


Figura 10. Arquitectura de Telefonía basada en la nube con Redundancia Geográfica

2.4) CIBERESPACIO Y GUERRA HÍBRIDA EN EL QUINTO DOMINIO.

El uso intenso de la *Red de Redes* ha generado un espacio virtual (denominado "quinto dominio" (Singer., 2014)) en el que se desarrollan aspectos sensitivos de la economía mundial, en el que también se han desarrollado muy significativamente las comunicaciones globales y, desafortunadamente, en el mencionado espacio virtual o ciberespacio, encuentran un ámbito propicio de concreción de agresiones entre estados naciones y también en las variantes más peligrosas del crimen organizado transnacional.

Ciberdefensa y ciberseguridad han devenido en cuestiones prioritarias tanto para los líderes gubernamentales como para los máximos responsables de corporaciones empresariales y también de organizaciones no gubernamentales. (Clarke, 2010). Existen casos tales como el del ciber financiamiento del terrorismo y el ciber lavado transnacional de activos en los cuales, desafortunadamente, existen indicios de un cierto "amparo" por parte de estados naciones. Muchas veces agentes gubernamentales han tratado de mimetizar sus ciber agresiones como provenientes de agentes no gubernamentales. También viene al caso mencionar que esas ciber agresiones provenientes de estados naciones han tenido como blancos a corporaciones empresariales privadas. (Diogenes, 2018).

2.5) IMPACTO DE LA CIBERDEFENSA y CIBERSEGURIDAD EN EL SERVICIO DE TELEFONÍA BASADA EN LA NUBE.

A medida que crece la cantidad de empresas que migran sus sistemas de telefonía a la nube y aumentan la cantidad total de puertos instalados, aumenta el riesgo de seguridad y ataques cibernéticos. El tipo de arquitectura en la nube hace posible el acceso desde cualquier ubicación geográfica en el mundo, tanto para los usuarios reales como para los atacantes.

2.5.1) IMPACTO EN ASPECTOS DE CIBERDEFENSA.

En el punto 2.3.3.3) se detalla la arquitectura de nube donde muchos clientes confluyen en un único centro de datos. Para el caso de las entidades de gobierno que migran, están concentrando en uno o dos puntos geográfico todas sus entidades, dependiendo del proveedor elegido, como puede observarse en la Figura 10.

Estos centros de datos quedan expuestos a ser blanco de ataque al sitio, así como a la conexión de fibra que lo conecta con el exterior. Este ataque resultará en una pérdida del servicio de telefonía de todos los organismos que estén instalados en ese sitio, activando el sistema de redundancia y disponibilidad de emergencia que el centro de datos pueda disponer. No solo los servicios de telefonía se ven afectados sino también la información que se guarda en relación a la misma tales como llamadas realizadas, horarios, fechas, grabaciones e información de usuarios.

2.5.2) IMPACTO EN ASPECTOS DE CIBERSEGURIDAD.

Como se observa en la **Figura 9,** se detalla un resumen de los protocolos y puertos abiertos y disponibles a ataques cibernéticos tanto por hackers individuales como por grupos de ataque persistentes conocidos como APT (Daly, 2009). Los principales ataques a la ciberseguridad de los servicios de telefonía en la nube conocidos y reportados están relacionados con el robo de credenciales de usuarios telefónicos para luego realizar llamadas telefónicas sin costo, también los ataques de denegación de servicio DOD (Diogenes, 2018) cuyo impacto es la caída total o parcial de los servicios. Generalmente estos ataques se realizan emulando múltiples registraciones falsas de teléfonos desde varios sitios utilizando *Bots* (Daly, 2009) o múltiples intentos de realizar llamadas simultáneas causando un inusual tráfico en los dispositivos de entrada *SBC.*

Sumados a estos riesgos, existe la posibilidad de interceptar los paquetes de voz sobre *IP* que no usen *SRTP* a través de métodos de captura de datos tales como *Port Mirroring*[5] o puerto espejo (Estrada, 2011) en *Switches* de capa 2, duplicación de direcciones *MAC* o el uso de múltiples registraciones de teléfonos *SIP*, los cuales permiten varias registraciones y la suplantación de identidad telefónica. Estas situaciones de suplantación de identidad (en este caso telefónica) crean el ámbito para luego desarrollar ataques conocidos como *Vishing* (Services, 2007) , que consta en realizar una llamada telefónica emulando la voz de quien no es. Se han reportado casos de *Vishing* [6]principalmente originados por sistemas de Inteligencia artificial basados en grabaciones de voz de la persona, en los que se crean sus patrones de comportamiento para llevar a cabo una conversación emulando su voz y así lograr una llamada fraudulenta, por ejemplo, llamando a un servicio de banca telefónica constituyendo un fraude financiero.

[5] *Port Mirroring* es el nombre como se conoce a la acción de configurar un puerto de un *Switch* de datos para que copie en espejo la actividad de otro puerto.

[6] *Vishing* es el nombre como se conoce a la técnica de emular la voz para simular que habla el usuario real.

Otro de los puntos de riesgo, es el cifrado utilizado tanto para la señalización *SIP* o *HTTP*s así como para los paquetes de *Voz sobre IP*. Para ellos los sistemas utilizan distintos tipos de cifrados y encriptación tales como *TLS, TLSv1, TLSv2, AES-256, DES*, todos ellos como parte del porfolio de algoritmos de cifrado. Sera vital prevenir el robo o copia de certificados de seguridad que puedan ser usados para desencriptar paquetes de Voz sobre *IP* o registrar teléfonos con suplantación de identidad.

La **Tabla 1** detalla los modos de ataque y los problemas causados para cada tipo de ataque en los servicios de telefonía. Estos casos serán analizados en el Capítulos 3 y 4 (Soluciones, Implementación y Análisis).

#	Tipo de Ataque	Modo de Ataque	Problema causado
1	Ataque de denegación de servicio (*DOS- Denial of Service*).	Múltiples y simultáneos solicitudes de conexión hacia los puertos abiertos para registración de teléfonos *IP*.	Caída del servicio – imposibilidad de realizar llamadas telefónicas.
2	Intento de Registrar usuarios desde personas no habilitadas e Intentos de realizar llamados telefónicos no autorizados.	Solicitudes de Registro de usuarios, probando con múltiples usuarios y contraseñas hasta encontrar un usuario válido.	Usuarios no autorizados pueden realizar llamadas telefónicas causando costos extras y riesgo de llamadas no deseadas.
3	Suplantación de identidad.	Teléfonos registrados usando credenciales robadas pueden realizar llamadas o atender en nombre de otro usuario.	Robo de llamadas de larga distancia *VISHING*. Grabación no autorizada de llamadas.
4	Robo de Certificados de Seguridad.	Teléfonos registrados usando credenciales robadas pueden realizar llamadas o atender en nombre de otro usuario. Captura de Datos en la red.	Robo de llamadas de larga distancia *VISHING.* Grabación no autorizada de llamadas Desencriptado de paquetes de Voz sobre *IP*.

#	Tipo de Ataque	Modo de Ataque	Problema causado
5	Captura de Paquetes de Voz.	*Port Mirror.*	Escucha ilegal de llamadas.
6	Ataque físico al Sitio del Proveedor de Nube Ataque físico a la conectividad de fibra del sitio.	Ataque físico – criminal Corte de Fibra óptica.	Caída del servicio – imposibilidad de realizar llamadas telefónicas. Robo o perdida de la información de usuarios y/o grabaciones de llamadas.
7	Acceso vía puertos de administración a la red interna privada y a los servers de infraestructura.	Ataques cibernéticos en sus distintos modos para ingreso indebido junto al uso de *Ransomware,* M*alwares*, virus y P*ishing.*	Desde caída total del servicio, robo y perdida de la información, hackeo total de los dispositivos y llamadas.

Tabla 1. Impacto a la Ciberseguridad en los servicios de telefonía basada en la nube.

2.6) PROTOCOLO *SIP*. FUNCIONES BÁSICAS.

El protocolo *SIP* funciona en la capa de aplicaciones según el modelo *OSI* y está definido por el *RFC3261* según la *IEEE.* Es usado principalmente para inicio de sesiones de telefonía IP y estas sesiones pueden ser de voz, video, chat o simplemente intercambiar información a través de un área libre definida como *SDP* en el cuerpo del mensaje. Al funcionar dentro de la capa de aplicación permite independencia de las capas anteriores, esto es del medio físico y protocolos de comunicación en capas 2 y 3 y transporte en capa 4. Se basa en un modelo de *REQUEST / RESPONSE*, esto es que están definidos una lista de mensajes de *REQUEST,* que siempre tienen un *RESPONSE* basado en grupos de mensajes previamente definidos por el protocolo.

El protocolo *SIP* tiene definidos variados procesos y métodos en distintos *RFCs*, como por ejemplo el *RC3515*[7] que define el método *REFER* para transferencias de llamadas. Este trabajo se

[7] https://tools.ietf.org/html/rfc3515

enfoca en el marco teórico necesario para solamente dos de los procesos más importantes, com son, el proceso de registración y autenticación de teléfonos *SIP (REQUEST = REGISTER)* y el establecimiento de una llamada tanto de teléfonos como de troncales *(REQUEST = INVITE).*

El estudio de estos métodos provee las bases para focalizar los aspectos relacionados a la ciberseguridad y riesgos expuestos según la Tabla 1.

2.6.1) REGISTRACIÓN DE TELÉFONOS *IP.*

El proceso básico de registración de un teléfono *IP SIP* en la red consta de la siguiente secuencia mensajes según la **Figura 11.**

Figura 11. Secuencia de señalización SIP de Registración de Teléfonos IP

En el primer mensaje "REGISTER" desde el teléfono hacia el Servidor de Registración vemos algunos datos importantes tales como la *IP* de origen, puerto UDP de origen, número de interno y usuario, clave de acceso, tipo de teléfono *IP* usado como puede observarse en la **Figura 12.**

Figura 12. Información y Datos dentro del mensaje de REGISTER de SIP.

El servidor *SIP* responde aceptando la registración e incluye información relevante tal como *IP* y puerto de origen, modelo del servidor, horario y dominio de *SIP*, como se detalla en la **Figura 13.**

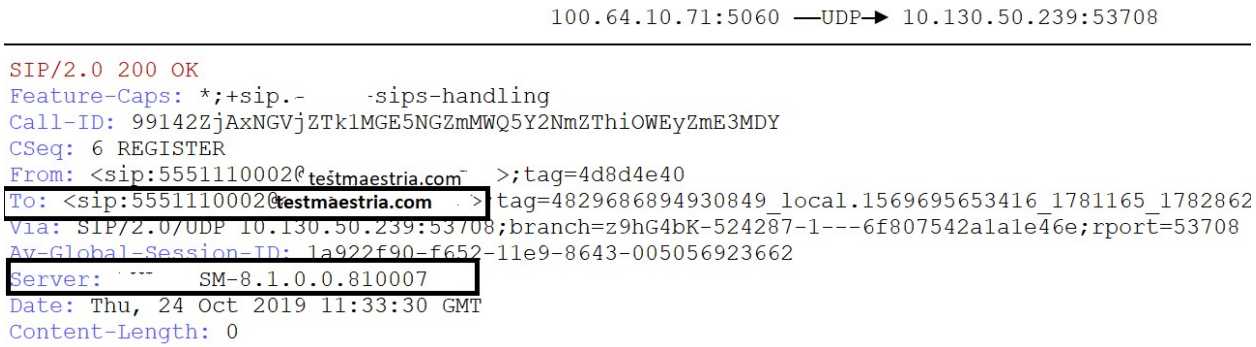


Figura 13. Información y Datos dentro del mensaje de aceptación de la Registración SIP.

Para concluir con la registración, el servidor *SIP* guarda la *IP* de cada usuario en el *location service*[8] para poder ubicarlo en futuras llamadas. La **Figura 14** detalla el proceso de registración y como se guarda la *IP* de cada teléfono.

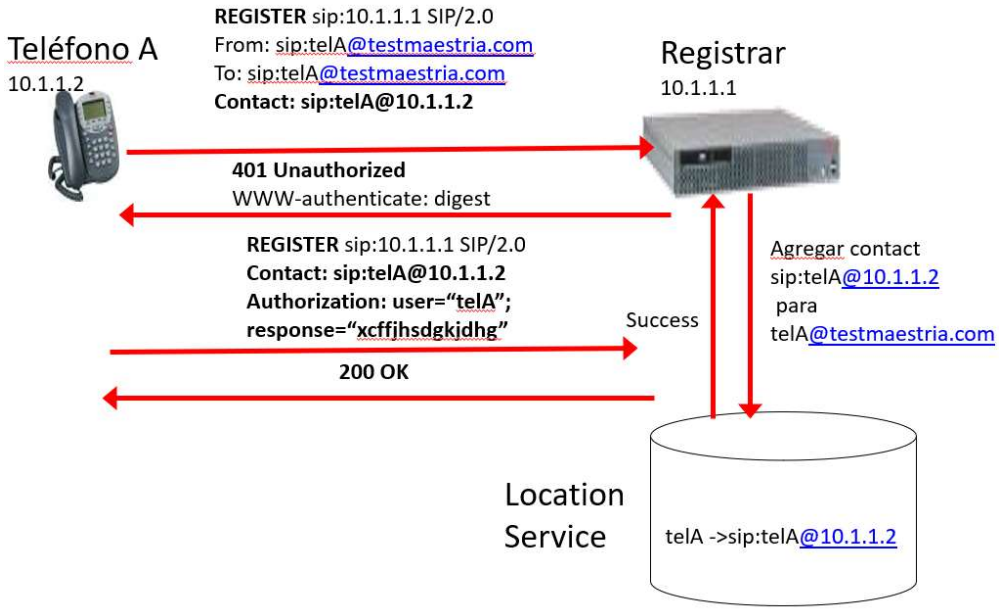


Figura 14. Secuencia de Registración de un usuario SIP.

[8] Location Service es el nombre como se conoce a la tabla dentro del SIP gateway que guarda la información de la dirección IP de cada usuario.

2.6.2) LLAMADAS TELEFÓNICAS IP.

El Proceso básico para establecer una llamada telefónica desde un Teléfono *IP* o troncal *SIP* en la red consta de la siguiente secuencia relevado en las pruebas de laboratorio de acuerdo a la **Figura 15.**

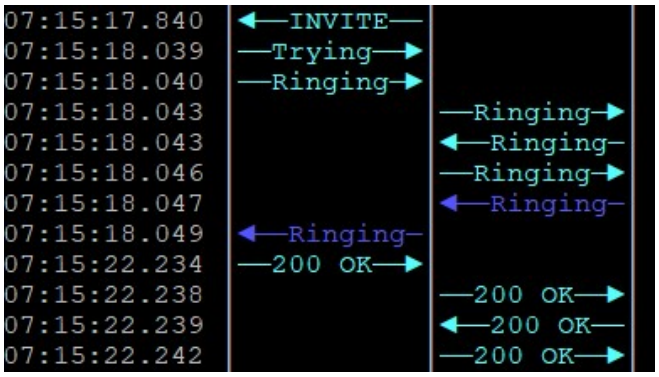


Figura 15. Secuencia de mensajes de un llamado Telefónico con señalización SIP.

La secuencia detalla los mensajes de *INVITE, Trying, Ringing y 200 OK* cuando la llamada es atendida. La **Figura 16** detalla la información relevante en el mensaje de INVITE para establecer la llamada incluyendo IP, puertos de origen y destino para señalización, *IP* usada para los paquetes de *voz sobre IP*, y método de compresión del audio.

```
                                        10.130.50.239:63953 —UDP→ 100.64.10.71:5060
INVITE sip:+155511100001@testmaestria.com SIP/2.0
Via: SIP/2.0/UDP 10.130.50.239:63953;branch=z9hG4bK-524287-1---d95ef75ae1c62959;rport
Max-Forwards: 70
Contact: <sip:5551110002@10.130.50.239:63953;rinstance=015320839a25f571>
To: <sip:+155511100001@testmaestria.com >
From: <sip:5551110002@testmaestria.com >;tag=22ebb110
Call-ID: 99142M2NlOGIzMzgzMDY2MGE3YTAzZmQ5ZjNiZWZlN2IyMTU
CSeq: 1 INVITE
Allow: OPTIONS, SUBSCRIBE, NOTIFY, INVITE, ACK, CANCEL, BYE, REFER, INFO
Content-Type: application/sdp
Supported: replaces
User-Agent: X-Lite release 5.6.1 stamp 99142
Content-Length: 336

v=0
o=- 13216393638006368 1 IN IP4 10.130.50.239
s=X-Lite release 5.6.1 stamp 99142
c=IN IP4 10.130.50.239
t=0 0
m=audio 61338 RTP/AVP 9 8 120 0 84 101
a=rtpmap:120 opus/48000/2
a=fmtp:120 useinbandfec=1; usedtx=1; maxaveragebitrate=64000
a=rtpmap:84 speex/16000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
```

Figura 16. Información y Datos dentro del mensaje de INVITE de SIP.

La **Figura 17** detalla el mensaje *200 OK* cuando la llamada es atendida incluyendo información de *IP* y puertos de señalización del receptor, lista de direcciones IP por donde han pasado los mensajes[9], sistema operativo del *Softphone* receptor, *IP*, puerto y tipo de compresión usada para los paquetes de voz sobre *IP*.

```
SIP/2.0 200 OK
From: "Station, 555111000?" <sip:+15551110002@testmaestria.com ;tag=9f33515af65941e9a5ef0505692b9d7
To: <sip:+15551110001@testmaestria.com ;tag=a099db4d-c54f-45c5-ad01-430711662816
Call-ID: 9f33516ef65941e9a5f00505692b9d7
CSeq: 1 INVITE
Via: SIP/2.0/TLS 100.64.10.71;branch=z9hG4bK782173335346709-AP;ft=9
Via: SIP/2.0/TLS 127.0.0.2:15061;branch=z9hG4bK782173335346709;rport=16307;ibmsid=local.1569695653416_1783947
Via: SIP/2.0/TLS 127.0.0.2:15061;branch=z9hG4bK544000829910654;ibmsid=local.1569695653416_1783946_1785697
Via: SIP/2.0/TLS 100.64.10.71:5071;branch=z9hG4bK9f33515af65941e9a5ef0505692b9d71-AP;received=100.64.10.71;rp
Via: SIP/2.0/TLS 100.64.10.11:5071;branch=z9hG4bK9f33515af65941e9a5ef0505692b9d71;      -reaction=shor
Via: SIP/2.0/TLS 100.64.10.71:5071;branch=z9hG4bK465423365121726-AP;ft=150858
Via: SIP/2.0/TLS 127.0.0.2:15061;branch=z9hG4bK465423365121726;rport=19862;ibmsid=local.1569695653416_1783945
Via: SIP/2.0/TLS 127.0.0.2:15061;branch=z9hG4bK391757681427946;ibmsid=local.1569695653416_1783944_1785695
Via: SIP/2.0/TLS 100.64.10.71:5071;branch=z9hG4bK9f335830f65941e9a5f10505692b9d7-AP;received=100.64.10.71;rpo
Via: SIP/2.0/TLS 100.64.10.11:5071;branch=z9hG4bK9f335830f65941e9a5f10505692b9d7
Supported: eventlist,outbound,replaces
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
User-Agent.          /3.0 (3.6.4.31.2;      CSDK; Microsoft Windows NT 6.2.9200 Service Pack 1)
Contact: <sips:5551110001@10.130.50.239:13936>;+sip.instance="<urn:uuid:0839ca66-9abc-4a22-b969-19549cda8696>
Accept-Language: en
Record-Route: <sips:SM1NAR1@100.64.10.71;transport=tls;lr;av-asset-uid=14b3a3da>
Record-Route: <sips:127.0.0.2:15061;lr;ibmsid=local.1569695653416_1783946_1785697>
Record-Route: <sip:SM1NAR1@100.64.10.71:5071;transport=tls;lr;av-asset-uid=14b3a3da>
Record-Route: <sip:SM1NAR1@100.64.10.71:5071;transport=tls;lr;av-asset-uid=14b3a3da>
Record-Route: <sip:127.0.0.2:15061;transport=tls;lr;ibmsid=local.1569695653416_1783944_1785695>
Record-Route: <sip:SM1NAR1@100.64.10.71:5071;transport=tls;lr;av-asset-uid=14b3a3da>
Record-Route: <sip:100.64.10.11:5071;transport=tls;lr>
P-Conference: OutdialPrompt=false, FeedbackPrompts=false, UCCP=true, Video=false, WebCollaboration=true
Content-Type: application/sdp
Content-Length:   230

v=0
o=sips:5551110001@10.130.50.239 4 2 IN IP4 10.130.50.239
s=-
c=IN IP410.130.50.239
b=TIAS:64000
t=0 0
a=activetalker:1
m=audio 5012 RTP/AVP 0 101
a=sendrecv
a=rtpmap:0 PCMU/8000/1
a=rtpmap:101 telephone-event/8000
```

Figura 17. Información dentro del mensaje de aceptación de llamadas en señalización SIP.

[9] De mucha utilidad para resolver el "problema de la atribución" mediante las técnicas de backtracing que es el nombre como se conoce a esta acción en el ámbito de la ciberdefensa.

2.7) ADOPCIÓN DE LA TELEFONÍA BASADA EN LA NUBE.

Según el reciente informe de GARTNER Inc (Gartner, 2019) la adopción de los servicios de Telefonía y computación en la nube se ha visto demorada debido a los cuidados necesarios en materia de ciberseguridad que requiere este tipo de arquitectura, muchas veces temores exagerados han causado demoras y pérdidas de oportunidades. Es importante la implementación de un programa de manejo del riesgo que cumple con las cinco condiciones preestablecidas de agilidad, disponibilidad, seguridad, viabilidad del proveedor de nube y cumplimiento de las regulaciones legales.

Los analistas del mencionado reporte estiman que para el año 2025, el 90% de las organizaciones fallará en el control de la nube pública y el uso inapropiado de datos sensitivos y esto requerirá un especial énfasis en desarrollar estrategias de seguridad e implementación en la nube. Otro de los puntos esperados es la eliminación progresiva del uso de contraseñas de autenticación, que serán reemplazadas paulatinamente por sistemas de reconocimiento biométrico.

Según el reporte privado, correspondiente al año 2019 realizado Frost & Sullivan acerca del estado, oportunidades y planes de migración de las 500 empresas más importantes de Latinoamérica para los servicios de telefonía privada basada en la nube, (Sullivan, 2019) , los tres factores que influyen a la hora de decidir la migración son la oportunidad de obtener flexibilidad , reasignación de recursos y la provisión de facilidades avanzadas en telefonía, mientras que el atributo de confiabilidad es el más importante, seguido por la seguridad y el costo.

Actualmente el 20% de las empresas detalladas en el informe han migrado parte de su telefonía a soluciones basadas en la nube, el 37% de ellas tienen planes de migración y estarían dispuestos a hacerlo en los próximos dos años y un 16% argumentó qué debido a los temores en la seguridad de la solución, no tienen aún planes de adoptar esta arquitectura.

3) INVESTIGACIÓN, IMPLEMENTACIÓN y SOLUCIONES

En el presente capítulo se realiza el análisis detallado de cado uno de los siete puntos descriptos en la Tabla 1, respecto al impacto a la ciberseguridad en la telefonía en la nube *y* por cada uno de ellos se detalla:

i. Resumen del problema.
ii. Pruebas, Contrastación y/o demostraciones en laboratorio técnico.
iii. Las soluciones propuestas a implementar para la mitigación de riesgos y contrastación de la hipótesis. Finalmente, los resultados consolidados en el análisis final elaborado en el capítulo 4, y las conclusiones del capítulo 5.

3.1) ATAQUE DE DENEGACIÓN DE SERVICIO POR MÚLTIPLES SOLICITUDES DE REGISTRACIÓN DE TELÉFONOS *IP*.

Los problemas #1, #2, #3 y #4 especificados en la **Tabla 1**, se encuentran interrelacionados al momento de realizar un análisis y pruebas de concepto, por ello que se realiza el estudio y análisis en una misma sección.

3.1.1) RESUMEN DEL PROBLEMA.

Como se describe en la sección 2.6.1), el proceso básico de registración de un Teléfono *IP SIP* en la red consta de la siguiente secuencia mensajes según la **Figura 18.**

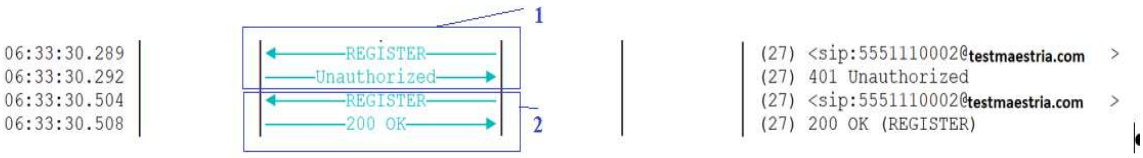


Figura 18. Registración de Teléfonos IP indicando los 2 mensajes de REGISTER

Esto significa dos mensajes de pedido de registración por cada teléfono *IP*, donde este teléfono puede estar ubicado en cualquier lugar con acceso a internet. El tiempo de cada registración es de aproximadamente 200 milisegundos. Esta solicitud de registración la realiza el

teléfono indicando la dirección *IP* o *DNS* del servicio de telefonía *IP* alojado en su proveedor de nube y que es recibido por el SBC, quien luego envía la solicitud al Gateway *SIP*. La **Figura 19** muestra esta situación con múltiples registraciones de teléfonos *IP* recibidas en el SBC luego de pasar por el firewall de red.

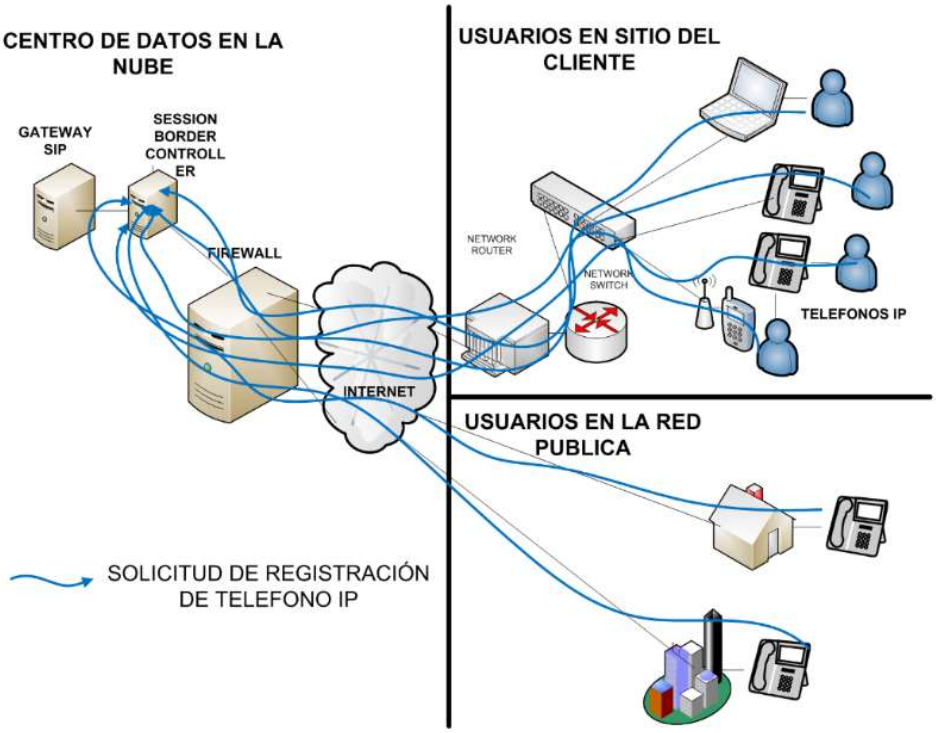


Figura 19. Múltiples Registraciones de Teléfonos IP

En este ejemplo las registraciones llegan desde diferentes dispositivos que puedan representar a un teléfono *IP SIP,* tales como, teléfonos de escritorio, teléfonos emulados por software o dispositivos móviles, en todos los casos a través de internet. Estas registraciones ocurren cada vez que un nuevo teléfono se conecta a la red y en cada una de ellas envían entre otros datos, la dirección *IP* del teléfono, su número de usuario y contraseña. Según el protocolo *SIP*, cada teléfono reenvía automáticamente una nueva registración antes que se cumpla el tiempo de expiración pactado en la primera, normalmente cada una hora, aunque este tiempo puede ser configurado por el administrador del sistema.

Esta información puede observarse en la **Figura 20** que es una captura de pantalla de un trazado tomado desde la consola de comando en tiempo real.

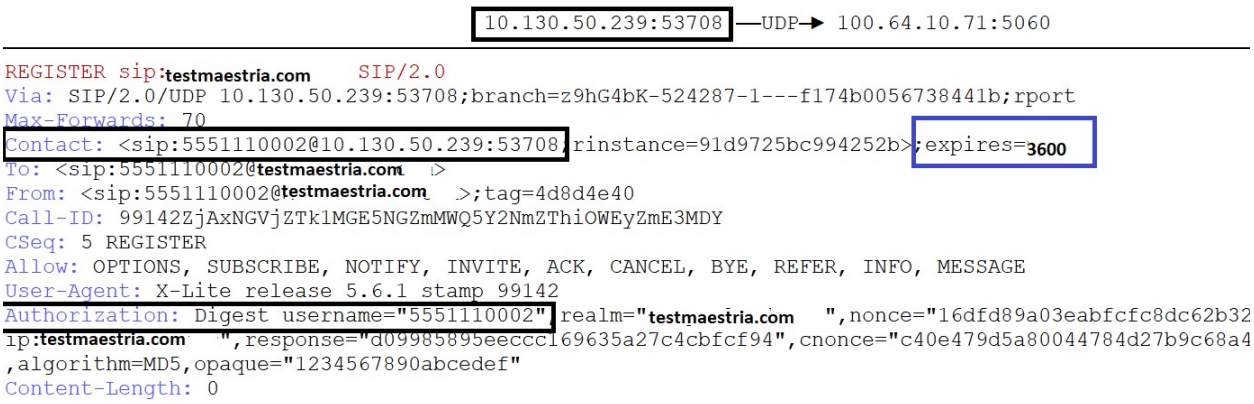


Figura 20. Información y Datos dentro del mensaje de REGISTER de SIP.

El servidor *SIP* responde aceptando la registración o denegando la misma. La **Figura 21** detalla cuando el pedido de registración es denegado por usar credenciales no autorizadas.

Figura 21. Registración no Autorizada

Los dispositivos que reciben estas solicitudes pueden procesar una cantidad finita de registraciones simultáneas. Este valor puede variar según la capacidad y performance del dispositivo según los datos del fabricante. Como mínimo debe estar preparado para soportar un evento de múltiples registraciones de todos los usuarios al mismo tiempo, pues es un evento que podría ocurrir luego de una falla generalizada por cualquier motivo que requiera que todos los teléfonos deban hacerlo al mismo tiempo.

Se analiza qué sucede en un sistema con 4000 teléfonos donde en un periodo de 10 segundos se envían todas las registraciones asumiendo una distribución de probabilidad de arribo uniforme durante ese periodo y cada una demora 200ms.

$$Registraciones\ Simultáneas = Cantidad\ de\ Telefonos/10\ Segundos * 0.2\ Segundos$$

Como resultado, el sistema debe procesar 80 solicitudes de registración en el mismo instante.

La **Figura 22** describe este escenario con un ataque distribuido de múltiples solicitudes de registración desde distintos sitios en la red que provienen de sistemas automáticos del tipo *Bots* que generan falsos pedidos de registración, en cantidades que podrían exceder la capacidad de procesamiento de los dispositivos.

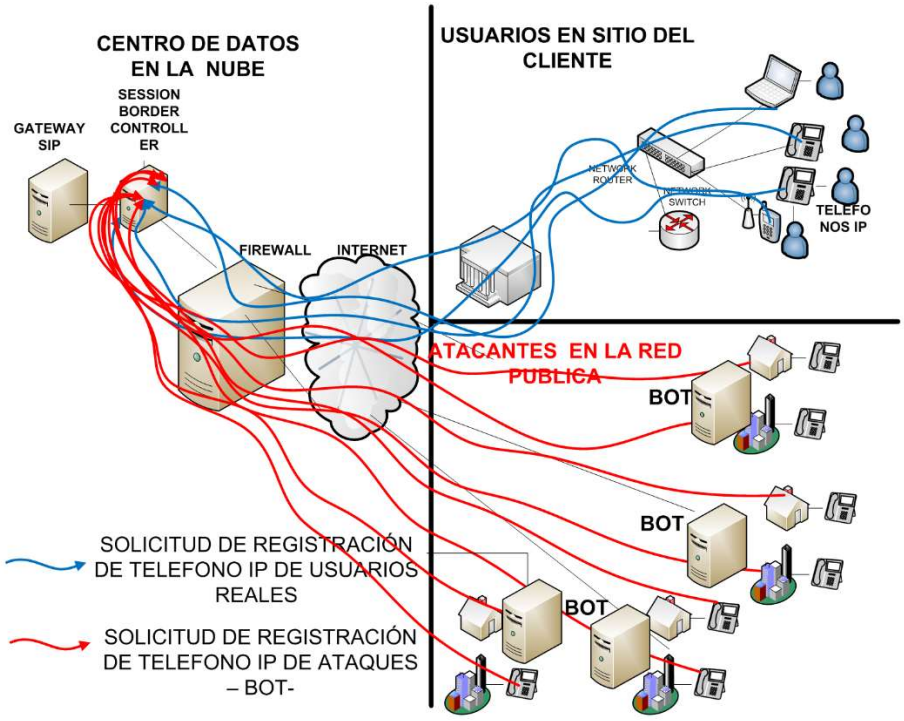


Figura 22. Ataque con Múltiples Solicitudes de registraciones

Si los *Bots* generan 20000 registraciones en un periodo de 10 segundos y asumiendo una distribución de probabilidad de arribo uniforme durante ese periodo el resultado sería:

$$Registraciones\ Simultáneas = Cantidad\ de\ Telefonos\ /\ 10\ Segundos * 0.2\ Segundos$$

Como resultado, el sistema debe procesar ahora 400 solicitudes en el mismo intervalo de tiempo, excediendo el tráfico esperado causando una posible caída del sistema, permitiendo generar una alarma de posible ataque en curso.

3.1.2) PRUEBAS Y DEMOSTRACIONES DE LABORATORIO TÉCNICO EN CAMPO. CONTRASTACIÓN DE LA HIPÓTESIS. ANÁLISIS DE LAS POSIBLES VULNERABILIDADES Y RIESGOS EN CIBERSEGURIDAD.

3.1.2.1) PRUEBAS DE REGISTRACIÓN. CAPTURA DE EJEMPLOS REALES DE ATAQUES DE SOLICITUDES NO AUTORIZADAS DE REGISTRACIÓN.

Usando una maqueta de pruebas donde el sistema de registración esta conectado a una *IP* pública, se observó que con frecuencia se reciben solicitudes falsas de registraciones de teléfonos *IP* con credenciales falsas ya sea de número de usuario, contraseña o dominio de *SIP* que son rechazadas. En esta prueba se observó que la dirección *IP* de origen estaba geográficamente en Holanda, en un sitio donde no hay usuarios autorizados. También se observó que las solicitudes eran ejecutadas periódicamente y cambiando el nombre de usuario en cada solicitud.

La **Figura 23**, muestra una captura de pantalla en la que se observan ataques persistentes, generando aleatoriamente falsas solicitudes de registración entre 15 y 25 segundos y probando con un número de usuario diferente en cada oportunidad. Si bien un intento de registración con esa periodicidad no es considerado un DDOS, el atacante podría reducir el tiempo entre intentos y afectar el normal funcionamiento del servicio.

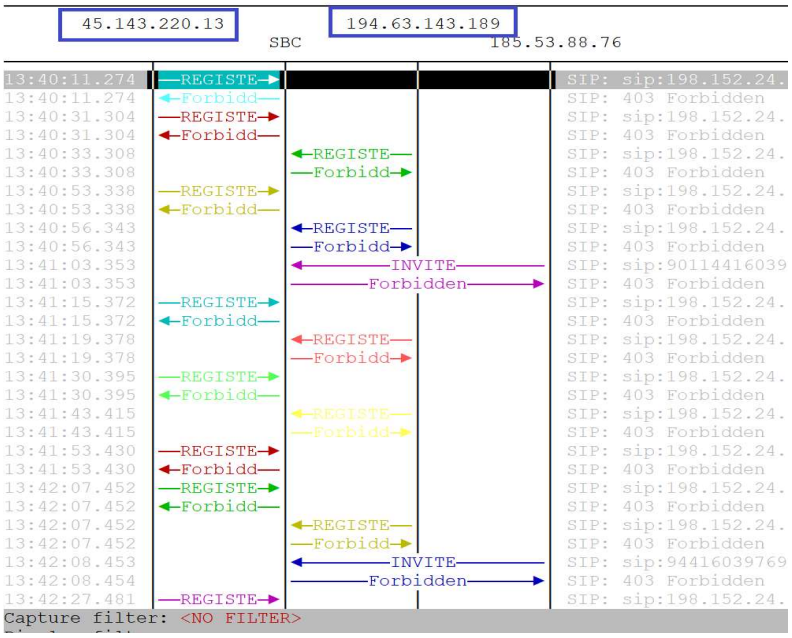


Figura 23. Captura de Red sobre SBC con ataques de Registración SIP.

3.1.2.1) CAPTURA DE EJEMPLOS REALES DE ATAQUES DE REGISTRACIÓN.

En la **Figura 24.** se muestra el detalle de un mensaje de registración utilizando el usuario 3001, inexistente en el sistema. Este intento corresponde a lo detallado en el Problema #2 de la Tabla 1.

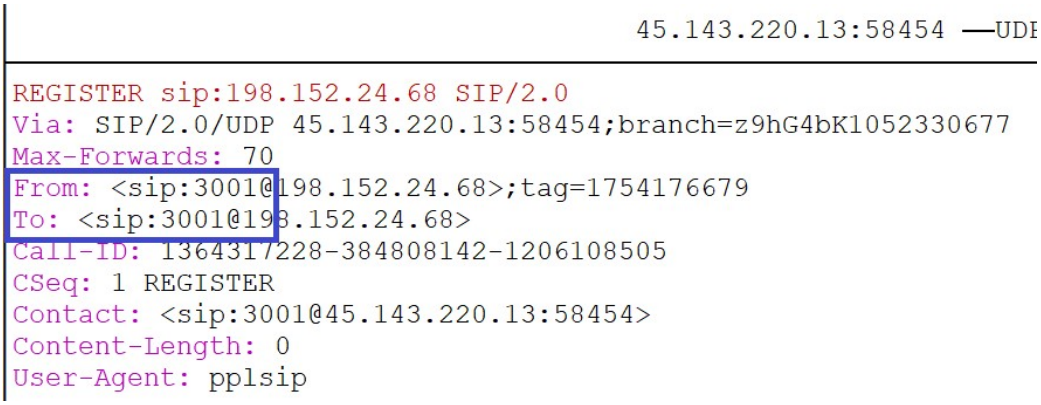


Figura 24. Intentos de Registración de usuario no existente

3.1.2.2) ANÁLISIS DE PROCEDENCIA DE DIRECCIÓN *IP*.

La **Figura 25** muestra el resultado del análisis de la *dirección IP* de procedencia del ataque realizado a través del sitio whois.com [10] en el mes de octubre del año 2019, observándose que *esa dirección* provenía geográficamente de subredes asignadas a proveedores de internet en la ciudad de Ámsterdam, Holanda, donde no se contaba con usuarios de prueba.

[10] https://who.is/whois-ip/ip-address/45.143.220.13

Figura 25. Trazabilidad de la IP de ataque

3.1.2.3) CAPTURA DE EJEMPLOS REALES DE ATAQUES DE LLAMADAS.

Una situación similar se presentó con ataques desde sitios no autorizados que intentaban realizar llamadas telefónicas en intervalos de 10 a 20 segundos como se observa en la **Figura 26**, las cuales fueron rechazadas por el sistema en el laboratorio de pruebas. Se recibieron intentos desde sistemas *Bots* con direcciones *IP* localizadas en China, Estados Unidos de América y Rusia.

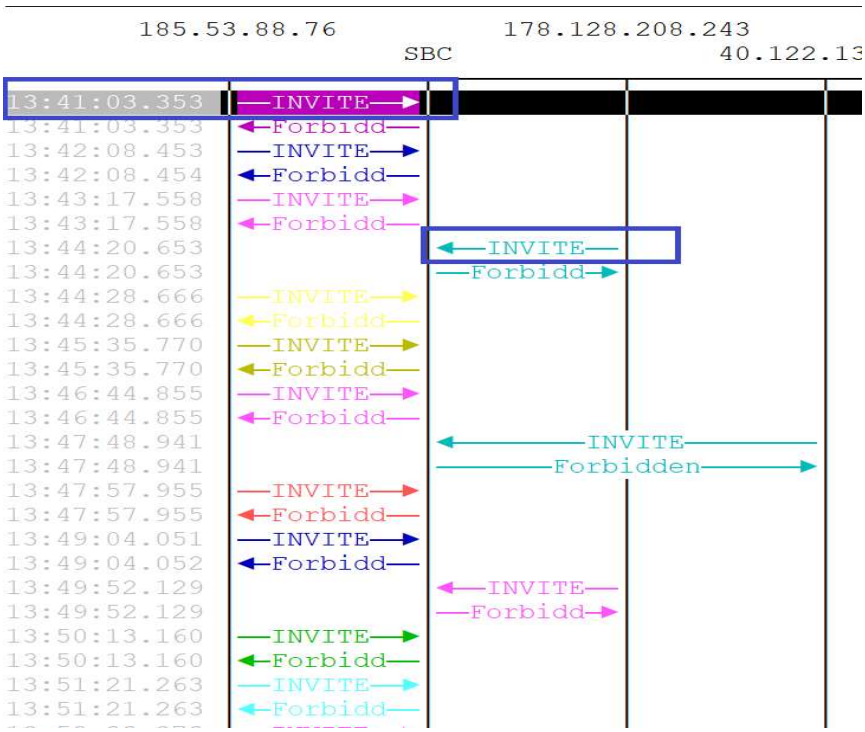


Figura 26. Ataque continuo de intentos de llamadas telefónicas

En este caso particular de la **Figura 27**, se registra un intento de llamada internacional a Gran Bretaña que luego fue rechazado. Si la registración hubiera sido exitosa usando credenciales falsas , como lo describe el Problema #3 de la Tabla 1, estaríamos ante un caso de *Spoofing* (Dean, 2010) donde el atacante podría realizar las llamadas como si fuera un usuario real.

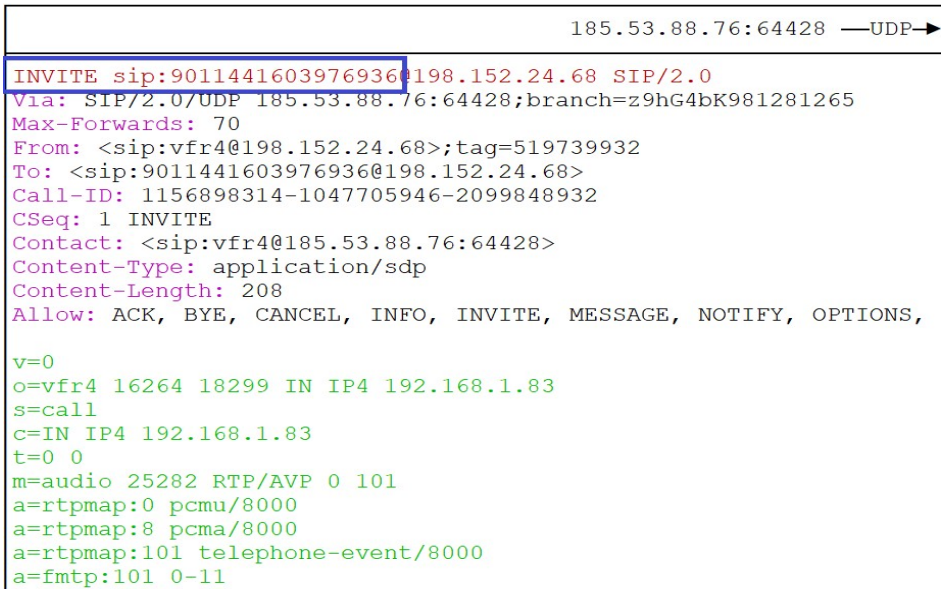


Figura 27. Captura de intento de llamada internacional

3.1.2.4) CERTIFICADOS DIGITALES. PRUEBAS DE REGISTRACIÓN EN LABORATORIO.

El uso de Certificados de Seguridad digitales provee una instancia inicial para la registración de usuarios previa al dialogo por señalización *SIP*.

La **Figura 28** detalla una registración real con el uso de certificados digitales, este certificado ha sido creado por una autoridad de certificación y luego se ha creado un certificado de identidad para el dispositivo especifico que recibe el pedido. Luego es instalado en el teléfono o dispositivo que realiza la registración. Se observa que la secuencia de intercambio de credenciales digitales entre el teléfono y el servidor ocurre antes de comenzar la registración *SIP*.

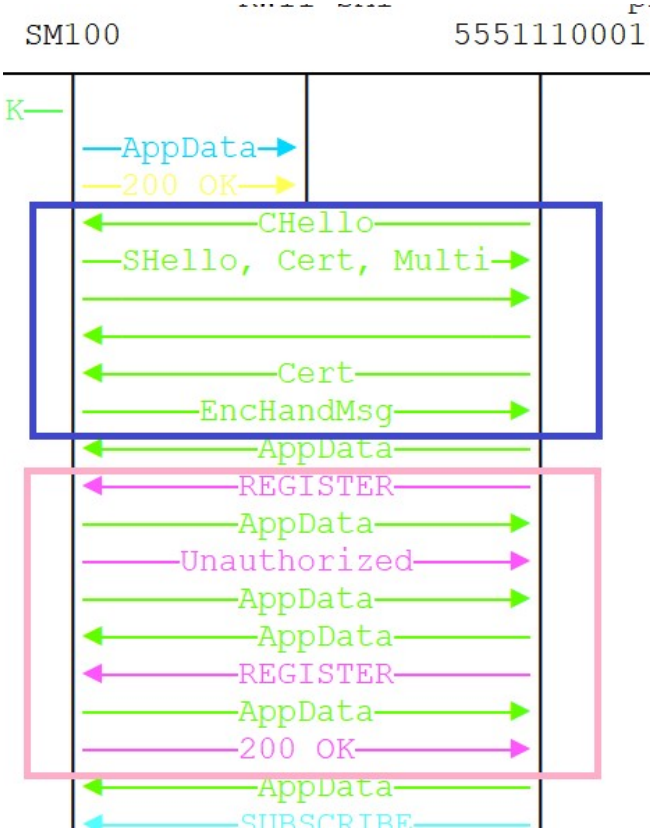


Figura 28. Intercambio de Certificado de Seguridad digital

Luego en el detalle del mensaje del certificado se observa que este es enviado a través del puerto 5061, utilizando *TLS*.

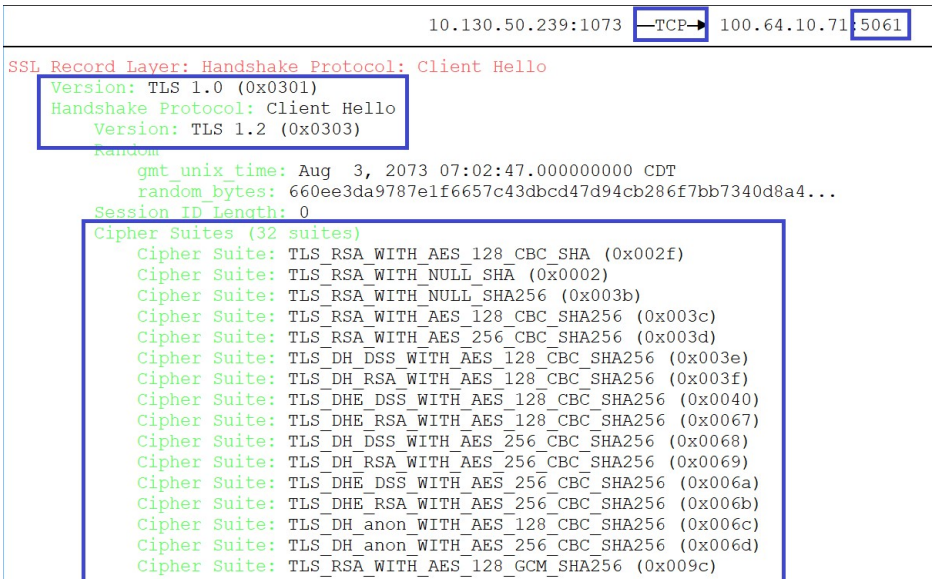


Figura 29. Detalle del Certificado

Como contraprueba, se intenta registrar un teléfono sin certificados y como resultado se observa en la **Figura 30,** que falla el proceso de intercambio de certificados digitales y la señalización *SIP* no se inicia con el mensaje de REGISTER.

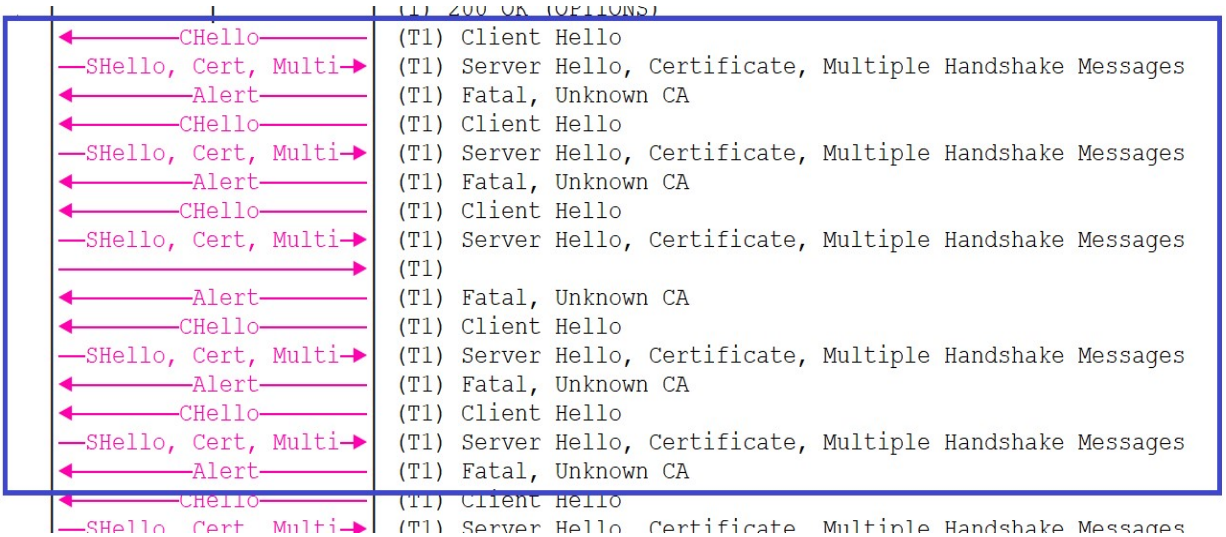


Figura 30. Falla de Certificado desconocido.

3.1.3) SOLUCIONES PROPUESTAS A IMPLEMENTAR PARA LA MITIGACIÓN DEL RIESGO ASOCIADO.

3.1.3.1) SOLUCIONES PROPUESTAS A ATAQUES DE DDOS.

Luego del análisis y las pruebas efectuadas, se aprecia que la solución de este problema se basa en encontrar el equilibrio para que los sistemas de detección y bloqueo puedan discriminar el tráfico de usuarios reales frente al malicioso evitando falso positivos. **La Figura 31** esquematiza la problemática a resolver.

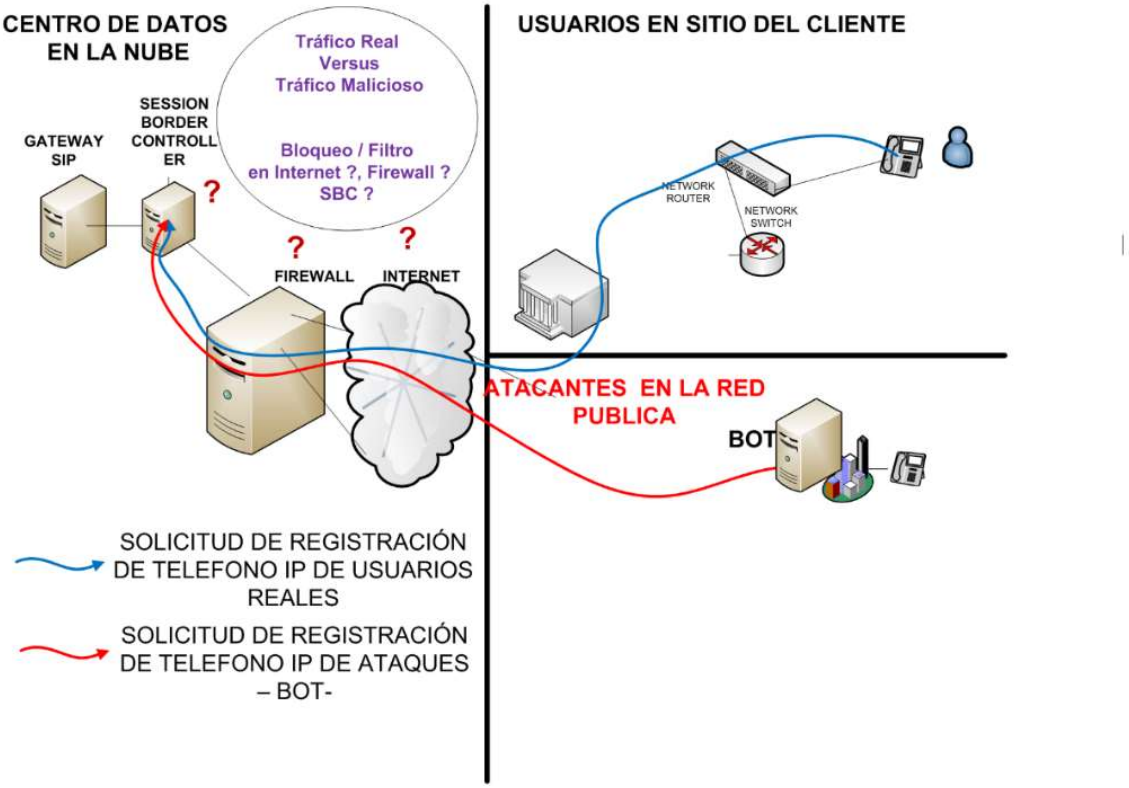


Figura 31. Tráfico Real versus tráfico malicioso - Puntos de Bloqueo

Para este caso particular, cabe señalar que el protocolo SIP se desarrolla en la Capa 7 del modelo OSI (capa de aplicación) en el SBC, el que debe estar configurado para aplicar la solución de bloqueo. Existen distintas formas de *DOS (Denegación de Servicio)* y para cada una de ellas se debe usar una lógica y un cálculo distinto para evaluar que tráfico bloquear y cuando bloquearlo.

La siguiente **Tabla 2**, consolida los valores recomendados para bloqueo de ataques DDOS según las mejores prácticas de configuración de un SBC. (AVAYA, 2019) , valores que se toman como referencia para las pruebas de concepto y laboratorio detalladas en la siguiente sección.

TIPO DE DENEGACIÓN DE SERVICIO	**TIPO MENSAJE *SIP***	**UMBRAL**	**INTERVALO**
DOS Fuente única hacia Interfase *SIP*	Todos los mensajes *SIP*	>300	5 segundos
DDOS Fuente Distribuida hacia dispositivos	Todos los mensajes *SIP*	>200	3 segundos
DDOS sigilosa hacia interfase *SIP*	*INVITE* *REGISTER*	Promedio 5 intentos	2 minutos
DDOS Rueda de Reconocimiento hacia interfase *SIP*	INVITE REGISTER	10 mensajes	1 minuto
DDOS Fuente Distribuida hacia un Server	Todos los mensajes *SIP*	>1700	10 segundos 10 segundos

Tabla 2. Valores Recomendados para bloqueo de distintos tipos de ataques DDOS

3.1.3.1.1) DENEGACIÓN DE SERVICIO DESDE UNA FUENTE ÚNICA.

Se refiere al caso donde el *DOS* se genera desde un único punto, todos los mensajes de ataque llegan desde una única dirección *IP*. En este caso se considera que el umbral de bloqueo debe ser mayor a la cantidad de mensajes en situaciones de registración o llamadas de teléfonos reales. Se estableció en el sistema de pruebas un valor de bloqueo cuando los mensajes *SIP* son mayores a 300 mensajes en 5 segundos, según lo determinado en la **Tabla 2**.

3.1.3.1.2) DENEGACIÓN DE SERVICIO A UN DISPOSITIVO ESPECÍFICO DESDE UNA O VARIAS FUENTES.

Se refiere al caso donde el *DOS* se dirige a un teléfono o dispositivo en particular. En este caso se considera que el umbral de bloqueo debe ser mayor a la cantidad de mensajes que puede recibir un teléfono en situaciones reales de recepción de llamadas o avisos de mensajes internos. Los valores de referencia pueden variar según el fabricante del dispositivo, es por ello qué es recomendable realizar capturas de prueba antes de configurar esos umbrales a fin conocer el tráfico de mensajes y realizar el ajuste para encontrar un balance adecuado y evitar falsos positivos.

Los valores iniciales de bloqueo deben fijarse para una cantidad de mensajes *SIP* mayor a 200 en 3 segundos, según lo determinado en la **Tabla 2**.

3.1.3.1.3) DENEGACIÓN DE SERVICIO SIGILOSA DESDE UNA O VARIAS FUENTES de ATAQUE.

Es el caso donde el ataque se produce desde una o varias fuentes distribuidas desconocidas cuando la cantidad y frecuencia de los mensajes son bajas, para sigilosamente explorar los puertos de entrada y vulnerabilidades, probando nombres y contraseñas de usuarios.

En este caso se considera que el umbral de bloqueo debe ser mayor a la cantidad de mensajes en situaciones de registración o llamadas de teléfonos reales en los que se pueda identificar este patrón sigiloso de reconocimiento.

Los valores iniciales de alerta se configuran para un umbral donde la cantidad de mensajes de intentos de violación son de un promedio de 5 intentos en intervalos de 2 minutos. según lo determinado en la **Tabla 2**.

3.1.3.1.4) DENEGACIÓN DE SERVICIO POR "RUEDA DE RECONOCIMIENTO" DESDE FUENTE ÚNICA.

Se refiere al caso donde el ataque proviene desde una fuente única y realiza un intento de ataque a un grupo específico de usuarios y luego se detiene una vez terminada su fase de reconocimiento y colección de datos. La **Figura 32** muestra una captura en línea del sitio web shodan.io (shodan, 2019), el cual realiza una rueda de reconocimiento para encontrar dispositivos SBC en la red , en este caso envía un mensaje SIP = OPTION , utilizando la respuesta *403 Forbidden* como prueba de que en esa dirección IP hay un dispositivo SBC.

Figura 32 Ejemplo de reconocimiento de dispositivos SBC en el sitio shodan.io

Los valores de bloqueo se configuran para un umbral donde la cantidad de mensajes *SIP* desde una fuente única hacia un grupo de usuarios es de 10 mensajes por minuto, 5 mensajes de *INVITE* o 5 mensajes *REGISTER* por minuto. según lo determinado en la **Tabla 2**.

3.1.3.1.5) DENEGACIÓN DE SERVICIO DESDE HACIA UN SERVER INTERNO.

Se refiere al caso donde el ataque proviene desde una fuente única o distribuida, que una vez realizada la "rueda de reconocimiento" logra conocer las *IP* de otros servidores de la infraestructura y envía ataques direccionados a bloquear el servicio del *Server* mismo.

Los Valores de bloqueo en este caso varían según la capacidad y cantidad de teléfonos con los que cuenta el sistema y se debe calcular en cada caso siguiendo las pautas para un sistema con 1000 Teléfonos/100 llamadas simultaneas de capacidad. Mensajes *SIP* totales > 17000 en 10 segundos y luego 1700 cada 10s.

3.1.3.1.6) SOLUCIONES ADICIONALES.

Sumado a la Tabla 2 de valores recomendados de bloqueos para DDOS, se deben considerar las siguientes acciones adicionales:

- Implementar el uso de direcciones DNS y evitar publicar la *IP* en primera instancia.
- Implementar correctamente el área DMZ entre firewall – SBC y red interna del cliente.

3.1.4) SOLUCIONES PROPUESTAS AL INTENTO DE REGISTRAR USUARIOS NO HABILITADOS Y DE REALIZAR LLAMADAS NO AUTORIZADAS.

Luego del análisis y las pruebas efectuadas, se aprecia que la solución de este problema se basa en detectar solicitudes de registración no autorizadas y bloquear los sucesivos intentos desde ese sitio según los valores descriptos para los DDOS.

Es necesario adoptar las medidas tendientes a aumentar la fortaleza de las contraseñas usadas por los usuarios siguiendo las políticas adecuadas según las normas ISO 27001.[11]

En las capturas de ataques en tiempo real se observa que las mismas son realizadas a través de los puertos UDP. Es por esto qué como solución al problema también es necesaria la adopción del uso de certificados de seguridad que actúan como un paso anterior al pedido de registración, esto es, los mensajes de registración no serán tomados como válidos (aunque el usuario y contraseña sean correctos) si anteriormente el dispositivo no completó el proceso de aprobación punto a punto e intercambio de certificados digitales de seguridad automático detallado en la sección 3.1.2.5.

Este proceso de intercambio de certificados *TLS* para dispositivos *SIP* se realiza a través del protocolo *TCP / TLS* utilizando el puerto 5061 para luego pasar a los mensajes *SIP* de registración también por protocolo *TCP / TLS* utilizando el puerto 5061, permitiendo bloquear el protocolo *UDP* utilizado para ataques de *DDOS.* **Las figuras 33 y 34** detallan esta situación y la solución al problema.

[11] https://www.iso.org/home.html

```
                                    45.143.220.13:58454 ——UDP——▶ 198.152.24.68 5060
REGISTER sip:198.152.24.68 SIP/2.0
Via: SIP/2.0/UDP 45.143.220.13:58454;branch=z9hG4bK1052330677
Max-Forwards: 70
From: <sip:3001@198.152.24.68>;tag=1754176679
To: <sip:3001@198.152.24.68>
Call-ID: 1364317228-384808142-1206108505
CSeq: 1 REGISTER
Contact: <sip:3001@45.143.220.13:58454>
Content-Length: 0
User-Agent: pplsip
```

Figura 33. Detalle de mensaje SIP de ataque DDOS por protocolo UDP puerto 5060

```
06:2
06:2                                10.130.50.239:1034 ——TCP——▶ 100.64.10.71:5061
06:2
06:2 SSL Record Layer: Handshake Protocol: Client Hello
06:2     Version: TLS 1.0 (0x0301)
06:2     Handshake Protocol: Client Hello
06:2         Version: TLS 1.2 (0x0303)
06:2         Random
06:2             gmt_unix_time: Nov 29, 2015 22:15:42.000000000 CST
06:2             random_bytes: 99e979cb42fe52afe8d57b2560a3f13f94444ba7b211ae4c...
06:2         Session ID Length: 0
06:2         Cipher Suites (32 suites)
06:2             Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
06:2             Cipher Suite: TLS_RSA_WITH_NULL_SHA (0x0002)
06:2             Cipher Suite: TLS_RSA_WITH_NULL_SHA256 (0x003b)
06:2             Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
06:2             Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
06:2             Cipher Suite: TLS_DH_DSS_WITH_AES_128_CBC_SHA256 (0x003e)
```

Figura 34. Detalle mensaje TCP/TLS para intercambio de certificados por protocolo TCP/TLS

3.1.5) SOLUCIONES PROPUESTAS A LA SUPLANTACIÓN DE IDENTIDAD DE USUARIOS Y EN LLAMADAS TELEFÓNICAS. (SPOOFING).

Se encuentra que la solución de este punto se basa en resolver en principio los problemas #1 y # 2 de la **Tabla 1**. Es necesaria la adopción del uso de certificados de seguridad que actúan como un paso anterior al pedido de registración según lo expuesto en la sección 3.1.2.2. La adopción de certificados soluciona en gran parte la suplantación de identidad pues solamente pueden registrarse y realizar llamadas telefónicas aquellos usuarios que dispongan del certificado digital entregado por el administrador.

Sin embargo, existe la situación donde un empleado o exempleado, ya sea por deslealtad, desconocimiento o error (a través de diversas técnicas de *Pishing* [12] o por ataques de *Malware*[13], *Ransomware*[14] o virus informáticos) podría compartir sus credenciales con alguna persona ajena a la organización, quien luego las utilice con fines delictivos realizando acciones de *spoofing*.[15]

Como primera medida de solución es importante que la organización adopte el uso de las normas 27001 para los procesos de altas y bajas de empleados asegurando el cuidado y resguardo de la información y certificados, así como la gestión de baja de las cuentas internas de usuario telefónico. La solución completa al problema de la suplantación de identidad podrá complementarse con el uso de sistemas de identificación biométrica (Borja, 2019) (huellas, pupilas, etcétera) aislando la autenticación del uso de claves alfanuméricas o certificados digitales que puedan ser compartidos por las partes en disputa.

3.1.6) SOLUCIONES PROPUESTAS AL ROBO DE CERTIFICADOS DIGITALES DE SEGURIDAD.

Como se detalla en las secciones anteriores 3.1.2.1, 3.1.2.2 y 3.1.2.3, el uso de los certificados digitales de seguridad es la solución que aplica para la mitigación del riesgo en ciberseguridad en los puntos tratados.

El robo o copia indebida de estos certificados es otra vulnerabilidad que debe ser considerada. Quien obtenga copia del certificado y las credenciales de usuario, podrá entonces ingresar al sistema como un usuario de teléfono válido. Considerando un sistema en la nube se amplía el universo de usuarios que puedan explotar esta vulnerabilidad.

Cabe aquí la misma mención de la sección anterior para las soluciones propuesta al problema #3 de la **Tabla 1**, pues la solución completa al problema de robo o reutilización de certificados podrá también complementarse con el uso de sistemas de identificación biométrica aislando la autenticación del uso de claves alfanuméricas o certificados digitales.

Queda planteado la posibilidad de investigar en futuros desarrollo de terminales de telefonía *IP* que puedan registrar al usuario con técnicas de identificación biométrica.

[12] Pishing es el nomnbre como se conoce a la técnica de intentar pescar información del usuario forzándolo a ingresar a un sitio falso.
[13] Software malicioso que generalmente se usa para el robo de información o para causar daño en dispositivos de computación.
[14] Tipo de Software con código Malicioso al ejecutarse cifra la información del usuario, la copia y luego la envía al atacante, el cual solicita un rescate mediante un pago, normalmente en Bitcoins para reestablecer los archivos.
[15] Spoofing es el nombre como se conoce a la técnica de suplantar la identidad de usuarios.

3.1.7) APORTE DE UN MODELO TEÓRICO PARA LA SOLUCIÓN DEL PROBLEMA DE DENEGACIÓN DE SERVICIO DISTRIBUIDO (DDOS) EN SISTEMAS DE TELEFONÍA *IP* BASADOS EN LA NUBE (SGIBA).

Luego de completar el estudio de las diversas alternativas y soluciones propuestas para el problema de los ataques DDOS en sistemas de servicios de telefonía *IP* basados en la nube, se observa que hasta el momento todas están basadas en medidas preventivas y en muchos casos consideradas estáticas para el bloqueo de ataques según determinadas reglas, tanto en el *firewall* como el *SBC.*

¿Cuál es el mejor lugar donde realizar el trabajo de filtrar y bloquear tráfico malicioso, y discriminarlo del tráfico de usuarios reales? Este estudio focaliza el bloqueo de ataques DDOS en la correcta configuración de los parámetros de bloqueo dentro del *SBC*, evitando la inspección de paquetes de datos a nivel aplicaciones por parte del firewall y el retraso en la comunicación en tiempo real.

Se detalla a continuación un modelo propuesto que abre la posibilidad a un sistema más robusto, complejo, eficiente y dinámico para el manejo del tráfico en la red a nivel mundial.

Este sistema será llamado "**Sistema Global inteligente de base de datos de direcciones *IP* de atacantes e ISP DDOS**", de aquí en adelante **"SGIBA"** (Sistema Global Inteligente Base Atacantes) en este documento.

El modelo actual bloquea los ataques de DDOS, sin embargo, el tráfico sigue llegando hasta el SBC en el borde de la red generando incremento en el tráfico de datos y baja de rendimiento en la red y en los dispositivos SBC tomando tiempo de máquina en procesar cada uno de estos ataques.

El modelo propuesto que queda como base de estudio para futuros trabajos de tesis se basa en la posibilidad de crear un servidor centralizado a nivel de red *del* proveedor de servicios de internet, quien pueda llevar un registro de las direcciones *IP* provenientes de sitios maliciosos (sin necesidad de tomar el trabajo de inspeccionar los paquetes como lo haría un firewall).

Esta información podrá ser compartida de manera dinámica por los principales proveedores de centro de datos servicios en la nube y de esa forma bloquear el tráfico al momento de pasar por la red del proveedor de internet, evitando que llegue hasta el centro de datos, reduciendo el tráfico entrante a los dispositivos que en el caso de la telefonía son principalmente los *SBC*.

Para el éxito de la implementación de este modelo, será fundamental el acuerdo y trabajo conjunto de los proveedores de internet junto a la autoridad mundial competente que tome la responsabilidad de implementar este modelo como parte de la reducción del cibercrimen.

El modelo propone una conexión segura utilizando certificados firmados digitalmente por una autoridad única y central creada para este propósito. Esta autoridad seria la responsable de generar certificados de identidad para cada uno de los ISP y empresas proveedoras de servicios de nube, asegurando la identidad de las partes que intercambian información y evita informes maliciosos que incorporen erróneamente falsos positivos.

El modo de funcionamiento sería el siguiente:

- El *SBC* dentro del proveedor de servicios de nube detecta el tráfico malicioso.
- EL *SBC* envía la información a través de una conexión segura, firmada y verificada hacia el servidor central que creará una base de datos de IPs maliciosas que están generando *DDOS.*
- El usuario final del *SBC* es quien tiene la decisión final de informar el ataque, solo los proveedores de servicios en la nube estarán autorizados por el ente regulador a obtener los certificados digitales de seguridad que le otorguen la posibilidad de enviar reportes de ataques al nodo central. (Considerando que la cantidad de empresas proveedoras de servicios en la nube en el mundo representan una cantidad discreta menor a 3000 sitios, es posible registrarlos individualmente y acordar términos de colaboración y uso de certificados para pertenecer al sistema).
- El *ISP* incorpora esas direcciones *IP* a su base y envía una alerta a todos los *ISP* que son nodos incorporados.
- Los nodos verifican si la *IP* y origen pertenece a alguno de sus clientes y responden al sistema central, a su vez el *ISP* investiga cual es el cliente exacto a fin de hacerle un monitoreo futuro.
- Se definirá un modelo de acciones incrementales a tomar en contra del sitio atacante que incluya desde avisos, alertas, penalidades y hasta el corte del servicio según intervalos de tiempo predefinidos tales como, alerta 8hs, aviso de corte temporario 24hs, corte total 48hs.

- El sistema bloquea el tráfico proveniente del sitio malicioso evitando que llegue al proveedor de la nube, disminuyendo el tráfico innecesario hacia el proveedor de nube.
- El servidor del sistema central podrá ser alimentado por un sistema de inteligencia artificial que pueda gestionar altas, bajas y actualizaciones de IPs maliciosas según lo informado por cada proveedor de servicios en la nube a fin de mantener un sistema dinámico.
- Eventualmente, las transacciones entre el nodo central y cada *ISP* por cada reporte aceptado como sitio considerado malicioso, pueden usar la tecnología *Blockchain*[16] a fin de llevar un registro trazable de cada dirección IP, su historia y actual situación. Se debe tener en cuenta que las direcciones *IP* pueden ser reusables, y el sistema tiene que tener la capacidad de cambiar dinámicamente el estado de una dirección *IP* en el caso que deje de ser una fuente maliciosa.

Queda así planteado este modelo para ser tomado como trabajo de investigación y desarrollo por quienes encuentren en él un camino de mitigación de los riesgos en la ciberseguridad y ciberdefensa.

Se espera que este tipo de modelos y soluciones donde se presenta una activa participación de los *ISP* en el bloqueo del tráfico de determinados usuarios sea objetado por no aplicar al concepto de neutralidad de la red en internet e ir contrario a quienes fomentan la democratización del ciberespacio, sin embargo, esta será una batalla que habrá que dar junto a los organismos pertinentes en el combate del anonimato y cibercrimen que se en el quinto dominio.

[16] Blockchain , técnica de cadena de bloques de transacciones conectados mediante un cálculo cifrado.

La **Figura 35** detalla un esquema del flujo de la información con el estado inicial cuando ocurre un ataque donde este flujo llega hasta el dispositivo de entrada del proveedor de la nube.

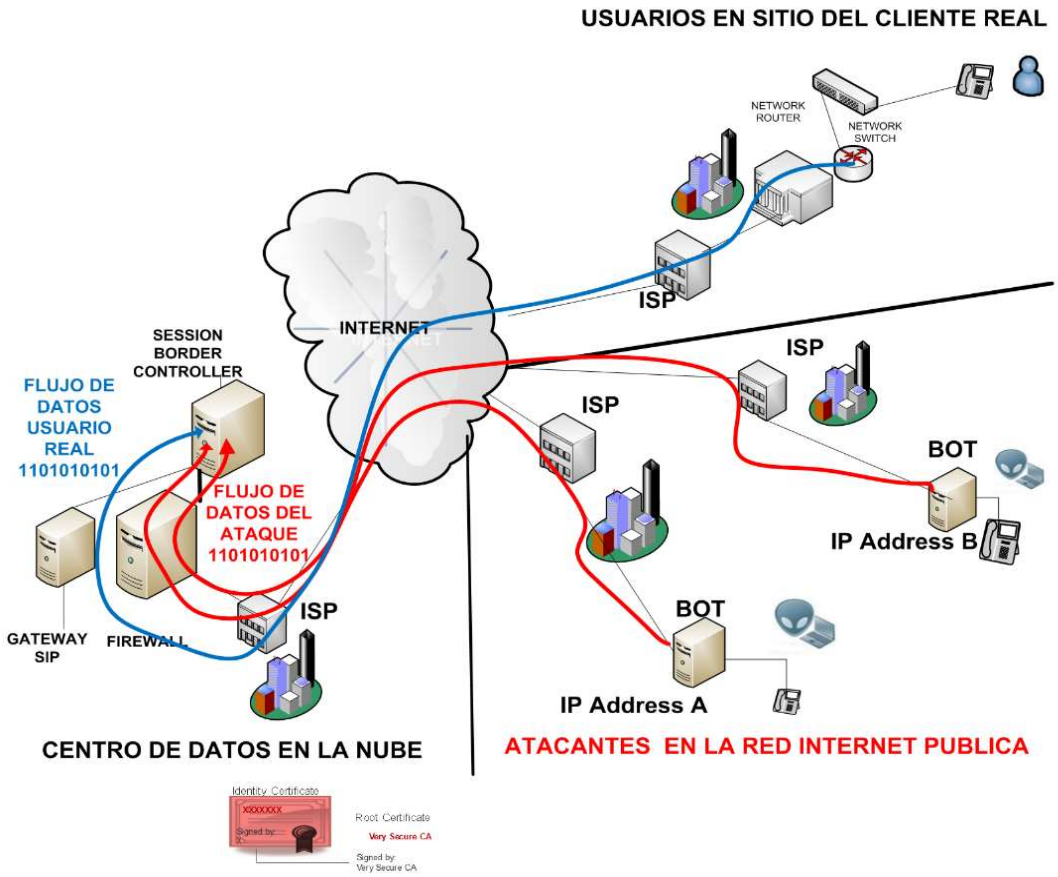


Figura 35. Flujo de Datos de Atacantes

En la **Figura 36** aparece el *SGIBA*. Cuando el *SBC* detecta uno de los tipos de *DDOS*, lo reporta luego al *SGIBA* con la dirección *IP* de origen. El *SGIBA* envía esta dirección *IP* a los ISP, que responden si es propio o no y toman acciones. Luego el *SGIBA* registra es *IP* en la base de datos y la envía a todos los nodos del *SGIBA* indicando el *ISP* y *dirección IP,* y creando un registro de transacciones en *Blockchain* para llevar el control y que cualquier nodo pueda actualizarse inmediatamente e inclusive la parte afectada pueda ver el registro de transacciones históricas y solicitar el regreso al sistema en casos de error reportando falsos positivos.

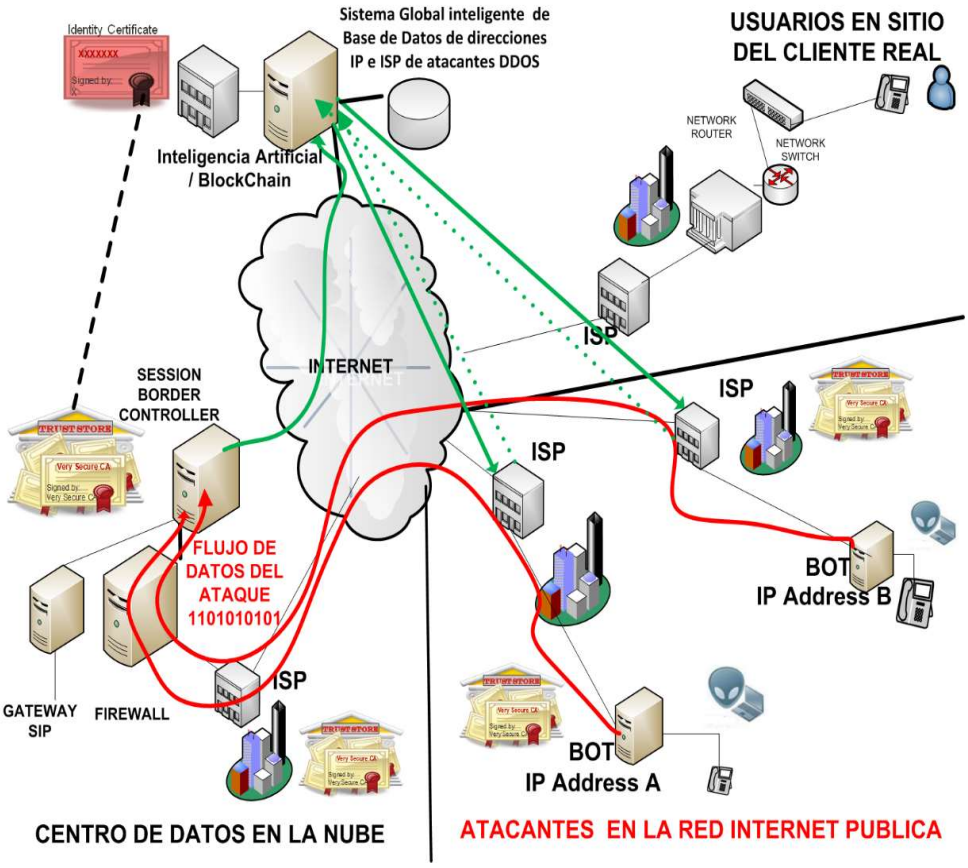


Figura 36. Sistema Global Inteligente de base de datos de direcciones IP e ISP de atacantes DDOS, Recibe alerta de IP de Ataque y alerta a los nodos

En la **Figura 37** los nodos del SGIBA se actualizan en forma dinámica y se observa que ahora el ataque es detenido y bloqueado a nivel ISP, evitando enviar esa i formación al proveedor de la nube.

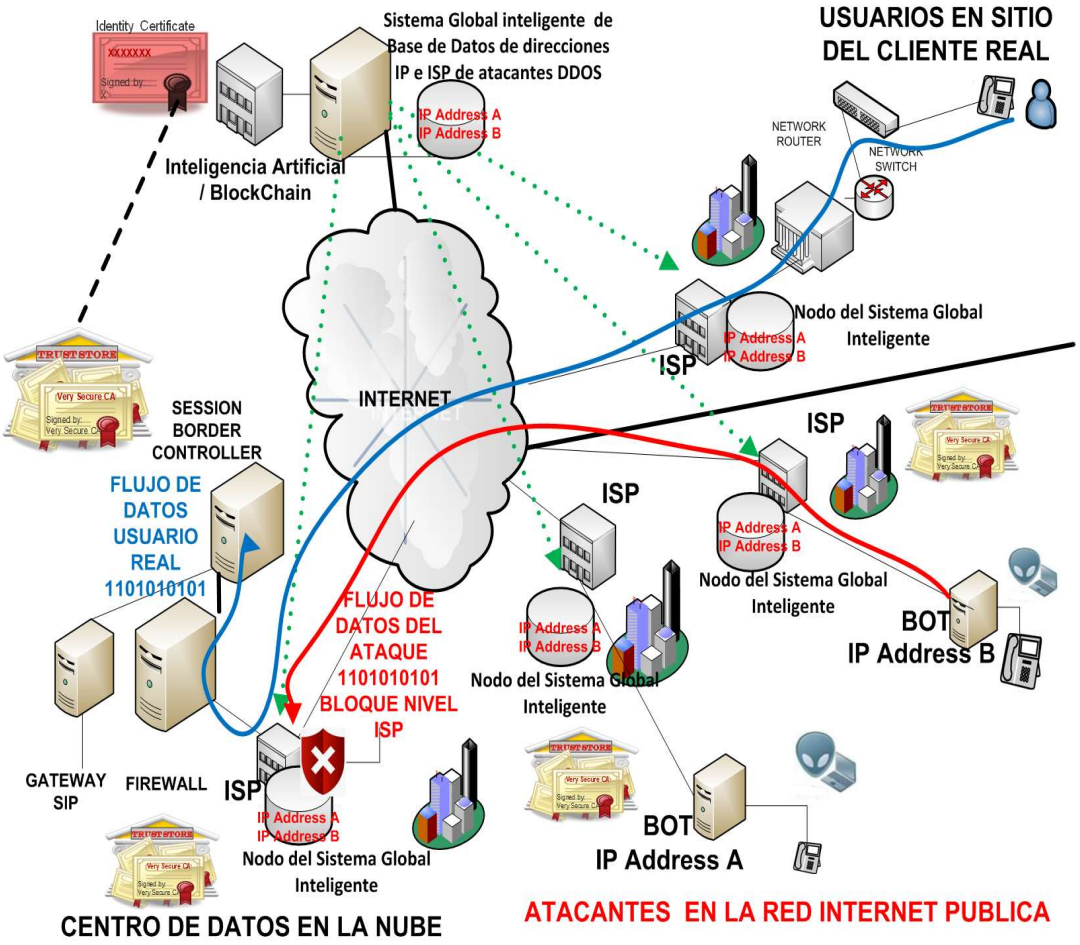


Figura 37. Nodos del Sistema Global Inteligente de base de datos de direcciones IP e ISP de atacantes DDOS, bloquean la entrada o salida de Datos provenientes de atacantes

En la **Figura 38** se detalla cuando el *ISP* detecta que la *IP* maliciosa ya no es usada por el mismo cliente, y envía una actualización al sitio central, quien actualiza a todos los nodos del *SGIBA*. Luego se observa que el tráfico desde esa dirección *IP* ahora puede ingresar al proveedor de la nube.

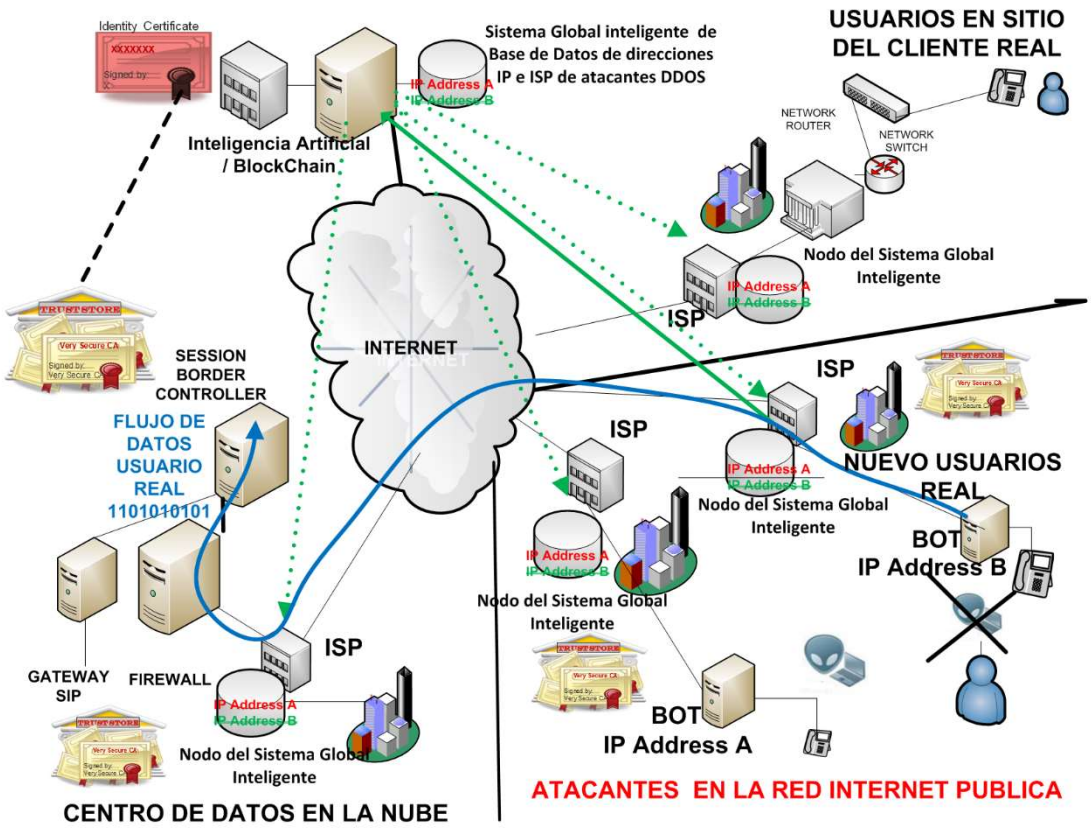


Figura 38. Nodos del Sistema Global Inteligente de base de datos de direcciones IP e ISP de atacantes DDOS actualizan Cambio de IP o de usuario y sistema actualiza a los nodos

3.1.7.1) ACLARACIONES, PREGUNTAS Y RESPUESTAS ACERCA DEL FUNCIONAMIENTO DEL SGIBA.

En esta sección se detalla una lista de preguntas y respuestas tendientes a aclarar el funcionamiento del SGIBA.

- ¿Quiénes pueden reportar evento de Denegación de servicio?
    - Solamente los proveedores de servicios de telefonía basada en la nube, registrados previamente en el ente regulador y organizador del SGIBA.
- ¿Cómo se registra un proveedor de servicios de telefonía basada en la nube en el SGIBA?
    - Completando un formulario de solicitud que debe ser aprobado por el comité de arbitraje dando fe que el solicitante es un proveedor válido, reconocido y confiable. Una vez aprobado se entrega copia de los certificados digitales de seguridad y confianza para que pueda reportar eventos DDOS cumpliendo con las normas de integridad, confidencialidad, disponibilidad, tanto como autorización, autenticación y no repudio.
- ¿Cómo se financia el sistema SGIBA?
    - Los proveedores de servicio de telefonía en la nube abonan un canon de inicio y un canon mensual. Un valor similar a un antivirus. La recaudación es usada para financiar la implementación, mantenimiento y arbitraje del sistema, a cambio de esto los proveedores en la nube estarán ofreciendo servicios más seguros.
- ¿Es necesario que el ISP revise el tráfico de los usuarios que han sido reportados como fuentes de DDOS?
    - En principio no, para evitar rechazos de la comunidad respecto a la neutralidad de la red y además para evitar sumar la tarea de inspección de paquetes que causaría retrasos en la velocidad de transmisión. Queda asignada al proveedor de servicios en la nube la tarea de inspeccionar los paquetes de datos, reconocer patrones y reportar DDOS al centro SGIBA,
- ¿El proveedor de la nube debe reportar todos los eventos DDOS?
    - No. Solamente los que consideré que son DDOS reales y quiera reportarlos.
- ¿Qué ocurre si se reportar un *DDOS* por error, y el *ISP* da de baja al usuario de origen?

- El usuario de origen puede realizar el reclamo mediando el un formulario en línea justificando su actividad, este reclamo es enviado al Proveedor de la nube que lo reportó y tiene la obligación de confirmar o denegar el pedido.
- Luego el ente regulador *SGIBA* puede arbitrar y tomar una decisión final basada en un análisis de la veracidad del reclamo.
- En muchos casos el atacante utiliza un servidor intermedia que no es de su propiedad para llevar a cabo el ataque, como por ejemplo instalar los programas tipo *Bots* en máquinas afectadas a través de un virus, en este caso la *IP* o conexión debe ser igual dada de baja y alertar al usuario, de la misma forma que ocurre en un organismo cuando el área de *TI* impide la conexión a la red de un usuario que se le haya detectado un virus en su *PC*. Para el caso de los *ISP,* este será un punto de disputa pues no querrán perder clientes entrando en conflicto con el contenido enviado, y justamente será el cambio de paradigma esperado y necesario de la misma forma que hoy lo realizan colaborando en la detección de situaciones de Grooming o de pornografía infantil.

- ¿Qué pasa si una *IP* bloqueada por el *ISP* es ahora asignada a un usuario nuevo?
  - El *ISP* puede levantar la sanción previa comprobación de que ya no es una fuente de *DDOS*
- ¿Puede esto transformarse en un sistema que requiera mucha actividad manual de reportes, reclamos, altas y bajas?
  - En un comienzo si, aunque el modelo tiende a ser un sistema autónomo donde el uso de sistemas de Inteligencia Artificial y *Blockchain* pueda ir resolviendo cada una de las solicitudes, reportes, reclamos, conflictos, altas y bajas.
- ¿Puede extenderse este sistema hacia otras necesidades?
  - Si, un modelo similar puede usarse para reportar *Malwares*, Virus Informáticos y otros tipos de ataques, sumando nuevos actores a la red que puedan asociarse como nodos confiables y reportar eventos que puedan ser verificados por Inteligencia Artificial e incluidos en una lista, creando un gran observatorio mundial en el combate al cibercrimen donde un acuerdo entre grandes compañías, entes de gobierno, proveedores de servicios de internet y estados participantes puedan regular y defenderse de estos ataques creando una red más segura.

3.2) SOLUCIÓN AL PROBLEMA DE LA CAPTURA DE PAQUETES DE VOZ.

Esta sección se enfoca en el estudio del problema #5 de la **Tabla 1**.

3.2.1) RESUMEN DEL PROBLEMA.

El siguiente diagrama de la **Figura 39** resume una comunicación de Voz sobre *IP* donde el flujo de paquetes de datos es transmitido desde un teléfono hacia el otro, pasando por la red de internet, entrando y saliendo al proveedor de servicios de telefonía en la nube. Estos paquetes de datos se transmiten a través de internet usando el protocolo *RTP* y por puertos preestablecidos, generalmente utilizando rango de puertos entre 35000 – 40000 como de describe en la Figura 8. Si bien no es objeto de análisis en este trabajo, cabe mencionar que existe la posibilidad de establecer el flujo del audio para que sea enviado directamente entre los 2 teléfonos mediante la técnica de Shuffling [17] en el caso que ambos trabajen con el mismo *Codec*.

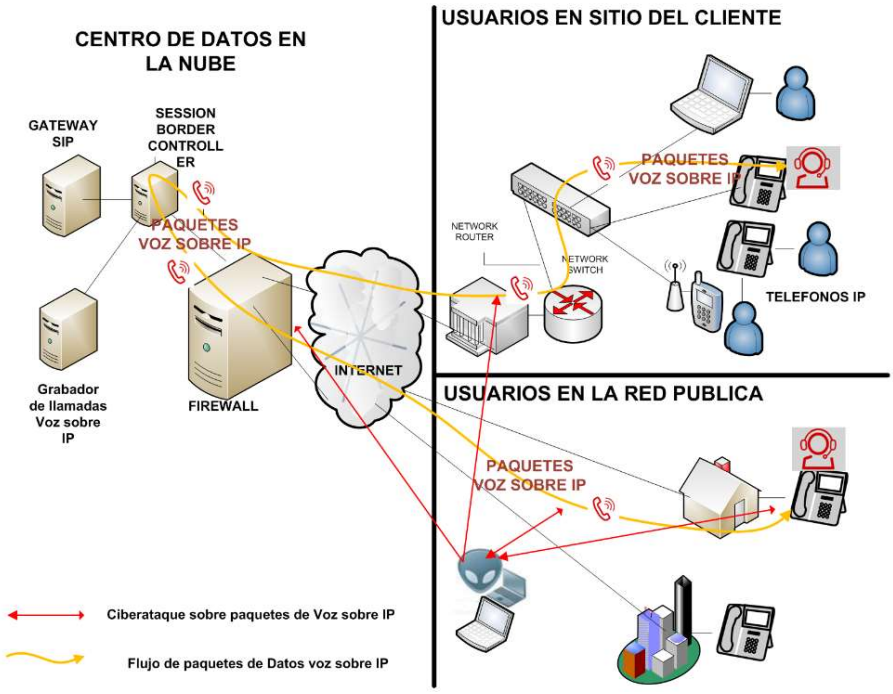


Figura 39. Flujo de paquetes de Datos para Voz sobre IP

[17] Shuffling : nombre en inglés como se conoce a la técnica de permitir la conexión de audio directa entre las partes.

Los puertos quedan expuestos a posibles ataques que puedan capturar información del contenido de las llamadas. Adicionalmente, en el caso que el usuario lo requiera, las llamadas pueden ser grabadas mediante el uso de un grabador digital dentro de los componentes de la arquitectura de telefonía en la nube.

3.2.2) PRUEBAS Y DEMOSTRACIONES EN LABORATORIO TÉCNICO.

La siguiente **Figura 40** detalla una captura de paquetes de datos expuestos en una llamada de voz sobre *IP* donde se observan los paquetes *RTP* por puerto *UDP*, puertos 5000 y 2808 entre las direcciones *IP* de los puntos en comunicación utilizados para la llamada de prueba, con compresión de audio *G.711* [18] que finalmente son traducidos a señales binarias 1 y 0.

Esta captura puede ser realizada atacando el dispositivo (*pishing*, virus, y otros vectores de ataque), o bien, con la técnica de *port mirror* o suplantación de identidad.

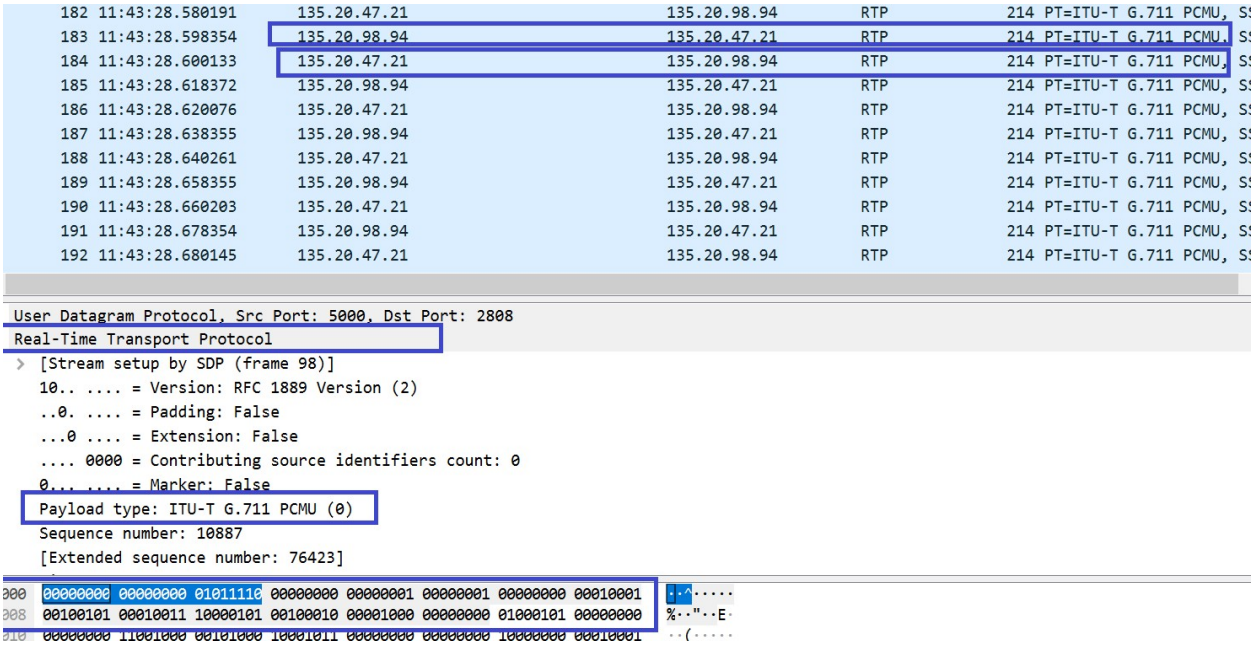
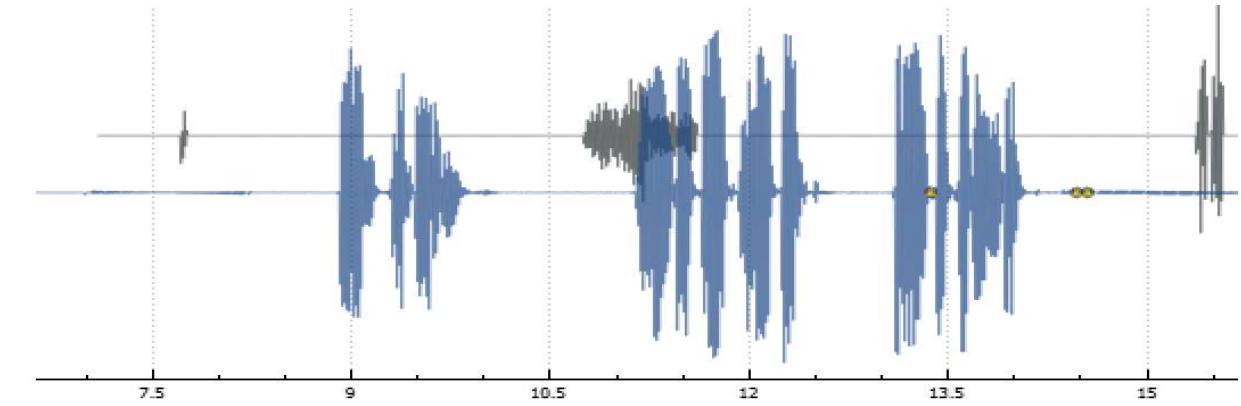


Figura 40. Captura de paquetes RTP

[18] G.711 es un algoritmo de compresión de paquetes de Audio que usa 64Kb por Segundo.

La captura de datos fue realizada utilizando la herramienta de software libre *Wireshark* (Wireshark, 2019) que además permite escuchar el audio como se detalla en la **Figura 41**.



Source Address	Source Port	Destination Address	Destination Port	SSRC	Setup Frame	Packets	Time Span (s)	Samp
135.20.98.94	5000	135.20.47.21	2808	0x33feeaef	98	434	7.11 - 15.7 (8.64)	8000
135.20.47.21	2808	135.20.98.94	5000	0x1d5e0af8	60	467	6.49 - 15.9 (9.4)	8000

Figura 41. Audio Real decodificado de paquetes RTP

3.2.3) LAS SOLUCIONES PROPUESTAS PARA LA MITIGACIÓN DE RIESGOS DE CAPTURA Y ESCUCHA DE PAQUETES DE VOZ SOBRE *IP*.

Para el caso de la *Voz sobre IP,* la solución para mitigar los riesgos de ciberseguridad es la implementación del protocolo *SRTP*, el cual utiliza certificados de seguridad digitales que encriptan los mensajes *RTP* y través de protocolo UDP según la muestra tomado en la **Figura 42.**

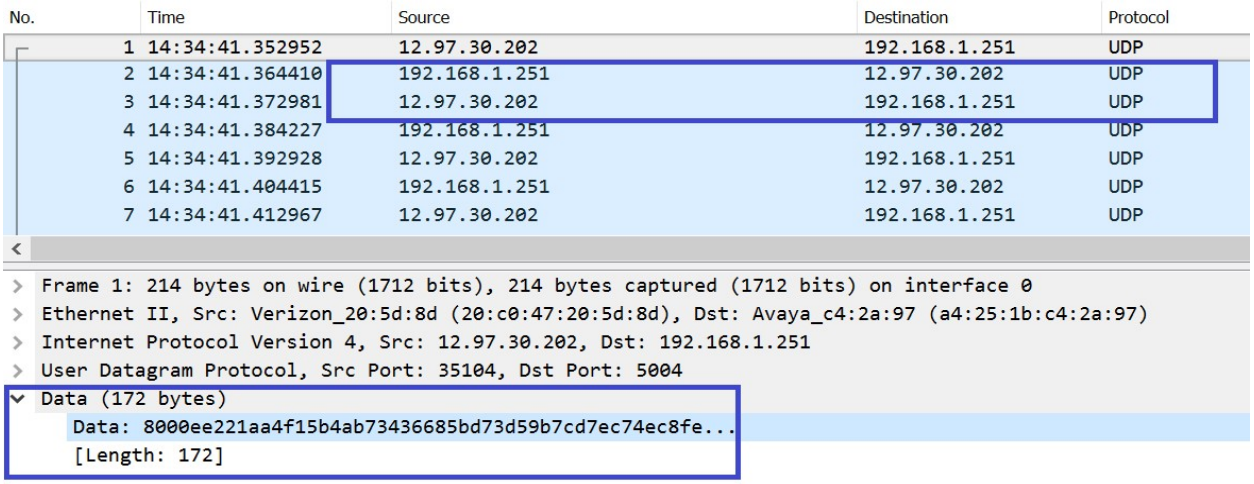


Figura 42. Captura de paquetes SRTP

Se observa en el mensaje *SIP,* que hay un acuerdo entre las partes involucradas en la llamada en el uso de *SRTP*, según el ejemplo de la **Figura 43** tomado en laboratorio, usando el algoritmo de encriptado *AES_128* con cifrado *SHA1.*

Figura 43. Detalle de encriptado de voz por SRTP

De esta forma, en caso de ataque, captura de datos o robo de los archivos de grabación digitales no se podrá escuchar el audio de la llamada, salvando el caso que se obtenga copia del certificado digital de seguridad de acuerdo a lo detallado en la sección 3.1.5.

3.3. SOLUCIÓN AL PROBLEMA DEL ATAQUE FÍSICO AL SITIO DE PROVEEDOR DE SERVICIOS DE NUBE.

Esta sección se enfoca en el estudio del problema #6 de la **Tabla 1**.

3.3.1) RESUMEN DEL PROBLEMA.

Como se detalla en el resumen y marco teórico esta arquitectura concentra la infraestructura de una gran cantidad de organismos y/o entes gubernamentales en uno o varios sitios proveedores de servicios en la nube de acuerdo al tamaño de cada centro de datos. pudiendo albergar los servicios de 1000 organismos y generando un nuevo escenario donde un ataque al sitio físico puede afectar el servicio de datos de múltiples clientes, pasando este sitio a ser considerado como parte de la infraestructura crítica de un país, más aún, en caso de albergar la información de entes de gobierno.

Si bien los proveedores de servicios en la nube poseen centros de datos redundantes, es de esperar que el restablecimiento del mismo ante situaciones de catástrofe no sea inmediato. Como se ha mencionado anteriormente, existen dos riesgos de ataques considerados como los más importantes: el ataque físico al predio ya sea por atentados criminales o acciones militares dentro de un conflicto bélico y el ataque a la conexión de fibra o conectividad de entrada a internet que puede dejarlo aislado.

A noviembre del año 2019, existen en el mundo aproximadamente 500 grandes sitios (datacenterknowledge, 2019) de proveedores de servicios en la nube, y esta cantidad irá creciendo según las predicciones de crecimiento del negocio.

3.3.2) ANÁLISIS SOBRE LOS CENTRO DE DATOS DE PROVEEDORES DE SERVICIOS LA NUBE.

Tomando el caso de una de las empresas proveedoras de servicios en la nube más importantes, *Amazon Web Services*, se observa que posee 22 centros de datos y cuatro en construcción según la **Figura 44** (AWS, 2019), que constituyen 69 zonas de disponibilidad, esto significa más de un centro de datos lógico en cada sitio. Como ejemplo se puede citar el centro de datos de Tokio que mantiene cuatro zonas de disponibilidad.

Figura 44. Amazon Web Services Centros de Datos en el mundo

Algunos de los 22 sitios, pueden observarse en el sitio de Google Maps (Google, 2019). A modo de ejemplo, la **Figura 45** (Google, Google maps en Plant City, 2019) muestra la ubicación de AWS en la ciudad de *Plant City*, estado de *Ohio, USA*.

Figura 45. Foto Satelital del Sitio AWS en Plant City- Ohio -USA

La **Figura 46** (Google, Google maps en Quebec, 2019) muestra el sitio en construcción de *AWS* en *Quebec, Canadá.*

Figura 46. Centro de Datos en construcción AWS en Canadá

La **Figura 47** (Google, Google Street view Quebec, 2019) muestra detalles internos de la construcción del techo del predio de este centro de datos.

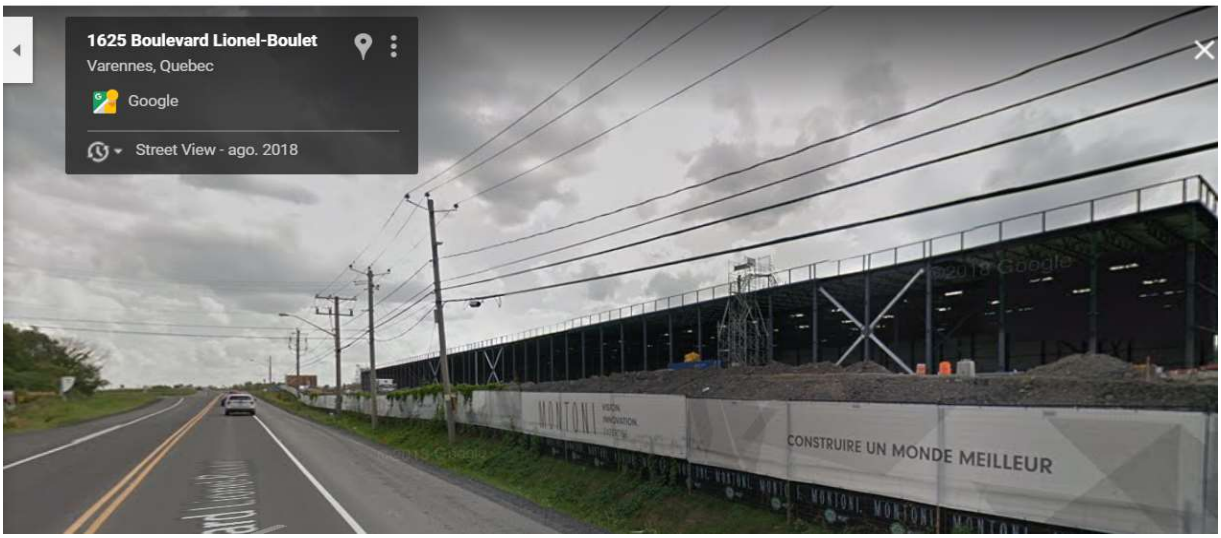


Figura 47. Data Center en Construcción AWS Canadá

La **Figura 47** (Microsoft, Microsoft Azure Clou Map, 2019) detalla los sitios de los centros de datos que ofrecen servicios en la nube de la empresa Microsoft - Azure.

Figura 48. Mapa de Data Centers Cloud de Microsoft Azure

Para el caso de la República Argentina, El boletín oficial #28631 de la provincia de Buenos Aires (GBA, 2019) informa el acuerdo de AWS para instalar un nuevo centro de datos en el predio de 133 hectáreas comprendidas en el partido de Bahía Blanca y de Cnel. Rosales de la provincia de Buenos Aires. La **Figura 49** (Rosaleño, 2019) detalla la ubicación geográfica de las 3 zonas asignadas y conocidas como Tango Sur, Tango Central y Tango norte. Una de las razones de la elección de este espacio es la ubicación cercana al parque eólico que se ampliará para dar energía a los centros de datos.

Esta nueva locación deberá entonces ser considerada dentro de la infraestructura crítica del país, pues albergará información crítica de sus ciudadanos y servicios críticos que pueden ir desde el funcionamiento de las ciudades inteligentes hasta servicios telefónicos.

Figura 49. Zona Geográfica donde se construirá el Centro de Datos de AWS en Argentina

La **Figura 50** detalla la Red nacional de Fibra Óptica (ARSAT, 2019) de la República Argentina y el recorrido que deberá ser custodiado especialmente para mitigar riesgos en la infraestructura crítica.

Un gran número de eventos delictivos de corte de fibra son reportados semanalmente tales como casos en Argentina en la ciudades de Trelew (radio3cadenapatagonia, 2019) (novachubut.com, 2019), San Juan (sanjuan8, 2019) y Puerto Madryn (eldiariodemadryn, 2019).

Figura 50. Red Nacional de Fibra Óptica Argentina, Zona Bahía Blanca

3.3.3) EL CASO AWS – WIKILEAKS.

En el año 2018, fue publicado en el sitio *Wikileaks* (Wikileaks, 2019) un documento de texto de 20 páginas llamado *AmazonAtlas_v1* detallando una gran cantidad de datos secretos acerca de los centros de datos del proveedor de servicios en la nube *Amazon Web Services*. Entre otros datos el informe incluye la dirección postal exacta, los nombres y direcciones de email de los responsables de cada uno de los 34 sitios disponibles en el mundo hasta el año 2015, y a quienes contactar en caso de tener que realizar un envío de partes.

Algunos de esos sitios alojan información de gobierno. También el reporte incluye la misma información de otros proveedores tales como *Equinix, CyrusOne, Digital Fortress, Hitachi, Terremark, KVH, KDDI, Keppel, Tata Communications, Colt, Global Switch, iseek-KDC, NextDC, and Ascenty.*

El hecho que todo esto haya sido revelado como datos que no estaban disponibles abiertamente, demuestra que los mismos proveedores tratan esta información de modo confidencial, aceptando el riesgo y vulnerabilidad de que la misma se haga pública, ya sea para la integridad de las mismas personas responsables de los centros, quienes eventualmente podrían ser reclutados para un eventual robo de información o acceso indebido, y entendiendo que esos centros de datos son parte de una infraestructura crítica. La **Figura 51** (Wikileaks, 2019) detalla cómo se presenta la información de cada sitio en el mencionado documento.

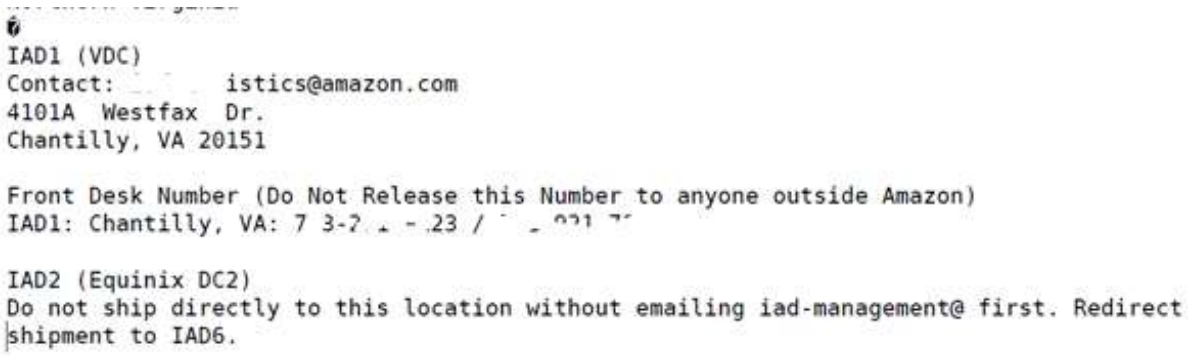


Figura 51. Ejemplo del documento expuesto en Wikileaks y los detalles de cada sitio

3.3.4) SOLUCIONES PROPUESTAS A IMPLEMENTAR PARA LA MITIGACIÓN DE RIESGOS DE ATAQUE FÍSICO AL SITIO DEL PROVEEDOR DE NUBE.

Queda planteado el escenario global donde los centros de datos en la nube albergaran información y servicios críticos de miles de empresas y organismos, transformando estos sitios en parte de la infraestructura crítica que deberá ser custodiada, proponiendo su incorporación al conjunto de infraestructuras críticas del país, así como también incorporar el tendido de fibra óptica que conecta a estos sitios, el tendido eléctrico o las fuentes de energía alternativa.

Este punto en particular es de vital importancia, dado que en este nuevo escenario de guerra híbrida, aparece este punto en particular vinculado a situaciones cercanas a acciones en una guerra tradicional.

3.4) SOLUCIÓN AL PROBLEMA DE ATAQUE A LA INFRAESTRUCTURA INTERNA DE NUBE VÍA PUERTO DE ADMINISTRACIÓN.

Esta sección se enfoca en el estudio del problema #7 de la **Tabla 1**.

3.4.1) RESUMEN DEL PROBLEMA.

Al adoptar el uso de la telefonía o cualquier otro servicio basado en la nube, la administración de todos los servidores y dispositivos que componen la arquitectura se realiza en la mayoría de los casos desde una conexión remota vía internet. Será necesario que los puertos de administración remota queden abiertos en el *firewall* para permitir esta conexión y que los dispositivos puedan ser administrados. En general, la mayoría de los dispositivos son administrados en forma remota usando los protocolos *SSH*[19] a través del puerto 22 o el puerto 222 para el ingreso a través de la interfase de línea de comando para sistemas operativos *Linux* (Linux, 2019), o usando el protocolo *HTTPs*, puerto 443, 8444 o 9443 para ingresar por interfase web. También es usada la conexión por *Remote Desktop*, puerto 10000 para los sistemas operativos Windows (Microsoft, Microsoft Corporation, 2019).

El cliente usuario del servicio de telefonía, en este caso debe gestionar el acceso remoto para cada uno de los dispositivos, para cada uno de los administradores designados para el sistema

[19] Protocolo de Conexión seguro vía remota utilizando el puerto 22.

y para cada función que sea necesaria administrar según la jerarquía de cada administrador y usuario.

Aquí se presenta uno de los mayores problemas no solo de la telefonía, sino de toda la infraestructura de soluciones en la nube. Todos los dispositivos quedan virtualmente expuestos en internet desde el momento que se habilita un acceso remoto, Esto es, expuestos para el administrador verdadero como para atacantes cibernéticos. La **Figura 52** detalla esta situación, diferenciando la conexión remota del administrador real a cualquiera de los dispositivos que componen la infraestructura de la nube versus la conexión remota del atacante hacia los mismos dispositivos.

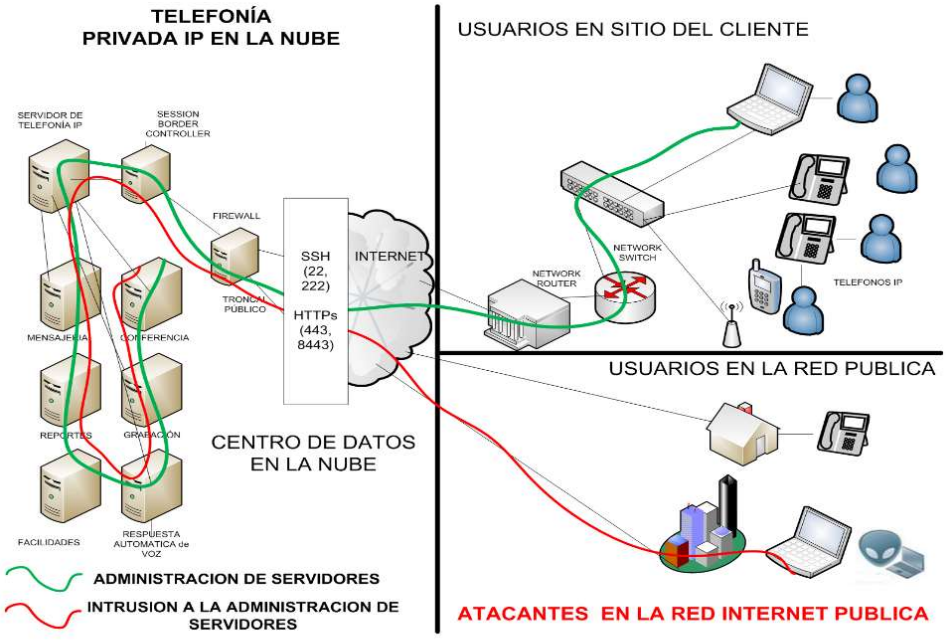


Figura 52. Intrusión a la administración de servidores

3.4.2) VULNERABILIDADES Y RIESGOS ASOCIADOS.

Claramente se visualiza una importante vulnerabilidad del sistema pues queda a merced de la habilidad del administrador del servicio en la nube en seguir las pautas, políticas de seguridad, implementación de certificados y permisos para acceso permitido solo de determinadas locaciones. Los riesgos en ese caso son altísimos pues una intrusión en cualquiera de los dispositivos puede causar todos los daños posibles, desde el robo de información hasta la caída total del servicio ofrecido.

Mas allá de la arquitectura de los servicios de telefonía *IP* basada en la nube, en este punto se unen todos los conceptos de seguridad informática y ciberseguridad relacionados con cualquier otro tipo de servicio en la nube.

Los atacantes podrán aplicar cualquiera de todos los métodos conocidos de ataques tales como las técnicas de *Pishing*, *Malware*, ingeniería social o instalación, copia de virus tipo *worm*, *Ransomware*, armas cibernéticas y explotación de vulnerabilidades de día cero.

El caso reportado por el banco internacional *Capital One* (CapitalOne, 2019) que afectó también los datos del banco *JP Morgan* (Morgan., 2019) en el mes de Julio del año 2019 detalla exactamente un hecho ocurrido de robo de información en un entorno de solución basada en la nube en un Data center provisto por *Amazon Web Services* como el descripto en esta sección.

Aproximadamente los datos de 106 millones de tarjetas de crédito fueron robados por un ataque realizado por un acceso al centro de datos de AWS que fue permitido debido a una mala configuración del *firewal*l y el uso de credenciales conocidas por un ex empleado de Amazon. Las notas citadas del *Wall Street Journal* (WSJ, 2019)*, New York Times* (TImes, 2019) describen el caso y proveen la siguiente tabla de la **Figura 53** y el ranking de eventos reportados de casos similares de robo de información en millones de usuarios .

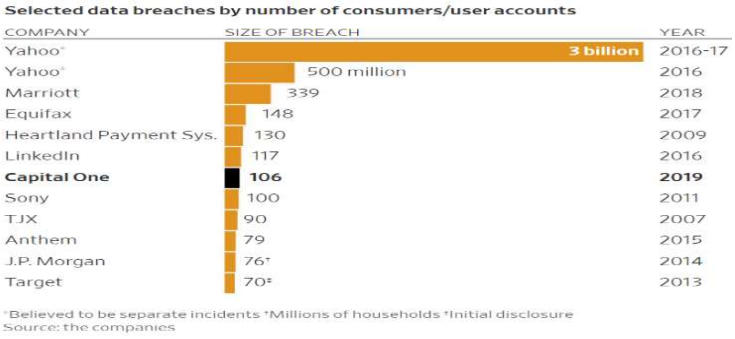


Figura 53. Tamaño de Robo de Información por ciberataques en millones de Usuarios, reportado por las empresas

Otra de las vulnerabilidades a mencionar se presenta en el caso que un dispositivo de la empresa basado en la nube es atacado desde un servidor con máquinas virtuales pertenecientes a otro usuario, cliente u organismo, en el mismo centro de datos mediante el acceso de un atacante que ingresa por el puerto de administración explotando cualquiera de las vulnerabilidades conocidas o una mala configuración en la seguridad realizada por el administrador de la red de otro cliente.

Cabe aclarar que según la infraestructura y arquitectura del proveedor de la nube un mismo servidor físico puede albergar información y procesar servicios de dos clientes diferentes, es por ello qué el acceso al servidor es un punto común de ataque al sistema completo. La **Figura 54** explica esta situación.

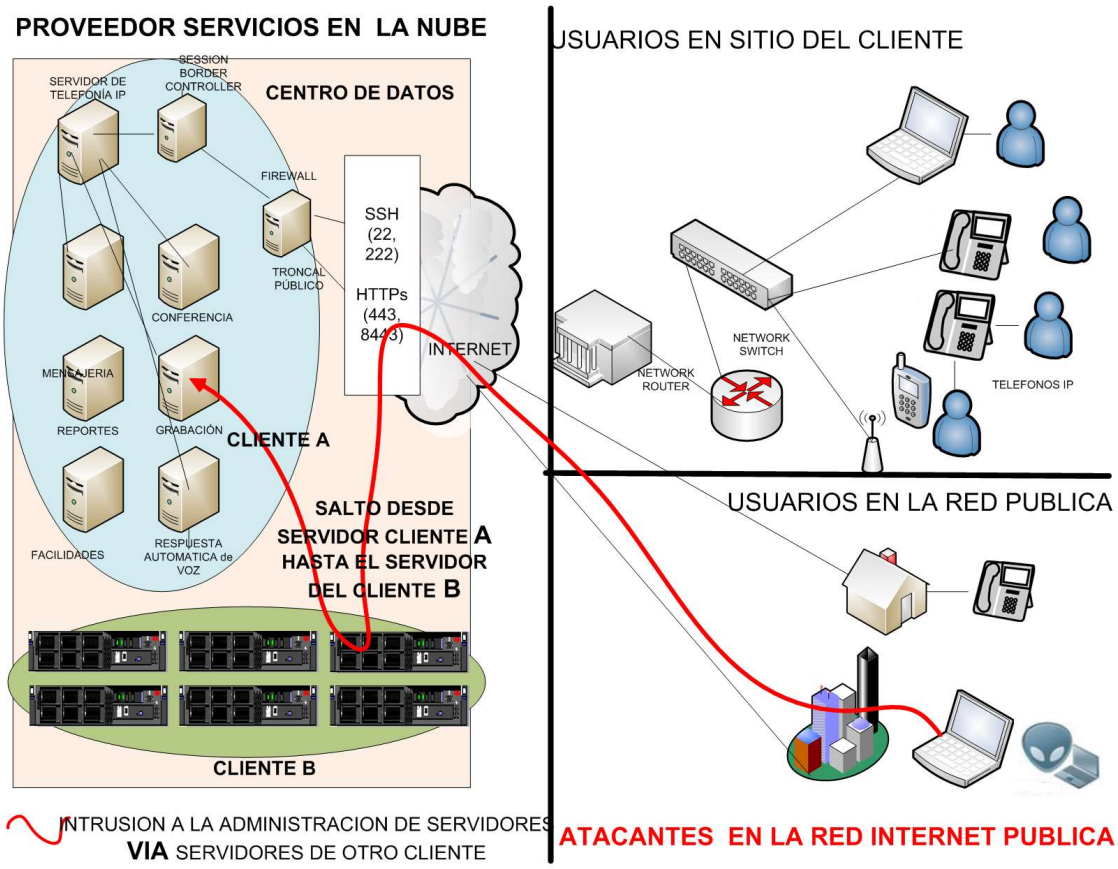


Figura 54. Intrusión a la administración de servidores vía servidores de otro cliente en el mismo Centro de Datos

3.4.3) SOLUCIONES PROPUESTAS AL PROBLEMA DEL ACCESO INDEBIDO VÍA PUERTOS DE ADMINISTRACIÓN A LA RED INTERNA PRIVADA Y A LOS SERVERS DE INFRAESTRUCTURA.

Luego del análisis en la reciente sección se llega a la conclusión de que hay factores fundamentales a implementar como solución al presente problema.

- La implementación del uso obligatorio de certificados digitales de Seguridad (Key). Estas "llaves" serán creadas por el administrador del sistema permitiendo el acceso remoto para la administración y configuración de los dispositivos sea exclusivamente con el uso de *VPN* y Certificados digitales, que serán distribuidos solamente a los usuarios válidos.

- La implementación y cumplimiento de las prácticas de seguridad informática detalladas en el capítulo de modelo *COBIT /ISO/IEC 27002:2013.* Punto 9 - Gestión de Accesos, punto 10-Cifrado[20] (ISACA, 2012) para la generación, mantenimiento y baja de usuarios atendiendo a todas las normas descriptas para creación de contraseñas, tiempo de expiración, caracteres aceptados, uso de Tokens de seguridad para doble autenticación y tiempos de auditoria acordes al plan.

- La implementación del testeo de penetración y comprobación de cumplimiento de todas estas normas, exposición de vulnerabilidades y explotación.

- La implementación de Sub redes aisladas dentro de la red interna del proveedor de los servicios en la nube a fin de evitar que la subred sea contactada por otras subredes de otros clientes.

- Conocer si el proveedor de servicios en la nube está ofreciendo Hardware compartido o asignado en su totalidad por cliente.

- Implementar un sistema de monitoreo y control de Flujo por captura de datos por puerto espejo a través de las interfaces de red en velocidades de Gigabit a fin de obtener toda la información de tráfico de datos entrante y saliente y evaluar posibles patrones de ataques informáticos,

[20] http://www.iso27000.es/

4) ANÁLISIS Y ELABORACIÓN DE LA MATRIZ DE MITIGACIÓN DE RIESGOS.

Luego del detallado análisis realizado en los capítulos 2 y 3 respecto a los 7 puntos principales a considerar en la mitigación de riesgos en ciberseguridad para la implementación de la telefonía privada en la nube, se elabora como resultado, una matriz de riesgo incluyendo las soluciones y modelos propuestos para cada uno de ellos.

Esta matriz puede ser tomada también como referencia para aquellas empresas o entes de gobierno que estén planificando una migración de sus servicios telefónicas en la nube o bien para quien quiera tomar alguno de todos los puntos mencionados para futuras investigaciones.

Como la mayoría de los cambios tecnológicos, la migración de servicios hacia arquitecturas basadas en la nube trae acompañado un cambio de paradigma en relación a las cuestiones de ciberdefensa y ciberseguridad, creando también un entorno propicio a la exposición de las llamadas vulnerabilidades de día cero, problemas que aparecen en nuevas soluciones, que no son conocidos por el fabricante o proveedor hasta tanto son reportados y solucionados.

Es de esperar este concepto de día cero, que se aplica al mundo del software, pero es aplicable a la implementación de una nueva arquitectura, es este caso, para la telefonía *IP* basada en la nube que por su misma naturaleza (el hecho de estar en la nube para aprovechar las múltiples ventajas en costos y funcionalidades) deja expuesto y abierto el uso de protocolos y puertos de red a todo tipo de ataques relacionados al concepto de ciberguerra en el quinto dominio y la necesidad de implementar mejores prácticas de seguridad que incluyen todos los conceptos detallados en la Norma *ISO/IEC 27017* - Controles de Seguridad para Servicios en la nube , sumados a cada uno de los 7 puntos analizados en este trabajo, muchos de ellos muy diversos entre sí y que conforman un tema de estudio en sí mismo.

4.1) MATRIZ DE RIESGO ELABORADA PARA LOS 7 PUNTOS DE ANÁLISIS.

A modo de resumen se ha elaborado la **Tabla 3**, con la matriz de riesgo que incluye el análisis realizado de cada uno los 7 problemas presentados en la **Tabla 1** y en la que se agregan las soluciones para cada caso planteado.

	Tipo de Ataque	**Modo de Ataque**	**Problema causado**	**Solución Recomendación Modelo**
		Múltiples y simultaneas solicitudes de conexión hacia los puertos abiertos para registración de teléfonos *IP*.	Caída del servicio – imposibilidad de realizar llamadas telefónicas.	Configurar la solución de bloqueo para paquetes *SIP* en el *Session Border Controller.*
		Denegación de Servicio desde una fuente única.	Caída del servicio – imposibilidad de realizar llamadas telefónicas.	Los Valores de bloqueo deben ser cuando la cantidad de mensajes *SIP* es > a 300 mensajes en 5 segundos.
#1	Ataque de denegación de servicio (*DOS-Denial of Servic*e).	Denegación de servicio hacia un teléfono o dispositivo específico desde una o varias fuentes.	Caída del servicio para un dispositivo en particular. Imposibilidad de realizar llamadas telefónicas para un dispositivo en particular.	Los Valores iniciales de bloqueo deben ser cuando la cantidad de mensajes *SIP* es > 200 mensajes en 3 segundos.
		Denegación de servicio sigilosa desde una o varias fuentes.	Dificultad y demora en reportar un problema de vulnerabilidad causando daño por más tiempo.	Los Valores iniciales de alerta deben ser cuando la cantidad de mensajes de intentos de violación son de un promedio de 5 intentos en intervalos de 2 minutos Los Valores de bloqueo deben cuando la cantidad de mensajes *SIP* desde una fuente.

		Denegación de servicio Método “llamada rueda de reconocimiento” desde una fuente única.	Una vez terminada la fase de DOS “rueda de reconocimiento” comienza la fase de ataque pudiendo causar hasta caída del servicio – imposibilidad de realizar llamadas telefónicas.	única hacia un grupo de usuarios es de 10 mensajes por 1 minuto, 5 mensajes de *INVITE* o 5 mensajes *REGISTER* en 1 minuto.
		Denegación de Servicio desde una fuente única o distribuida hacia un server interno.	Cambio en la configuración del server provocando desde robo de información, caída del servicio, robo de llamadas generando cargos adicionales.	Los Valores de bloqueo en este caso varían según la capacidad y cantidad de teléfonos con los que cuenta el sistema y se debe calcular en cada caso siguiente las pautas para un sistema con 1000 Teléfonos / 100 llamadas simultaneas de capacidad. Mensajes *SIP* totales > 17000 en 10 segundos y luego 1700 cada 10s.
		Soluciones adicionales.	Cambio en la configuración del server provocando desde robo de información, caída del servicio, robo de llamadas generando cargos adicionales.	Implementar el uso de direcciones *DNS* y evitar publicar la *IP* en primera instancia. Implementar el área *DMZ* entre *firewall – SBC* y red interna del cliente.

	Tipo de Ataque	Modo de Ataque	Problema causado	Solución Recomendación Modelo
#2	Intento de Registrar usuarios desde personas no habilitadas e Intentos de realizar llamados telefónicos no autorizados.	Solicitudes de Registro de usuarios, probando con múltiples usuarios y contraseñas hasta encontrar un usuario válido.	Usuarios no autorizados pueden realizar llamadas telefónicas causando costos extras y riesgo de llamadas no deseadas. Eventos de suplantación de identidad. Robo de información por eventos de *Vishing.*	Implementar y seguir *COBIT5* Proceso *APO12- Guía de gestión de riesgos COBIT 5* para riesgos. Norma *ISO 27002* - Controles de Seguridad Item 9. Norma *ISO/IEC 27017* - Controles de Seguridad para Servicios Cloud. Adopción y uso de certificados digitales de Seguridad siguiendo Norma *ISO 27002* - Controles de Seguridad Item 10.
	Tipo de Ataque	Modo de Ataque	Problema causado	Solución Recomendación Modelo
#3	Suplantación de identidad.	Teléfonos registrados usando credenciales robadas pueden realizar llamadas o atender en nombre de otro usuario.	Robo de llamadas de larga distancia. *Vishing*. (suplantación de la Voz). Grabación no autorizada de llamadas.	Implementación de sistemas de identificación biométrica. Norma ISO 27002 - Controles de Seguridad Item 9. Uso de Certificados Digitales de Seguridad.

	Tipo de Ataque	Modo de Ataque	Problema causado	Solución Recomendación Modelo
#4	Robo de Certificados de Seguridad.	Teléfonos registrados usando credenciales robadas pueden realizar llamadas o atender en nombre de otro usuario. Captura de Datos en la red. Acceso remoto no autorizado a servidores (Item #7) para el robo de clave privada.	Robo de llamadas de larga distancia. *Vishing*. (suplantación de la Voz). Grabación no autorizada de llamadas. Desencriptado de paquetes de Voz sobre *IP* y escucha de llamadas en caso de robo de la clave privada.	Renovación periódica de los certificados e implementación de tiempo de expiración acorde Norma *ISO 27002* - Controles de Seguridad Item 10. Control de Registración basado en *IP* de origen cuando es posible (*White list*). Auditoria de disponibilidad de claves privadas visibles en archivos de los servidores.
	Tipo de Ataque	Modo de Ataque	Problema causado	Solución Recomendación Modelo
#5	Captura de Paquetes de Voz.	*Port Mirror.* Acceso remoto no autorizado a servidores (Item #7). Captura de Datos en la red. Acceso remoto al servidor de grabación de llamadas Robo de archivos de respaldo de grabaciones de llamadas. Suplantación de Identidad (item #3).	Escucha ilegal de llamadas y todas sus consecuencias asociadas.	Control de manejo de Certificados, expiración, copias según Norma *ISO 27002* - Controles de Seguridad Item 10. Implementación de Soluciones y Recomendaciones en item#7 (Acceso Remoto a servidores) Implementación de Soluciones y Recomendaciones en item#3 (Suplantación de identidad) Escaneo de Red periódica para detectar falsos nodos.

	Tipo de Ataque	Modo de Ataque	Problema causado	Solución Recomendación Modelo
#6	Ataque físico al Sitio del Proveedor de Nube Ataque físico a la conectividad de fibra del sitio.	Ataque físico o como parte de una guerra armada y/o criminal. Corte del tendido de Fibra óptica que conecta el sitio.	Caída del servicio – imposibilidad de realizar llamadas telefónicas. Robo o perdida de la información de usuarios y/o grabaciones de llamadas.	Realizar un relevamiento de infraestructura crítica de los Centro de Datos proveedores de servicios en la nube. incorporación de estos sitios críticos a la lista de sitios que componen la infraestructura crítica de las naciones, así como también incorporar el tendido de fibra óptica que conecta a estos sitios, el tendido eléctrico o las fuentes de energía alternativa que les proveen a los sitios. Determinar esquema de protección y guardia militar al sitio.
	Tipo de Ataque	Modo de Ataque	Problema causado	Solución Recomendación Modelo
#7	Acceso vía puertos de administración a la red interna privada y a los servers de infraestructura.	Ataques cibernéticos en sus distintos modos para ingreso indebido junto al uso de *Ransomware, malwares,* virus y *pishing.*	Desde caída total del servicio, robo y perdida de la información, hackeo total de los dispositivos y llamadas.	Implementación de sistemas de identificación biométrica. Norma *ISO 27002* - Controles de Seguridad Item 9 Control de manejo de Certificados, *Keys* y expiración, copias según.

				Norma *ISO 27002* - Controles de Seguridad Item 10. Realizar periódicamente el test de penetración. Analizar si el proveedor de servicios en la nube ofrece servidores físicos compartido para 2 clientes diferentes.

Tabla 3. Matriz de riesgo elaborada para la solución de Telefonía IP basada en la nube.

5) CONCLUSIONES Y TRABAJOS FUTUROS.

Mediante la exposición del marco teórico se repasó la evolución de la telefonía privada desde sus orígenes basados en sistemas en sito analógicos y digitales, pasando por los sistemas de telefonía *IP* hasta la arquitectura actual basada en la nube.

Esta arquitectura sin duda deviene en un cambio de paradigmas tanto en el aspecto financiero, en cuanto los dispositivos pasan de ser un costo de capital a un costo operativo (Capex[21] Versus Opex[22]), como en el aspecto tecnológico, que conlleva un radical cambio en la arquitectura presentando puertos y protocolos expuestos en la red con el fin de permitir la conectividad de usuarios, pero también abriendo una ventana a la exposición de ataques en el ciberespacio y siendo ahora parte de la guerra hibrida y asimétrica desarrollada en el quinto dominio.

Este último punto es objeto de estudio que lleva a demostrar, contrastar y comprobar en esta tesis cada uno de los aspectos y vulnerabilidades de esta solución, detallando para cada uno de ellos el impacto para la ciberdefensa de una nación y entes de gobierno, así como la ciberseguridad de las empresas que adoptan esté tipo de soluciones.

[21] Capex es la abreviación del término “Capital Expense” el cual es usado en ámbitos de trabajo financieros.
[22] Opex es la abreviación del término “Operating Expense”, el cual es usado en ámbitos de trabajo financieros.

La matriz elaborada es un punto de referencia para quienes estén desarrollando futuros proyectos de implementación o migración de los servicios de telefonía *IP* basada en la nube y para investigadores o empresas que quieran ahondar en la investigación de algunas de las propuestas más relevantes en este documento y que todavía no son parte de un estándar mundial.

En particular, el modelo teórico, SGIBA descripto en la sección 3.1.7, para la solución del problema de denegación de servicio distribuido (DDOS) en sistemas de telefonía *IP* basados en la nube y la incorporación de los Data center de proveedores en la nube como parte oficial de la infraestructura crítica de un país.

Indefectiblemente el mundo va hacia un crecimiento exponencial de dispositivos conectados a internet, el aumento de ciberataques, la aceleración en la aparición de nuevos *malwares,* el incremento de grupos organizados tanto de civiles o que responden a gobiernos o fuerzas militares y los grupos de ataques descentralizados para ataques persistentes, modelan un escenario futuro donde el control y la defensa del ciberespacio adoptando las mejores prácticas, conocimientos y formación de recursos, serán claves en el éxito de la adopción de las nuevas tecnologías, en el caso de esta tesis, los servicios de telefonía *IP* basada en la nube.

6) BIBLIOGRAFÍA Y REFERENCIAS.

Abdula, M. (2018). *The Cloud Adoption Playbook.* USA: John Wiley & Sons Inc.

Academy, L. (2019). Amazon Web Services Cloud Computing Solution Architect Practitioner Certification Course. USA: Linux Academy.

Aguilar, L. J. (2017). *Computación en La Nube.* Marcombo.

ARSAT. (2019, noviembre). *ARSAT*. Retrieved from ARSAT: https://datos.arsat.com.ar/visualizations/28598/fibra-optica-en-servicio/

AVAYA. (2019). *Session Border Controller Port Matrix.* USA: AVAYA.

AWS. (2019, noviembre). *AWS*. Retrieved from AWS: https://aws.amazon.com/about-aws/global-infrastructure/

Borja, C. T. (2019). *Sistemas Biometricos.* Retrieved from https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

Bunge, M. (1967). *La investigación científica.* Argentina: Editores Argentina.

CapitalOne. (2019). *CapitalOne*. Retrieved from CapitalOne: https://www.capitalone.com/

Clarke, R. A. (2010). *Cyber War.* USA: HarperCollins Publishers.

Daly, M. K. (2009). *The Advanced Persistent Threat.* Retrieved from http://static.usenix.org/event/lisa09/tech/slides/daly.pdf

datacenterknowledge. (2019). *datacenterknowledge*. Retrieved from datacenterknowledge: https://www.datacenterknowledge.com/cloud/analysts-there-are-now-more-500-hyperscale-data-centers-world

Dean, T. (2010). *Network+ Guide to networks.* Boston : Course Technology.

Diogenes, Y. (2018). *Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics.* UK: Packt Publishing.

Dwivedi, H. (2008). *Hacking VoIP: Protocols, Attacks, and Countermeasures.* USA: William Pollock.

Eco, H. (1995). *Cómo se hace una tesis.* Spain: Editorial Gedisa.

eldiariodemadryn. (2019). *eldiariodemadryn*. Retrieved from eldiariodemadryn: https://www.eldiariodemadryn.com/2019/10/reiterados-cortes-a-la-fibra-optica-tienen-en-vilo-a-la-comunidad-de-trelew/

Erl, T. (2013). *Thomas Erl . Cloud Computing: Concepts, Technology & Architecture.* USA: Arcitura Education Inc.

Estrada, A. C. (2011). *Seguridad por Niveles.* RPI (Madrid): 03/119554.9/11.

Gartner. (06 de 2019). Obtenido de Gartner Inc.: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

GBA, B. O. (2019, noviembre). *Boletin Oficial GBA*. Retrieved from Boletin Oficial GBA: https://www.boletinoficial.gba.gob.ar/sections/9936/view

Google. (2019, noviembre). *Google Maps* . Retrieved from Google Maps: https://goo.gl/maps/8wDZjsGaZQRPxyst8

Google. (2019, noviembre). *Google maps en Plant City*. Retrieved from Google maps: https://www.google.com/maps

Google. (2019, noviembre). *Google maps en Quebec*. Retrieved from Google maps: https://goo.gl/maps/4Uvuo7mbwwbu94dw8

Google. (2019, noviembre). *Google Street view Quebec*. Retrieved from Google Street View Quebec: https://goo.gl/maps/4Uvuo7mbwwbu94dw8

Hubbard, D. W. (2016). *How to Measure Anything in Cybersecurity Risk.* USA: John Willey & Sons inc.

IEEE. (2019, noviembre). *IEEE*. Retrieved from https://www.ieee.org/

IETF. (2019, noviembre). *RFC 1122 Requirements for Internet Hosts -- Communication Layers.* Retrieved from IETF: https://www.ietf.org/rfc/rfc1122.txt

IETF. (2019, noviembre). *RFC 3711 The Secure Real-time Transport Protoco SRTP.* Retrieved from IETF: https://tools.ietf.org/html/rfc3711

IETF. (2019, noviembre). *RFC 7478 Web Real-Time Communication Use Cases and Requirements.* Retrieved from IETF: https://tools.ietf.org/html/rfc7478

IETF. (2019, noviembre). *RFC2616 Hypertext Transfer Protocol -- HTTP/1.1.* Retrieved from IETF: https://tools.ietf.org/html/rfc2616

IETF. (2019, noviembre). *RFC3261 SIP Session Initiation Protocol.* Retrieved from IETF: https://tools.ietf.org/html/rfc3261

IETF. (2019, noviembre). *RFC3550 RTP: A Transport Protocol for Real-Time Applications.* Retrieved from IETF: https://tools.ietf.org/html/rfc3550

ISACA. (2012). *COBIT 5 Procesos Catalizadores.* ISACA.

Linux. (2019, noviembre). *Linux Org*. Retrieved from Linux Org: https://linux.org/

McAffe. (2019). *cloud adoption risk report*. Obtenido de McAffe: https://cloudsecurity.mcafee.com/cloud/en-us/forms/white-papers/wp-cloud-adoption-risk-report-2019-banner-cloud-mfe.html

Microsoft. (2019, noviembre). *Microsoft Azure Clou Map*. Retrieved from Microsoft Azure: https://azure.microsoft.com/en-us/

Microsoft. (2019, noviembre). *Microsoft Corporation*. Retrieved from Microsoft Corporation: https://www.microsoft.com/en-us/windows/

Morgan., J. (2019). *J.P. Morgan.* Retrieved from J.P. Morgan.: https://www.jpmorgan.com

novachubut.com. (2019). *novachubut.com*. Retrieved from novachubut.com: http://www.novachubut.com/nota.asp?n=2019_10_27&id=25966&id_tiponota=24

radio3cadenapatagonia. (2019). *radio3cadenapatagonia*. Retrieved from radio3cadenapatagonia: https://radio3cadenapatagonia.com.ar/movistar-confirmo-actos-de-vandalismo-en-su-fibra-optica/

Rosaleño, D. e. (2019, noviembre). *Diario el Rosaleño*. Retrieved from Diario el Rosaleño: http://elrosalenio.com.ar/noticias/16/10/2019/10027843/el-arribo-de-amazon-a-coronel-rosales-genera-expectativas

Sampieri, R. H. (2014). *Metodología de la investigación.* Mexico: McGraw Hill.

sanjuan8. (2019). *sanjuan8*. Retrieved from sanjuan8: https://www.sanjuan8.com/mendoza/el-corte-supercanal-fue-un-acto-vandalismo-denuncio-esa-empresa-n1628890.html

Services, I. G. (2007). *The Vishing Guide.* Retrieved from http://www.infosecwriters.com/text_resources/pdf/IBM_ISS_vishing_guide_GOllmann.pdf

shodan. (2019). *shodan*. Retrieved from shodan: https://www.shodan.io/search?query=SBC

Singer., P. W. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* UK: Oxford University Press.

Snowden, E. (2019). *Vigilancia Permanente.* Planeta.

Stalling, W. (2000). *Comunicaciones y Redes de Computadores.* Prentice Hall.

Sullivan, F. &. (2019). *Improving understanding on Cloud & Enterprise Communications Technologies Market Opportunities in Latin America.* Frost & Sullivan.

TImes, N. Y. (2019). *New York Times*. Retrieved from New York TImes: https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html

Wikileaks. (2019, noviembre). *Wikileaks*. Retrieved from Wikileaks: https://wikileaks.org/amazon-atlas/document/AmazonAtlas_v1/

Wireshark. (2019). *Wireshark*. Retrieved from Wireshark: https://www.wireshark.org/

WSJ. (2019). *WSJ*. Retrieved from WSJ: https://www.wsj.com/articles/capital-one-breach-casts-shadow-over-cloud-security-11564516541

Wu, C. (2015). *Cloud Data Centers and Cost Modeling.* USA: Todd Green.