UNIVERSIDAD CATÓLICA ANDRÉS BELLO
FACULTAD DE INFENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

MODELO DE SEGURIDAD IMS PARA EL ASEGURAMIENTO DE PLATAFORMA Y SERVICIOS – FASE CONCEPTUAL

TRABAJO ESPECIAL DE GRADO

Presentado ante la

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

Como parte de los requisitos para optar al título de

INGENIERO DE TELECOMUNICACIONES

REALIZADO POR Monegui Rosas, Fernando Roberto
Suarez Laguna, Ignacio

TUTOR Ing. Eugenio Flores

FECHA Caracas, 1 de Marzo de 2012

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
FACULTAD DE INFENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

MODELO DE SEGURIDAD IMS PARA EL ASEGURAMIENTO DE PLATAFORMA Y SERVICIOS – FASE CONCEPTUAL

REALIZADO POR Monegui Rosas, Fernando Roberto
Suarez Laguna, Ignacio

TUTOR Ing. Eugenio Flores

FECHA Caracas, 1 de Marzo de 2012

Resumen

MODELO DE SEGURIDAD IMS PARA EL ASEGURAMIENTO DE PLATAFORMA Y SERVICIOS – FASE CONCEPTUAL

Fernando Roberto Monegui Rosas
fernandomonegui@gmail.com
Ignacio Suarez Laguna
ignacio.suarez.88@gmail.com

A medida que la tecnología avanza nos vemos en la necesidad de incluir nuevos y mejores servicios, así como su integración y reducción de costos al operador. La empresa de Telecomunicaciones en Venezuela (CANTV) está evolucionando a nuevas tecnologías, para la convergencia de servicios, garantizando el funcionamiento y la operación, con la incorporación de diseños/arquitecturas seguros, así como mecanismos de seguridad para el aseguramiento de las plataformas y los servicios. El siguiente trabajo de grado tiene su fundamento en la definición de un modelo conceptual de seguridad que permita la unificación de criterios de evaluación, definición de estrategias y aspectos relevantes en materia de Seguridad que garanticen el óptimo funcionamiento de las plataformas convergentes (IMS), definiendo los aspectos mandatorios para una eventual implementación cumpliendo con los requerimientos de Seguridad, a través del estudio y evaluación de la actual plataforma NGN para determinar vulnerabilidades y brechas existentes, elaborando las matrices de riesgos pertinentes para la elaboración de una arquitectura conceptual que especifique a través de diagramas, esquemas y análisis los requerimientos y especificaciones técnicas a nivel de capa de control, que garanticen la continuidad del negocio y los servicios a los usuarios finales con la calidad de servicio exigida.

Palabras clave: Tecnología, Convergencia, IMS, NGN, Seguridad, Riesgos, Modelo Conceptual, Calidad de Servicios, Mitigación, Arquitectura.

Abstract

IMS SECURITY MODEL FOR ASSURANCE SERVICES AND PLATFORM - CONCEPTUAL PHASE

Fernando Roberto Rosas Monegui
fernandomonegui@gmail.com
Ignacio Suarez Laguna
ignacio.suarez.88 @ gmail.com

As technology advances we feel the need to include new and improved services and their integration and cost reduction to the operator. The telecommunications company in Venezuela (CANTV) is evolving to new technologies for converged services, guaranteeing the performance and operation, with the addition of secure designs / architectures and security mechanisms for the insurance of the platforms and services. This Thesis is based on the definition of a security conceptual model that allows the unification of evaluation criteria, defining strategies and relevant aspects concerning security to ensure the optimal functioning of convergent platforms (IMS), defining mandatory aspects for possible implementation in compliance with the requirements of Security, through the study and evaluation of the current NGN platform to identify vulnerabilities and breaches, developing risk matrices relevant to the development of a conceptual architecture specified by diagrams, charts and analysis requirements and technical specifications at control layer, to ensure business continuity and service to end users with the quality of service required.

Keywords: Technology, Convergence, IMS, NGN, Security, Risk, Conceptual Model, Quality of Services, Mitigation, Architecture.

Dedicatorias

Le dedico esta tesis a todos los que creyeron en mí, a Dios, a mis amigos,
a mi familia y mis padres, María Rosa e Ignacio, por todo su amor y cariño durante
este largo camino.
A mi abuelo Goyo y mis abuelas,
siempre estarán presentes en mi corazón. Los amo.
A Jeraldin,
por estar a mi lado siempre, en las buenas y en las malas.
Todas aquellas personas que me dieron su apoyo incondicional,
esto es gracias a ustedes.
Sin sacrificio no existe recompensa.
Ignacio Suarez

A mis Padres Fernando y Alelí,
por la paciencia, comprensión, apoyo y el amor que siempre me han dado.
A mis hermanos Alejandro y Diego,
por ser quiénes son y por hacerme feliz en tantos buenos momentos.
A Jacklyn,
por el amor y apoyo incondicional durante este largo viaje.
Y a mis familiares y amigos,
por sus buenos consejos y por estar ahí siempre que los necesité.
Y a todos los que creyeron en mí,
Por ustedes y para ustedes es mi triunfo.
Fernando Monegui

Agradecimientos

Primeramente agradecemos a Dios, por siempre estar presente, llenándonos de bendiciones, darnos la fuerza y el valor para superar los obstáculos que se han presentado en nuestro camino.

A nuestra familia, papas, hermanos y abuelos, por todo el apoyo incondicional, son los pilares de nuestro éxito y somos el resultado de todos los valores, trabajo y dedicación puesto en nosotros. Los queremos de corazón.

Agradecimientos especiales a nuestro tutor, Eugenio Flores, por su apoyo y orientación en la realización del presente trabajo, y estar ahí presente para nosotros en las buenas y en las malas.

A Francisco Lagos, Antonieta Lobo, Eduardo Vásquez, Jody Gener y demás personalidades, por su disposición y acertada guía para alcanzar los objetivos planteados.

A la Compañía Nacional Teléfonos de Venezuela (CANTV), por permitirnos realizar nuestro primer trabajo profesional, proporcionándonos valiosa información para la elaboración de nuestro Trabajo de Grado.

A la Universidad Católica Andrés Bello y sus profesores, por ser nuestra Alma Mater y habernos brindado los conocimientos necesarios para ser los profesionales que somos hoy en día, y por hacernos sentir orgullosos de ser Ucabistas.

A todas las personas que nos influenciaron de forma positiva y nos brindaron su cariño y apoyo para formarnos como profesionales integrales, productivos para nuestro país. Con valor, sacrificio y humildad se consigue todo lo que uno se proponga.

Índice General

Índice de Figuras

Índice de Tablas

Introducción

Actualmente es necesario seguir evolucionando a nuevas tecnologías, en este caso nos referimos al mundo de las telecomunicaciones donde la demanda y el crecimiento de este sector va cada día en aumento. Hoy en día es mayor la necesidad de la convergencia de los servicios y demás aplicaciones, garantizando el funcionamiento y la operación, al igual que el aseguramiento de las plataformas, para brindar servicios de calidad. Por estas razones el siguiente Trabajo Especial de Grado se basa en el desarrollo y descripción de un modelo de seguridad, donde se manejen e incluyan arquitecturas y diseños de red seguros, que además es complementado con pruebas de laboratorio en cuanto a seguridad de la operación, para la identificación de riesgos en la capa de control y elementos asociados, para la prestación de servicios de voz y datos (tanto en la plataforma NGN como en la IMS). La proposición e implementación de un modelo de seguridad deben ser requisitos indispensables siempre que se desee implementar una nueva tecnología en cualquier empresa, para establecer los mecanismos de seguridad necesarios para el aseguramiento de la plataforma y los servicios, evitando que estas se encuentren comprometidas, y actuando de forma preventiva ante eventos de negación o degradación del servicio y fraude. Es mandatorio la elaboración de documentos conceptuales que definan estrategias a seguir, mecanismos de prevención, detección y corrección de fallas que mitiguen los riesgos presentes en las plataformas. Además de lo señalado anteriormente se pretende que el presente documento sirva como guía de análisis y estudio para una posible implementación de la tecnología IMS por parte de CANTV.

Para lograrlo se iniciará con una investigación acerca las definiciones importantes de la metodología de riesgos, seguido por las redes por conmutación de circuitos, las redes telefónicas públicas conmutadas (por sus siglas en inglés PSTN), y las redes paquetizadas, para finalmente llegar a las Redes de Próxima Generación (por sus siglas en ingles NGN). Posterior a esto se realizó una investigación exhaustiva para

analizar los conceptos, elementos, funcionamiento, aplicaciones y servicios generales de las redes IMS.

Para la elaboración del marco teórico del presente trabajo, se utilizará la información documentada en trabajos de grado, documentos y artículos especializados elaborados y publicados previos a la elaboración del presente trabajo. Actualmente la Gerencia de Seguridad de la Operación (GSOS) maneja el ISO 31000, como estándar para la identificación y gestión de los riesgos que pueden afectar la operación de la compañía en el cumplimiento de sus objetivos, de forma sistemática y transparente. De igual forma CANTV utiliza ETOM (*Enhanced Telecom Operations Map*), el cual sirve como guía para la empresa, ya que define el estándar más ampliamente utilizado y aceptado para los procesos de negocio en la industria de las telecomunicaciones. El modelo ETOM describe el alcance completo de los procesos de negocio requeridos por un proveedor de servicios y define los elementos clave y la forma en que interactúan. Estos estándares son manejados por la herramienta ERA (*Enterprise Risk Assesor*), el cual es un Software que permite a CANTV implementar una solución flexible y global para la gestión empresarial, el cual se encarga de documentar y analizar los riesgos identificados.

Una vez realizadas las dos primeras fases de investigación de nuestro trabajo, se manejarán la información y los conocimientos necesarios para proceder a las evaluaciones de las diferentes tecnologías (NGN e IMS), en cuanto a la seguridad de la operación, enfocándose en la capa de control, para garantizar buenas prestaciones de los servicios, detectando las posibles fallas o vulnerabilidades, potenciales o existentes, y el impacto de cada una de ellas.

Para la evaluación de ambas tecnologías, se utilizaron como apoyo fundamental los conocimientos adquiridos anteriormente y adicionalmente se realizaron entrevistas a expertos en los temas abarcados, complementadas por la ejecución de protocolos de pruebas en cuanto a seguridad de la operación. Mediante el levantamiento de

información y las entrevistas se detectaron vulnerabilidades desde el punto de vista teórico, y por medio de las pruebas realizadas de detectaron los riesgos presentes desde un enfoque práctico.

Después de realizadas las evaluaciones de ambas tecnologías, el estudio y la documentación de cada una de las vulnerabilidades identificadas, se realizará la presentación y el análisis de los resultados obtenidos en las fases anteriores. Finalmente en base a las conclusiones obtenidas de analizar los resultados, se realizará el diseño conceptual del modelo que contendrá la arquitectura y las especificaciones técnicas de seguridad en cuanto a la tecnología IMS, que garantice la continuidad de la prestación y la convergencia de los servicios con la calidad de servicio exigida.

Acrónimos

3GPP: *Third Generation Partnership Project*

3GPP2: *Third Generation Partnership Project 2*

A

AAA: *Authentication, Authorization, Accounting*

AG: *Access Gateway*

AH: *Authentication Header*

ANF: *Access Network Functions*

AOR: *Address of Record*

API: *Application Programming Interface*

B

BG: *Business Gateway*

BGCF: *Breakout Gateway Control Function*

BHCA: *Busy Hour Call Attempt*

C

CAC: *Call Admittance Control*

CAMEL: *Customized Applications for Mobile Network Enhanced Logic*

CAP: *CAMEL Application Part*

CDMA: *Code Division Multiple-Access*

CDR: *Call Detail Record*

COPS: *Common Open Policy Service*

CS: *Circuit Switched*

CSCF: *Call State Control Function*

D **DCC:** *Diameter Credit Control*

DDos: *Distributed Denial of Service*

DHCP: *Dynamic Host Configuration Protocol*

DNS: *Domain Name System*

DoS: *Denial of Service*

DSL: *Digital Subscriber Line*

DTMF: *Dual-Tone Multi-Frequency*

E **EDGE:** *Enhanced Data Rates for GSM Evolution*

ESP: *Encapsulating Security Payload*

ETSI: *European Telecommunications Standards Institute*

F **FQDN:** *Full Qualified Domain Name*

G **GPRS:** *General Packet Radio Service*

GSM: *Global System for Mobile Communications*

H **HSDPA:** *High-Speed Downlink Packet Access*

HSS: *Home Subscriber Server*

HTTP: *Hyper Text Transfer Protocol*

I **I-CSCF:** *Interrogating-Call State Control Function*

IETF: *Internet Engineering Task Force*

IKE: *Internet Key Exchange*

IMS: *IP Multimedia Subsystem*

IP: *Internet Protocol*

IPSec: *IP Security*

ISDN: *Integrated Services Digital Network*

ITU: *International Telecommunication Unit*

L **LAN:** *Local Area Network*

LCS: *Location Services*

M **MAN:** *Metropolitan Area Network*

MCU: *Multipoint Control Unit*

MDF: *Main Distribution Frame*

MGC: *Media Gateway Controller*

MGW: *Media Gateway*

MitM: *Man in the Middle*

MPLS: *Multi-Protocol Label Switching*

MRFP: *Multimedia Resource Function Processor*

MSC: *Mobile Switching Center*

MSML: *Media Server Markup Language*

N **NACF:** *Network Attachment Control Functions*

NAPT: *Network Address and Port Translation*

NAT: *Network Address Translation*

NGN: *Next Generation Networks*

O **OSA:** *Open Service Architecture*

OSI: *Open System Interconnection*

P **PCM:** *Pulse Code Modulation*

P-CSCF: *Proxy-Call State Control Function*

PDF: *Policy Decision Function*

PDP: *Policy Decision Point*

PEP: *Policy Enforcement Point*

POTS: *Plain Old Telephone Service*

PS: *Packet Switched*

PSTN: *Public Switched Telephone Network*

Q **QoS:** *Quality of Service*

R **RACF:** *Resource and Admission Control Functions*

RFC: *Request for Comment*

RG: *Residential Gateway*

RSVP: *Resource Reservation Protocol*

RTCP: *Real-Time Control Protocol*

RTP: *Real-Time Transport Protocol*

S **SBC:** *Session Border Controller*

SCP: *Signal Control Point*

SCS: *Service Capability Server*

S-CSCF: *Serving-Call State Control Function*

SCTP: *Stream Control Transmission Protocol*

SDP: *Session Description Protocol*

SIP: *Session Initiation Protocol*

SIP-UA: *SIP User Agent*

SLA: *Service Level Agreement*

SLF: *Subscriber Location Functions*

SMTP: *Simple Mail Transfer Protocol*

SSF: *Service Switching Function*

SSP: *Service Switching Point*

STP: *Signal Transfer Point*

T

TCP: *Transmission Control Protocol*

TG: *Trunking Gateway*

THIG: *Topology Hiding Inter-Network Gateway*

TISPAN: *Telecoms & Internet Converged Services & Protocol for Advanced Networks*

TLS: *Transport Layer Security*

TPS: *Triple Play Services*

U

UA: *User Agent*

UAC: *User Agent Client*

UAS: *User Agent Server*

UDP: *User Datagram Protocol*

UE: *User Equipment*

UMTS: *Universal Mobile Telecommunications System*

URI: *Uniform Resources Identifiers*

URL: *Uniform Resource Locator*

UTRAN: *UMTS Terrestrial Radio Access Network*

V **VoAG:** *Voice over ATM Gateway*

VOIP: *Voice over IP*

W **WAN:** *Wide Area Network*

WCDMA: *Wideband Code Division Multiple-Access*

WLAN: *Wireless Local Area Network*

Capítulo I
Planteamiento del proyecto

Este capítulo hace referencia a las causas ó motivaciones para la realización de este Trabajo Especial de Grado, explicando el problema actual, la necesidad de resolver dicho problema, planteando el objetivo general a cumplir y los objetivos específicos que contribuirán a resolver el problema. De igual forma se observa la justificación para entender el planteamiento de este proyecto y, finalmente, los límites o alcances del proyecto.

I.1 Planteamiento del problema

Los seres humanos siempre han visto la necesidad de comunicarse unos con otros y buscar que sea de la manera más segura y confiable posible. Hemos estado viviendo los cambios tecnológicos que permiten comunicarnos, superando barreras que antes parecían infranqueables, pero así como avanzan los métodos de comunicación también lo hacen los atacantes y posibles eventos que atentan contra la continuidad, la calidad y la seguridad en las comunicaciones. La transmisión de voz o datos a grandes distancias ya no supone un obstáculo, es una realidad, y una necesidad en nuestros días.

Desde Bell (1876) que diseñó e implementó el primer teléfono, pasando por numerosos cambios y evoluciones a esta idea original, hasta conocer las comunicaciones de voz como las conocemos hoy en día, que nos permiten estar conectados con nuestros amigos y familiares sin importar las distancias.

A medida que la tecnología avanza vemos la necesidad de incluir nuevos y mejores servicios, así como su integración. Desde el año 2005, CANTV como empresa de

Telecomunicaciones del Estado Venezolano, ha iniciado el camino de la modernización e instalación de nuevas tecnologías en relación a la red de telefonía fija, de la cual se destaca la Red de Próxima Generación o NGN, tecnología basada en la conmutación de paquetes.

A la fecha es necesario seguir evolucionando a nuevas tecnologías para la convergencia de servicios, donde es necesario garantizar su funcionamiento y operación, pero también Asegurar las plataformas, servicios y clientes, con el fin de evitar eventos de negación o degradación del servicios, fraude entre otros.

En la actualidad, el sector de las telecomunicaciones se encuentra en constante cambio dada la necesidad y demanda de nuevos servicios, así como llegar a cubrir mayores áreas. En este sentido, es necesaria la convergencia de servicios, tratando de evitar cualquier impacto, optimizar las redes, la calidad del servicio y la gestión, entre otros. Previo a la implementación de una tecnología nueva, es necesario el estudio de la misma y determinar mecanismos de control para la determinación de los riesgos presentes o futuros en caso de una posible adopción de la tecnología. Para la implementación de cualquier plataforma o servicio, es necesario contar con la evaluación de riesgos y cómo afectan la operación y el correcto funcionamiento de las plataformas legadas. De esta forma, el propósito de este Trabajo Especial de Grado, tomando en cuenta las necesidades mencionadas anteriormente, es la definición de un modelo conceptual de seguridad que permita la unificación de criterios de evaluación, definición de estrategias y aspectos relevantes en materia de Seguridad que garanticen el óptimo funcionamiento de las plataformas convergentes (IMS), definiendo los aspectos mandatorios para una eventual implementación cumpliendo con los requerimientos de Seguridad, para ello será necesario el estudio de la tecnología actual de conmutación de paquetes (NGN) y de la tecnología de convergencia (IMS).

I.2 Objetivo General

Desarrollar un Modelo de Seguridad IMS para el Aseguramiento de Plataforma y Servicios - Fase Conceptual.

I.3 Objetivos Específicos

- Investigar y analizar conceptos, aplicaciones y servicios de la plataforma de Próxima Generación (NGN) e implementación caso CANTV.
- Investigar y analizar conceptos, aplicaciones y servicios de plataformas IMS (*IP Multimedia Subsystem*).
- Evaluar la tecnología NGN en cuanto a seguridad de la operación: capa de control y elementos asociados, para la prestación de servicios de voz y datos.
- Evaluar la tecnología IMS en cuanto a seguridad de la operación: capa de control y elementos asociados, para la prestación de servicios de voz y datos.
- Desarrollar documento conceptual que contenga: arquitectura conceptual y especificaciones técnicas de seguridad en cuanto a la tecnología IMS, que garantice la continuidad en la prestación y convergencia de los servicios.

I.4 Justificación

Actualmente CANTV es la empresa líder de telecomunicaciones a nivel nacional, se encuentra en constante crecimiento y expansión de servicios y nuevas tecnologías, comprometido con brindar a sus clientes cada vez mejores servicios de calidad y más robustos en su seguridad.

Para una eventual migración de plataforma y servicios es necesaria una excelente planificación y estudio del impacto que tendrán estas tecnologías de ser

implementadas por la empresa, y si la inversión es justificada por ganancias a futuro y por su impacto social llevando las telecomunicaciones en Venezuela a mayor cantidad de personas, mejorando las relaciones con sus clientes, así como el soporte de los sistemas y tecnologías actuales. Hoy en día, las empresas de telecomunicaciones a nivel mundial al igual que CANTV, se encuentran con la necesidad de la convergencia total de sus servicios, en una plataforma común, apostando por una tecnología nueva e innovadora como lo es la tecnología IMS.

La rápida proliferación de la tecnología IP (Internet) como mayor medio de comunicación usado en el mundo, está transformando radicalmente el sector tecnológico. La adopción de IMS (*IP Multimedia Subsystem*) le permitirá a CANTV integrar las llamadas fijas con las móviles, la voz con el acceso a Internet de banda ancha (*VoIP*), la televisión y el vídeo, y las aplicaciones multimedia residenciales y empresariales. Es un reto importante la definición de estrategias y reglas comunes que permitan la convergencia de servicios, así como la interacción y continuidad de los sistemas legados, como la de facturación, entre otros incorporando los mecanismos de seguridad que prevengan y controlen situaciones irregulares en los servicios, sistemas y equipos asociados. El objetivo de este Trabajo Especial de Grado radica en la elaboración de un documento teórico, que exponga el modelo de seguridad IMS para el Aseguramiento de la plataforma y servicios.

I.5 Limitaciones y Alcances

Limitaciones

- Las herramientas con las cuales se contará para realizar las evaluaciones, ya que es necesario realizar pruebas previas.
- Equipos IMS en laboratorio, los cuales poseen configuraciones básicas y no se encuentran todos los equipos utilizados en este tipo de plataforma.
- Dado que este tipo de plataformas normalmente cuentan con aplicaciones propietarias, se hace difícil cumplir con exactitud el Decreto 3390, publicado

en Diciembre del año 2004, el cual se dispone que la APN (Administración Pública Nacional) emplee prioritariamente SL (Software Libre) desarrollado con estándares abiertos, en sus sistemas, proyectos y servicios informáticos. Sin embargo, para la elaboración de las pruebas se utilizaron herramientas de tráfico de llamadas de *VoIP* de código abierto, así como también se recomienda que las interfaces y otros aplicativos permitan la integración con herramientas de la empresa favoreciendo el Software Libre

Alcances

- El trabajo de grado es desarrollado en la empresa de telecomunicaciones CANTV.
- Las evaluaciones de seguridad de la operación y servicios realizadas están orientadas al Acceso, Capa de Control de la Plataforma NGN de CANTV en el laboratorio.
- Las evaluaciones realizadas están orientadas al Acceso, Capa de Control de la Plataforma IMS en el laboratorio de CANTV.
- Evaluaciones de Seguridad de la Operación y Servicios están orientadas a la identificación de Riesgos / Vulnerabilidades en la Plataforma NGN.
- Las Evaluaciones de Seguridad de la Operación y Servicio están orientadas a la identificación de Riesgos / Vulnerabilidades en la Plataforma IMS.
- Desarrollar Modelo, que conste de Arquitectura y especificaciones técnicas de Seguridad de la Operación y Servicios para la Plataforma IMS.
- El modelo resultante está orientado a definir las estrategias de seguridad, para brindar robustez a una eventual implementación y operación de la Plataforma IMS en CANTV.

Capítulo II
Marco Teórico

En este capítulo del Trabajo Especial de Grado se describen las definiciones importantes acerca de la metodología de riesgos, pasando por tecnologías de conmutación de circuitos y terminando en la conmutación de paquetes, donde finalmente se explican las definiciones y principales características tanto de las redes NGN (*Next Generation Networks*) como de la tecnología IMS (*IP Multimedia Subsystem*) que es el tema central de la investigación. Todos estos conceptos fueron de vital importancia para la realización del presente Trabajo Especial de Grado.

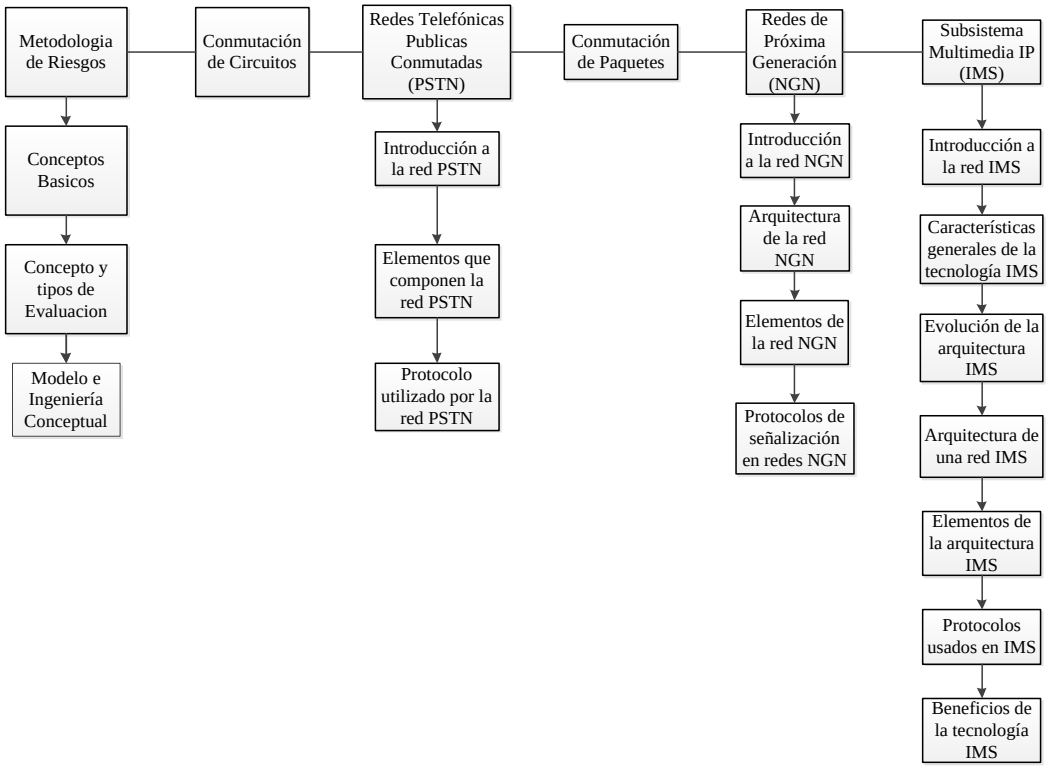


Figura 1: Esquema de Marco Teórico.

Fuente: [Elaboración propia].

II.1 Definición y conceptos importantes de la Metodología de Riesgos

El principal objetivo de la metodología de riesgos es mejorar la objetividad y transparencia, y ofrecer bases sólidas para la evaluación de las necesidades y la preparación de la planificación. A continuación se presentan una serie de conceptos importantes referentes a lo que trata la metodología de riesgos. (Compañía Anónima Nacional Teléfonos de Venezuela. CANTV, 2010)

II.1.1 Conceptos Básicos.

Riesgo: se trata de un evento presente o futuro e incierto que podría tener repercusiones negativas para el logro de los objetivos de una organización.

Probabilidad de riesgo: se trata de la probabilidad de que un riesgo ocurra. Los factores que se tienen en cuenta para determinar la probabilidad son los siguientes: el origen de la amenaza, el potencial del origen, la naturaleza de la vulnerabilidad y, por último, la existencia de mecanismos de control y la eficacia de éstos. La probabilidad puede describirse como alta, media y baja.

- Alta: el evento ocurrirá en la mayoría de casos
- Media: el evento ocurrirá probablemente en muchos casos
- Baja: el evento puede ocurrir en algún momento

Impacto del riesgo: se trata del impacto probable que podría tener el riesgo sobre la organización en caso de que ocurriera. Cabe mencionar que no todas las amenazas tendrán el mismo impacto, ya que cada sistema de la Organización tiene distinto valor. La magnitud del impacto también puede clasificarse como alta, media y baja.

- Alta: impacto grave sobre las operaciones, reputación o situación de financiación

- Media: impacto importante sobre las operaciones, reputación o situación de financiación
- Baja: impacto menos importante sobre las operaciones, reputación o situación de financiación

Consecuencia: el producto de un evento expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia. Podría haber un rango de productos posibles asociados a un evento.

Control de riesgos: la parte de administración de riesgos que involucra la implementación de políticas, estándares, procedimientos y cambios físicos para eliminar o minimizar los riesgos adversos.

Evaluación de riesgo: el proceso global de análisis de riesgo y evaluación de riesgo, así como también el proceso utilizado para determinar las prioridades de administración de riesgos comparando el nivel de riesgo respecto de estándares predeterminados, niveles de riesgo objetivos u otro criterio.

Evento: un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo particular.

Matriz de riesgo: Es una combinación de medición y priorización de riesgos, que consiste en la graficación de los mismos en un plano cartesiano, donde el eje de las X identifica la consecuencia que un factor dado tiene, y el eje de la Y identifica la probabilidad de ocurrencia de dicho factor.

Mitigación (reducción): Planificación y ejecución de medidas de intervención dirigidas a reducir o disminuir el riesgo. La mitigación es el resultado de la aceptación de que no es posible controlar el riesgo totalmente; es decir, que en muchos casos no es posible impedir o evitar totalmente los daños y sus consecuencias y sólo es posible atenuarlas.

Monitoreo: comprobar, supervisar, observar críticamente, o registrar el progreso de una actividad, acción o sistema en forma sistemática para identificar cambios.

Organización: una compañía, firma, empresa o asociación, u otra entidad legal o parte de ella, sea o no incorporada, pública o privada, que tiene sus propias funciones y administración.

Probabilidad: la probabilidad de un evento específico o resultado, medido por el coeficiente de eventos o resultados específicos en relación a la cantidad total de posibles eventos o resultados.

Reducción de riesgos: una aplicación selectiva de técnicas apropiadas y principios de administración para reducir las probabilidades de una ocurrencia, o sus consecuencias, o ambas.

Tratamiento de riesgos: selección e implementación de opciones apropiadas para tratar el riesgo. (Compañía Anónima Nacional Teléfonos de Venezuela. CANTV, 2010)

II.1.2 Concepto de Evaluación y sus tipos.

Proceso que tiene como finalidad determinar el grado de eficacia y eficiencia, con que han sido empleados los recursos destinados a alcanzar los objetivos previstos, posibilitando la determinación de las desviaciones y la adopción de medidas correctivas que garanticen el cumplimiento adecuado de las metas presupuestadas.

Evaluación continua: pretende superar la relación evaluación-examen o evaluación-calificación final, y centra la atención en otros aspectos que se consideran de interés para la mejora del proceso. Por eso, la evaluación continua se realiza a lo largo de todo el proceso y pretende describir e interpretar, no tanto medir y clasificar.

Evaluación criterial: A lo largo del proceso, la evaluación criterial compara el progreso del proceso en relación con metas graduales establecidas previamente a partir de la situación inicial. Por tanto, fija la atención en el progreso personal, dejando de lado la comparación con la situación en que se encuentran otras personas.

Evaluación formativa: Recalca el carácter educativo y orientador propio de la evaluación. Se refiere a todo el proceso, desde la fase de detección de las necesidades hasta el momento de la evaluación final o sumativa. Tiene una función de diagnóstico en las fases iniciales del proceso, y de orientación a lo largo de todo el proceso e incluso en la fase final, cuando el análisis de los resultados alcanzados tiene que proporcionar pistas para la reorientación de todos los elementos que han intervenido en él.

Evaluación global: Considera comprensivamente todos los elementos y procesos que están relacionados con aquello que es objeto de evaluación. Si se trata de la evaluación del proceso, la evaluación global fija la atención en el conjunto de las áreas y, en particular, en los diferentes tipos de contenidos (hechos, conceptos y sistemas conceptuales; procedimientos; actitudes, valores y normas).

Evaluación inicial: Se realiza al iniciarse cada una de las fases del proceso, y tiene la finalidad de proporcionar información sobre los conocimientos previos para decidir el nivel en que hay que desarrollar los nuevos contenidos y las relaciones que deben establecerse entre ellos. También puede tener una función motivadora, en la medida en que ayuda a conocer las posibilidades que ofrecen los nuevos aprendizajes.

Evaluación normativa: Usa estrategias basadas en normas estadísticas o en pautas de normalidad, y pretende determinar el lugar que se ocupa en relación con el rendimiento de las personas de un grupo que han sido sometidos a pruebas de este tipo. Las pruebas de carácter normativo pueden ser útiles para clasificar y seleccionar a personas según sus aptitudes, pero no para apreciar el progreso de una persona según sus propias capacidades.

Evaluación cualitativa: Describe e interpreta los procesos que tienen lugar en el entorno considerando todos los elementos que intervienen en él, subrayando la importancia de las situaciones que se generan. Es decir, fija más la atención en la calidad de las situaciones creadas que en la cantidad de los resultados obtenidos.

Evaluación sumativa: Su objeto es conocer y valorar los resultados conseguidos al finalizar el proceso. Así considerada recibe también el nombre de evaluación final. (Ramos & Armas, 2009)

Evaluación de Seguridad de la Operación y Servicios: Es el conjunto de evaluaciones teóricas y prácticas (campo y laboratorio) en materia de Seguridad Operacional y de los Servicios, con el fin de identificar y detectar riesgos (actuales o potenciales) en Plataformas y Servicios. Su objetivo es lograr aplicar medidas de mitigación para estas situaciones o eventos identificados. La responsabilidad de la mitigación esta a cargo de las unidades responsables de las plataformas o servicios. Estas evaluaciones se realizan en las diferentes fases de un proyecto u operación, es decir, en la fase de conceptualización y planificación, ingeniería e implementación, pase a producción, y posterior operación, monitoreo y control. Estas evaluaciones son reflejadas en el documento denominado Matriz de Riesgos.
(Compañía Anónima Nacional Teléfonos de Venezuela. CANTV, 2010)

II.1.3 Modelo, Ingeniería Conceptual y Arquitectura Conceptual.

II.1.3.1 Conceptos de modelo

Puede considerarse que los campos de la ingeniería desarrollan sus aplicaciones basados en modelos, al igual que muchas acciones de la vida diaria. Los modelos se usan para explicar y controlar fenómenos a nuestro alrededor y pueden predecir eventos que están por ocurrir.

También se puede definir un modelo como un ente que representa de forma precisa algo que será realizado o que ya existe. Para los efectos de simulación de sistemas, se considera un modelo a una descripción matemática de un sistema físico que puede obtenerse a partir de la evaluación de su conducta basada en mediciones estimadas, observadas o realizadas directamente sobre el sistema que se pretende modelar.

Se ha propuesto, igualmente, que un modelo es una estructura conceptual que sugiere un marco de ideas que de otra manera no podrían ser sistematizadas. El modelo concebido en esta forma, impulsa la inteligibilidad y ayuda a la comprensión de los fenómenos, ya que proporciona los canales de interconexión entre hechos que sin la existencia de los lazos inferenciales, podrían permanecer aislados e independientes unos de otros.

Otra versión del concepto de modelo es aquella que lo define como una serie de realizaciones que sirven durante una época de ciencia normal para definir problemas y métodos legítimos en un campo específico de investigación. Es en estas realizaciones en las que se forman generaciones sucesivas de futuros practicantes.
(Lopez Austin, 2005)

II.1.3.2 Aplicación del concepto de modelo al desarrollo del tema.

En este caso podemos aplicar el concepto de modelo al tema a desarrollar (IMS- IP Multimedia Subsystem), enfocados en el tema de seguridad, como un modelo de seguridad de la plataforma IMS a implementar. Específicamente este modelo estará dirigido a establecer las normas o parámetros bajo los cuales debería regirse la plataforma IMS a implementar, para que se garantice la continuidad en la prestación de servicios, alto rendimiento, establecer los niveles de seguridad necesarios para evitar fraudes y vulnerabilidades, así como ataques de negación y degradación de servicios.

II.1.3.3 Ingeniería conceptual.

La Ingeniería Conceptual es una de las etapas, fases o partes que conforman un proyecto de ingeniería. La Ingeniería Conceptual es la primera fase o etapa de un proyecto de ingeniería, es la fase en la cual se fijan los objetivos deseados por el cliente, se establecen qué tipo de tecnologías se aplican, se definen el marco de normas técnicas que regularán los diseños, se establecen los criterios de evaluación económica y de cálculo de rentabilidad. Una vez definidos estos, se procede conciliar las bases o criterios de norma de las entidades financieras o crediticias con los establecidos por el cliente, para el desarrollo de alternativas de los diseños (llamados Casos) y las evaluaciones de rentabilidad del proyecto o tasa de retorno, para cada caso. Con el fin de elegir la alternativa con la cual se procede a desarrollar la siguiente fase o se define la cancelación del proyecto por baja rentabilidad. (Compañía Anónima Nacional Teléfonos de Venezuela. CANTV, 2010)

II.1.3.4 Arquitectura Conceptual.

Se entiende como arquitectura conceptual al proceso de definición de la estructura y comportamiento de los componentes de un sistema, utilizando en primer lugar las ideas base o patrones de diseño que mejor se adapten a las necesidades, posteriormente, concretando las tecnologías que las soportan, y finalmente definiendo los parámetros para el uso de dichas tecnologías.

II.2 Conmutación de Circuitos

Las distintas redes de telecomunicación se pueden clasificar de acuerdo a la técnica de conmutación empleada, cada una adecuada para prestar determinados servicios, siendo la conmutación de circuitos la más adecuada para cursar el tráfico de voz ya que no introduce retardo, esto debido a que la transmisión de voz es muy sensible,

llegando incluso a ser ininteligible una conversación si los niveles de retardo son muy elevados. La conmutación de circuitos es la técnica que permite que dos terminales, emisor y receptor, se comuniquen a través de un circuito único y especifico establecido para tal propósito antes del inicio de la comunicación y es liberado una vez que haya finalizado, quedando así disponible para que otros usuarios la utilicen de igual forma**.** (Gil, Pomares, & Candelas, Redes y Transmisión de datos, 2010)

II.3 Redes Telefónicas Públicas Conmutadas (PSTN)

II.3.1 Definición

Las Redes Telefónicas Públicas Conmutadas o PSTN (*Public Switched Telephone Networks*), son las redes telefónicas básicas empleadas en todos los países para la comunicación vocal. Son redes de conmutación de circuitos tradicional optimizada para las comunicaciones de voz en tiempo real. Cuando se realiza una llamada, se cierra un conmutador al marcar y establece así un circuito con el receptor de la llamada. PSTN garantiza la calidad del servicio (QoS) al dedicar el circuito a la llamada hasta que se cuelga el teléfono. Independientemente de si los participantes en la llamada están hablando o en silencio, seguirán utilizando el mismo circuito hasta que la persona que llama cuelgue. (Huidobro & Conesa, 2007)

II.3.2 Elementos que componen la red PSTN

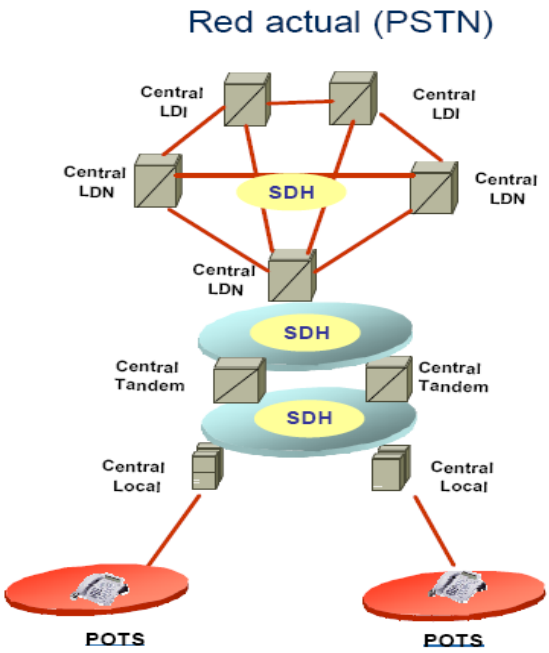


Figura 2: Red actual PSTN

Fuente: (Compañía Anónima Nacional Teléfonos de Venezuela. CANTV, 2006)

Según (Huidobro & Conesa, 2007), en la actualidad tenemos lo que llamamos PSTN (*Public Switching Telephone Network*), la cual es el conjunto global de las interconexiones originalmente diseñado para soportar conmutación de circuitos de comunicación de voz. Como se observa en la figura 2, la red PSTN ofrece la tradicional POTS (*Plain Old Telephone Service*) para residencias y muchos otros establecimientos. En las residencias, la línea telefónica PSTN suele ser un cable de cobre. En la red PSTN se encuentra la central local, que conecta llamadas locales; existen tres conmutadores, los primarios, que están inmediatamente en la zona de servicio, los tándem que conectan varios conmutadores primarios y los tándem superiores que conectan a varios tándem. Partes de la PSTN se utilizan también para DSL (*Digital Subscriber Line*), VoIP (*Voice on IP Protocol*) y otras tecnologías basadas en Internet de la red. El vínculo básico de la red PSTN soporta 64 Kbps de ancho de banda.

II.4 Conmutación de Paquetes

Conmutación de Paquetes es el establecimiento, por parte de una red de telecomunicaciones, de un intercambio de bloques de información o paquetes, con un tamaño específico entre dos puntos, un emisor y un receptor. En el extremo emisor, la información se divide en paquetes a los cuales se les indica la dirección del destino. Cada paquete contiene, además de datos, un encabezado con información de control (prioridad y direcciones de origen y destino).

Estos paquetes se transmiten a través de la red y, posteriormente, son reensamblados en el destino obteniendo así el mensaje original. En cada nodo de la red, un paquete puede ser almacenado brevemente y enrutado dependiendo de la información de la cabecera. De esta manera, pueden existir múltiples vías o rutas de un punto a otro.

La conmutación de paquetes resulta más adecuada para la transmisión de datos comparada con la Conmutación de circuitos. Su principal ventaja es que únicamente consume recursos del sistema cuando se envía o se recibe un paquete, quedando el sistema libre para manejar otros paquetes con otra información o de otros usuarios. Por esto, la conmutación de paquetes permite la compartición de recursos entre usuarios y entre informaciones de tipo y origen distinto.

Algunas de sus principales ventajas son que mejora la calidad del servicio, la velocidad de transmisión, optimización de los recursos, etc, y todo por un mismo precio. Pero por otro lado las principales desventajas son la perdida de paquetes y la obtención de retrasos considerables, por lo que para la transmisión de voz y servicios en tiempo real generan cierta complejidad en las redes de conmutación de paquetes. (García, Estrategia de Migración de las Redes de voz alambricas, inalambricas y móviles a la arquitectura de Redes de Nueva Generación, 2003)

II.5 Redes de Próxima Generación (NGN)

II.5.1 Introducción a la red NGN

Las Redes de Próxima Generación (NGN) son redes capaces de manejar voz, datos y video y proporcionar múltiples aplicaciones y servicios. Estas redes unifican las redes telefónicas públicas conmutadas (PSTN), las redes de televisión y las redes de datos, creando una única red multiservicio de plataforma basada en la paquetización de la información usando el Protocolo de Internet (IP). (Centro de Investigación para la Sociedad de la Información, 2009)

Entre las características principales de las Redes de Nueva Generación se encuentran:

- Transferencia de la información basada en paquetes (Protocolo IP).
- Red con el plano de control (señalización, control) separado del plano de transporte.
- Desarrollo de servicios a través de interfaces abiertas entre el transporte, el control y las aplicaciones.
- Soporte de un amplio rango de servicios y aplicaciones (tiempo real, streaming y multimedia).
- Capacidad de banda ancha con calidad de servicio (QoS) extremo a extremo.
- Trabajo integrado de redes precedentes (PSTN y otras) a través de interfaces abiertas.
- Movilidad generalizada. Esto se refiere a la movilidad de distintos usuarios y dispositivos a través de diferentes tecnologías de acceso sin interrupción del servicio.
- Acceso de los usuarios a servicios ofrecidos por diferentes proveedores.
- Variedad en los esquemas de identificación de usuarios y dispositivos.
- Trabajo con un mismo perfil de servicio para un usuario a través de toda la red.

- Convergencia de los servicios fijos y móviles.
- Soporte de múltiples tecnologías de última milla.
- Cumplimiento de todos los requerimientos regulatorios (comunicaciones de emergencia, seguridad, intercepción legal y otros).

II.5.2 Arquitectura de la red NGN

Según (Estrella Bonilla, Diseño de un Prototipo de Red de Nueva Generación NGN (Next Generation Network), basado en una arquitectura MetroEthernet para proveer servicio de VoIP, 2007), la arquitectura general de una NGN está compuesta principalmente de tres (3) capas o niveles para su mayor efectividad, desempeño y administración. En la figura 4, se pueden observar los niveles de la arquitectura de las redes NGN:

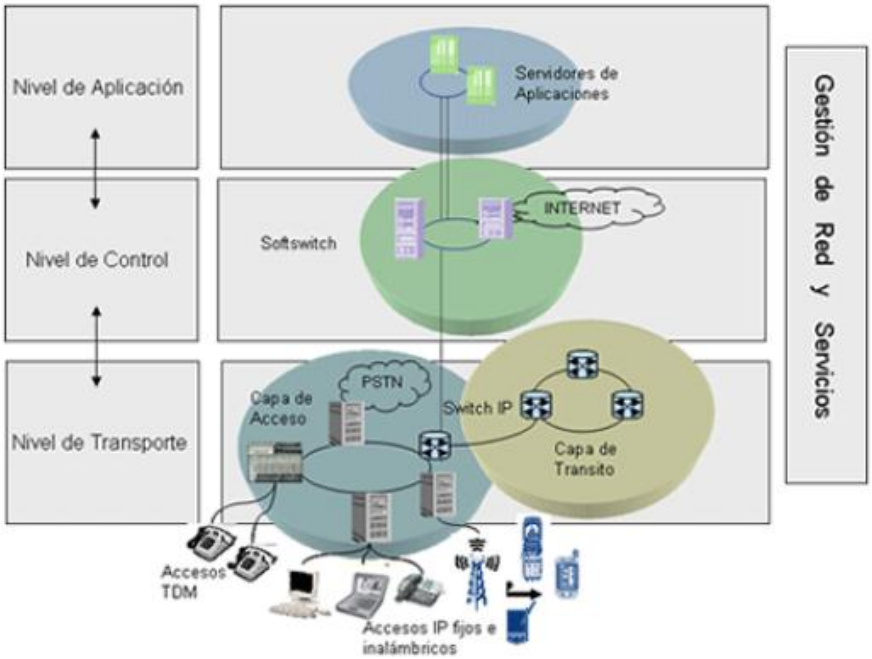


Figura 3: Capas o niveles de una arquitectura general de una NGN.

Fuente: (Tejedor Millán, 2006)

II.5.2.1 Nivel de Aplicación y Servicios

En el nivel de aplicación o servicios se encuentran los servidores en donde residen y se ejecutan las aplicaciones que permiten la prestación de los servicios a los clientes. Esta capa se refiere a la provisión de funciones, interfaces y API estándar para el acceso de las aplicaciones para la NGN.

II.5.2.2 Nivel de Control

El nivel de control coordina todos los elementos en las capas de Aplicación y Transporte, se encarga de asegurar en funcionamiento entre la red de Transporte y los servicios y las aplicaciones, mediante la interpretación, generación, distribución y traducción de la señalización correspondiente, con el uso de protocolos de señalización como H.323, SIP, MGCP, MEGACO/H.248.

II.5.2.3 Nivel de Transporte

En el nivel de transporte se ubican las tecnologías de red, cuya tarea es encargarse de la conmutación, enrutamiento y transmisión de los paquetes IP. Esta capa se suele dividir en dos subniveles adicionales. La capa de acceso que comprende la red de banda ancha que da acceso al usuario a la NGN. Este acceso puede ser fijo, móvil, etc. utilizando múltiples tecnologías (xDSL, 802.11(x), 802.16(x), celular, POT y TDM para permitir la coexistencia con las redes heredadas, etc.) y medios de transmisión, y la capa de tránsito que permite el enrutamiento y conmutación de los paquetes de extremo a extremo. Asegura la interconexión de todas las redes de acceso con los otros niveles. Y además permite el transporte de diferentes tipos de tráfico con variados requerimientos de calidad de servicio. (Estrella Bonilla, Diseño de un Prototipo de Red de Nueva Generación NGN (Next Generation

Network), basado en una arquitectura MetroEthernet para proveer servicio de VoIP, 2007).

II.5.3 Elementos de la red NGN

La infraestructura de las comunicaciones públicas conmutadas en la actualidad consiste en una variedad de diferentes redes, tecnologías y sistemas, la mayoría de las cuales se basan sobre estructuras de conmutación de circuitos. La tecnología evoluciona hacia redes basadas en paquetes y los proveedores de servicio necesitan la habilidad para interconectar sus clientes sin perder la fiabilidad, conveniencia y funcionalidad de las redes telefónicas públicas conmutadas. En la figura 4, se pueden observar los elementos más importantes de una arquitectura NGN.

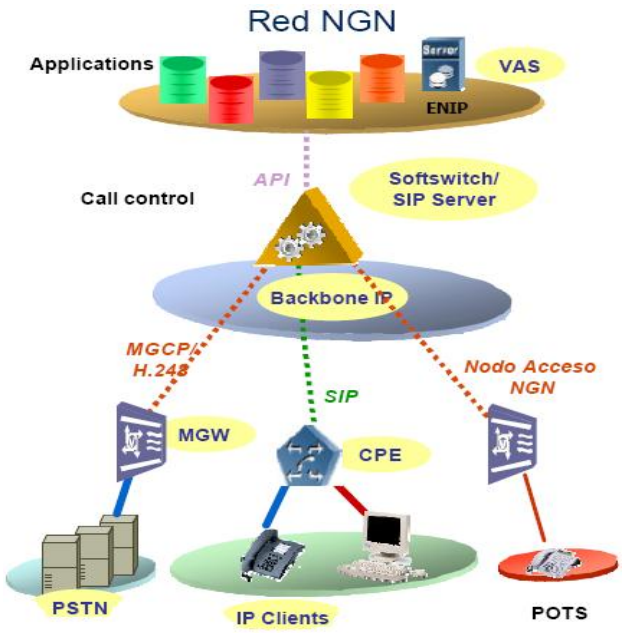


Figura 4: Red NGN (conmutación de paquetes IP).

Fuente: (Centro de Investigación para la Sociedad de la Información, 2009).

II.5.3.1 Softswitch

La tecnología Softswitch resulta de enfocar estas necesidades. La idea es proporcionar una diversidad de servicios de comunicaciones basados en IP (Protocolo de Internet) equivalentes a los servicios de redes tradicionales por su calidad y facilidad de uso. El Softswitch se encuentra en la capa de control de las NGN.

II.5.3.1.1 Definición

El Softswitch es un dispositivo de comunicaciones que comprende hardware y software, que utiliza estándares abiertos para crear redes integradas de última generación capaces de transportar voz, datos y video con gran eficiencia.

II.5.3.1.2 Características del Softswitch

El Softswitch provee además el control de llamadas y servicios inteligentes para las redes de conmutación de paquetes, sirviendo como plataforma de integración para aplicaciones e intercambio de servicios, permitiendo transportar tráfico de voz, video y datos. (Estrella Bonilla, Diseño de un Prototipo de Red de Nueva Generación NGN (Next Generation Network), basado en una arquitectura MetroEthernet para proveer servicio de VoIP, 2007).

Una característica clave del Softswitch, es su capacidad de proveer a través de la red IP un sistema telefónico tradicional, confiable y de alta calidad en todo momento. Si la confiabilidad de una red IP llega a ser inferior al nivel de la calidad de la red tradicional, simplemente el tráfico se desvía a esta última. Las interfaces de programación permitirán que los fabricantes independientes de software creen rápidamente nuevos servicios basados en IP que funcionen a través de ambas redes: la tradicional y la IP.

Los beneficios que nos proporciona el Softswitch, según (Rios & García, Softswitch, 2005) son:

- Bajo costo de desarrollo.
- Fácil integración de redes diversas.
- Mejora los servicios para el cliente lo cual reduce el tiempo para mercadear.
- Mensajes unificados.
- Flexibilidad al soportar el desarrollo de equipos de telefonía de gran nivel.
- Mejores ingresos para los proveedores de servicios y operadores.

II.5.3.2 Elementos de Acceso

La capa de transporte de las redes NGN, según (Real Martín, 2008)soporta diferentes conjuntos funcionales:

Funciones de Acceso (*Access Network Functions, ANF*). Para diversas tecnologías porque los servicios deben ser ajenos a la tecnología subyacente. Permiten conectividad IP entre el extremo usuario y el núcleo NGN.

Funciones del núcleo de transporte. Proporcionan conectividad IP, en el estrato de transporte, a través del núcleo. Se compone de dos conjuntos funcionales de interés, que son:

- Funciones de control de adhesión a la red (*Network Attachment Control Functions, NACF*). Agrupa las funciones de iniciación y registro del usuario para acceder a los servicios de la NGN: identificación, autenticación, gestión de la dirección IP, acceso a las sesiones, etc.
- Funciones de control de admisión de recursos (*Resource and Admission Control Functions, RACF*). Proporciona las capacidades para el control que ofrece la red NGN interactuando en el nivel de transporte. Controla y gestiona la QoS con las soluciones de filtrado de paquetes, políticas de clasificación del tráfico, reservas de ancho de

banda y localización, traslación direcciones de red (*Network Address and Port Translation, NAPT*), etc.

RACF y NACF interactúan durante el acceso del usuario a la red comprobando el nivel de servicio acordado con el proveedor de los servicios de la NGN. (Real Martín, 2008)

II.5.4 Protocolos de Señalización en redes NGN

II.5.4.1 Protocolo SIP

SIP (*Session Initiation Protocol*) es un protocolo definido por la IETF que permite el establecimiento, modificación y la liberación de sesiones multimedia (voz, texto, datos, video, etc). Existen otros protocolos de sesiones multimedia relacionados con el protocolo SIP:

- SDP (*Session Description Protocol*): es un protocolo incluido en el cuerpo del mensaje SIP. Descripción de la sesión (SDP) separada de la gestión de la sesión (SIP).
- RTP (*Real-Time Transport Protocol*): establecida la sesión, el protocolo RTP permite la transmisión de la media (voz, video, etc).
- RTCP (*Real-Time Transport Control Protocol*): su propósito es la de reportar y ajustar la transmisión de la media.

Características del protocolo SIP:

- SIP es un protocolo basado en el modelo cliente-servidor, donde un cliente SIP envía peticiones (*Request Messages*) a un servidor SIP, el cual responde al cliente con uno o más mensajes de respuesta (*Response Messages*), dependiendo de la cantidad de solicitudes enviadas por el cliente.
- SIP es uno de los protocolos de Internet basados en texto como HTTP.

- El protocolo SDP (*Session Description Protocol*) siempre está incluido en el contenido del mensaje SIP.
- Es un protocolo que puede estar basado en UDP / TCP / SCTP, aunque el más común es UDP.
- Es usado en NGN como protocolo de señalización para el control de sesiones y el control de servicio.

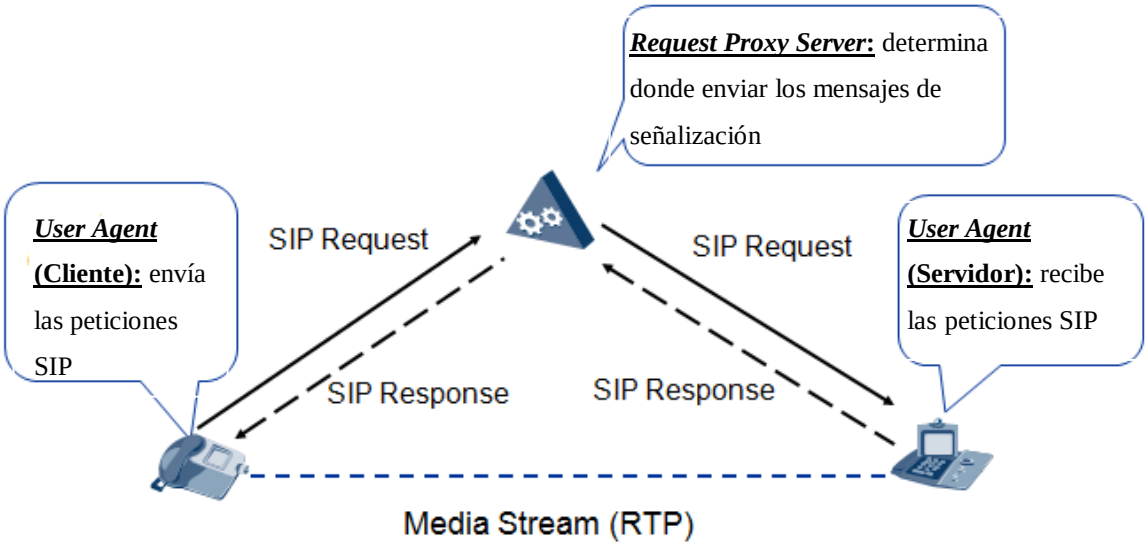


Figura 5: Arquitectura simplificada de una red SIP.

Fuente: (Huawei Technologies. Co., 2010)

Las entidades lógicas de SIP son:

- UA (*User Agents*): son los elementos que establecen las sesiones, pueden ser personas o aplicaciones de software, por ejemplo un videoteléfono, un cliente de software, son considerados agentes de usuario. Los agentes de usuario pueden comportarse como clientes (*UAC- User Agent Client*) si realizan una petición o como servidores (*UAS- User Agent Server*) si reciben una petición específica. Ambos agentes son capaces de terminar una llamada. Los agentes de usuario actúan como UAC y como UAS dependiendo de la situación.

- Servidores de Registro (*Register Server*): cada usuario tiene una dirección lógica invariante (dirección IP), de la forma usuario@dominio es decir tiene la misma forma que una dirección de correo electrónico, denominada URI (*Uniform Resources Identifier*). Mantienen la localización actual de los usuarios SIP. Se utiliza para que los terminales registren la localización en la que se encuentran. Los clientes SIP necesitan actualizar su localización con peticiones de registro.
- Servidor Proxy (*Proxy Server*): se encarga de encaminar los mensajes (peticiones/respuestas) desde el origen hacia el destino final y enviar las solicitudes. El encaminamiento se realiza salto a salto de un servidor a otro hasta alcanzar el destino final.
- Servidor de Redirección (*Redirect Server*): se encarga de aceptar la solicitud SIP y la traslada a una nueva dirección, para que el Servidor Proxy observe la nueva dirección y sea capaz de encaminar correctamente el paquete hasta su destino. (Huawei Technologies. Co., 2010)

SIP-URI

Un SIP-URI (SIP - *Uniform Resource Identifier*), como su nombre lo indica es un identificador uniforme de usuarios SIP. Tiene el mismo formato que una dirección de correo electrónico. El SIP URI proporciona una forma sencilla y extensible para identificar a los usuarios en redes que manejen protocolos SIP. El formato de un SIP URI es **sip: nombreusuario@dominio:puerto**, donde el dominio representa la dirección IP del usuario.

Existen dos tipos de direcciones SIP URI:

- AOR (*Address of Record*): es la dirección que identifica al usuario, su formato es como un correo electrónico. Esta abierta al público.
  SIP: admin@dominio.com.

- FQDN (*Full Qualified Domain Name*): es la dirección que identifica a la maquina o dispositivo, es decir, la dirección IP de origen.
  SIP: admin@172.128.0.3.

En las tablas 1, 2 y 3, se pueden observar los principales mensajes usados por el protocolo SIP, tanto mensajes de solicitud como respuesta.

Solicitudes Básicas	
INVITE	Para iniciar una sesión.
REGISTER	Para registrarse (usuario) con un servidor SIP.
ACK	Para responder a un mensaje INVITE e iniciar la sesión.
CANCEL	Para cancelar una sesión.
BYE	Para terminar una sesión.
OPTIONS	Para consultar a los servidor sobre sus capacidades.

Tabla 1: Solicitudes básicas Protocolo SIP.

Fuente: (Huawei Technologies. Co., 2010)

Solicitudes Extendidas	
MESSAGE	Aplicado para la mensajería instantánea (IM).
SUBSCRIBE	Para subscribirse a un evento de notificación.
NOTIFY	Para enviar un evento de notificación.
UPDATE	Para modificar los atributos de la sesión cuando se está estableciendo una llamada.
PUBLISH	Distribución de su estado de eventos para el estado del servidor.
PRACK	Para indicar la fiabilidad de una respuesta temporal.

Tabla 2: Solicitudes extendidas Protocolo SIP.

Fuente: (Huawei Technologies. Co., 2010)

Tipos de mensajes respuesta SIP		
1xx	Provisional	Petición recibida, continuando con el proceso de la solicitud.
2xx	Éxito	La acción fue recibida con éxito, entendida y aceptada.
3xx	Redirección	Es necesario tomar otras acciones para completar la solicitud.
4xx	Error cliente	Solicitud con sintaxis incorrecta o no se puede cumplir (servidor).
5xx	Error servidor	El servidor no pudo cumplir con una petición valida.
6xx	Fracaso global	La solicitud no puede cumplirse en cualquier servidor.

Tabla 3: Tipos de mensajes de respuesta Protocolo SIP.

Fuente: (Huawei Technologies. Co., 2010)

Flujo básico SIP

- Establecimiento de la sesión

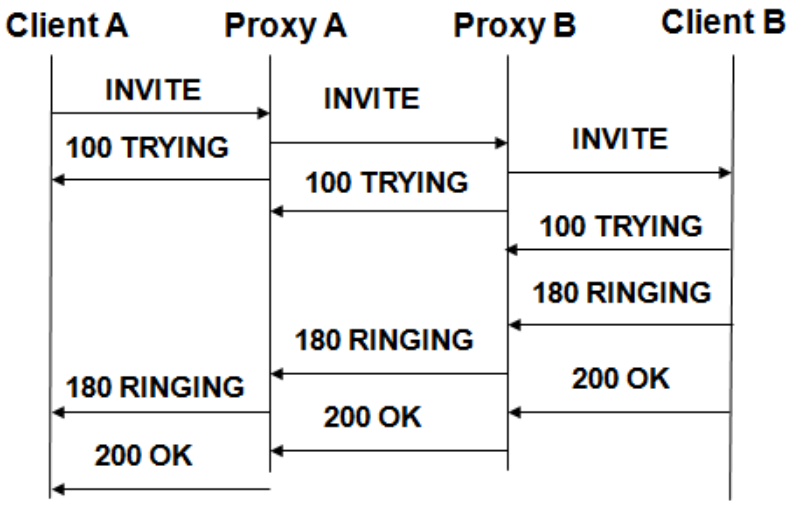


Figura 6: Establecimiento de la sesión SIP.

Fuente: (Huawei Technologies. Co., 2010)

- Registro del usuario

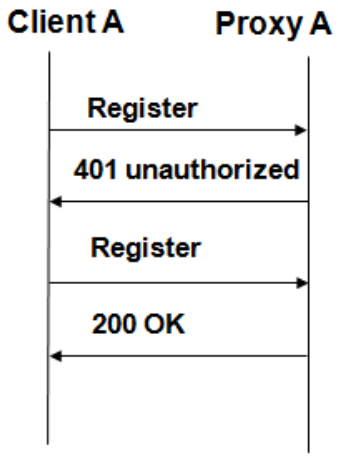


Figura 7: Registro de usuario SIP.
Fuente: (Huawei Technologies. Co., 2010)

II.5.4.2 Protocolo MEGACO o H.248

El protocolo H.248, también conocido como MEGACO, es el resultado de la cooperación entre la UIT (Unión Internacional de Telecomunicaciones) y la IETF (*Internet Engineering Task Force*) y se podría contemplar como un protocolo complementario a los dos anteriores. (Huawei Technologies Co., 2010). Los componentes que intervienen en este protocolo son:

- Pasarela de medios o MG (*Media Gateways*): Son los elementos funcionales que median entre los puntos finales, es decir, los clientes.
- Controlador de la pasarela de medios o MGC (*Media Gateway Controller*):
- Controlaran a los MG para una buena gestión en el intercambio de información a través del protocolo MGCP. El MGC también se suele llamar Agente de Llamada (*Call Agent*). Una de las características

fundamentales de este modelo, es que los MG son capaces (en teoría) de mantener comunicaciones tanto con el H.323 como con el SIP, algo fundamental para la óptima implantación del sistema VoIP.

Según (Huawei Technologies Co., 2010)**,** si un usuario desea realizar una llamada, mediante este sistema, los pasos que se realizan son los siguientes:

1.-) El usuario descuelga el teléfono y marca el número de teléfono del destinatario. Esta llamada, le llega al MG.
2.-) El MG, notifica al MGC de que una llamada está en camino.
3.-) El MGC busca en su base de datos, el número de teléfono del destinatario para saber su IP y su número de puerto. Entonces, busca el MG del destinatario, y le envía un mensaje para indicarle que le esta llegando una llamada.
4.-) El MG del destinatario, abre una comunicación RTP (*Real-Time Transport Protocol*) cuando el usuario descuelga. El protocolo RTP proporciona los servicios de entrega end-to-end para los datos de características en tiempo real, tales como audio y vídeo interactivos. (Huawei Technologies Co., 2010)

II.5.4.3 Protocolo MGCP

El protocolo MGCP (*Media Gateway Control Protocol*) permite controlar las pasarelas de medios (Gateways) de comunicaciones de los elementos de control de llamada externas que se llaman Agente de Llamada (Call Agent). La pasarela de medio es, típicamente, un elemento de la red que proporciona la conversión entre señal de audio de un teléfono conmutado por circuito y la señal de paquete que se puede transportar a través de Internet o sobre la red de conmutación de paquete como ATM o Frame Relay. El protocolo MGCP presenta una arquitectura de control de llamada donde la "inteligencia" está fuera de las pasarelas y es manejado por elementos de control de llamada externos, conocidos como Agentes de Llamada.

Los mensajes MGCP viajan sobre UDP, por la misma red de transporte IP. El formato de trabajo genera una inteligencia externa a la red (concentrada en el MGC) y donde la red de conmutación está formada por los router de la red IP. El GW solo realiza funciones de conversión vocal (analógica o de velocidad digital) y genera un camino RTP entre extremos. La sesión de MGCP puede ser punto-a-punto o multipunto, utilizando protocolo RTP (*Real-Time Transport Protocol*). (Huawei Technologies. Co., 2010)

II.6 Subsistema Multimedia IP (IMS)

II.6.1 Introducción a la red IMS

La proliferación de la tecnología IP, la necesidad de convergencia total y el despliegue de IMS en todas las redes de telecomunicación están transformando radicalmente el sector y posibilitará que las operadoras integren las llamadas fijas con las móviles, y la voz con el acceso a Internet de banda ancha, la televisión y el vídeo bajo demanda, y las aplicaciones multimedia residenciales y empresariales.

El sistema estándar IMS (*IP Multimedia Subsystem*) define una arquitectura genérica que fue diseñada para facilitar la unión de dos mundos: redes fijas y móviles, cuyo objetivo es proveer servicios multimedia con aplicaciones comunes a muchas tecnologías tanto de redes móviles (GSM, WCDMA, CDMA2000, WIMAX, etc.) como a redes fijas (PSTN, NGN, etc.)

IMS (*IP Multimedia Subsystem*) es una arquitectura de referencia genérica para ofrecer servicios multimedia sobre infraestructura IP. Su idea fundamental es la de integrar la telefonía fija y móvil, proporcionando en un futuro los mismos servicios. Se trata de un estándar internacional aún en evolución, especificado originariamente en el Release 5 y 6 del 3GPP (*Third Generation Partnership Project)*, en estrecha

colaboración con el IETF (*Internet Engineering Task Force*), y que ha sido adoptado también por otros organismos de estandarización como 3GPP2 y ETSI.

El estándar soporta múltiples tipos de tecnologías de acceso tanto fijas como móviles, incluyendo: PSTN, NGN, GSM, GPRS, UMTS, HSDPA, DSL, HFC, Wi-Fi, Wi-Max, Bluetooth, etc. Es decir, el concepto actual de las comunicaciones telefónicas y por Internet dará un giro radical a medio plazo, gracias a esta nueva tecnología que permitirá pasar de un sistema a otro sin interrumpir la conexión, utilizar varios medios a la vez o compartirlos e intercambiarlos con varios usuarios. (Huawei Technologies Co., 2010)

II.6.2 Características generales de la tecnología IMS

Las principales características, según (Huawei Technologies Co., 2010) tecnológicas de IMS son:

- El control de la sesión es realizado por el protocolo de control de llamada IMS basado en SIP y SDP. La señalización de IMS se realiza mediante el protocolo SIP (*Session Initiation Protocol*), diseñado originariamente por el IETF para la gestión de sesiones multimedia en Internet. SIP aporta las funciones para el registro, establecimiento, modificación y finalización de las sesiones IMS entre dispositivos diversos. Puesto que no todos los dispositivos son capaces de soportar los mismos servicios, al establecer la sesión se negocian las características de ésta mediante el protocolo SDP (*Session Description Protocol*), también diseñado por el IETF. Mediante SDP, los extremos de una sesión pueden indicar sus capacidades multimedia y definir el tipo de sesión que desean mantener. En este intercambio de señalización se negocia también la QoS, tanto durante el establecimiento como durante la sesión en curso. Por ello, y puesto que con IMS es posible monitorizar en todo momento la calidad del servicio en términos de latencia, ancho de banda y

seguridad, la calidad de servicio (QoS) en IMS es mucho más dinámica que en las tradicionales redes de telecomunicación.

- El transporte de red es realizado mediante IPv6 en vez de IPv4. La razón es que la migración a IPv6 está siendo paulatinamente desplegado en Internet y actualmente existen muchas empresas e instituciones que lo emplean internamente. Entre las ventajas de IPv6 cabe destacar la QoS y seguridad integradas, la autoconfiguración, un mayor espacio de direccionamiento y que el tráfico en el plano de usuario se transfiere directamente entre terminales siguiendo el modelo P2P.
- La provisión de servicios multimedia es realizada por protocolos del IETF. Además de SIP/SDP e IPv6, IMS emplea otros protocolos estándar de Internet para la provisión de servicios multimedia, como: RTP (*Real Time Protocol*) y RTCP (*Real Time Control Protocol*) para el transporte de flujos IP multimedia en el plano de usuario, RSVP (*Resource Reservation Protocol*) y DiffServ para asegurar la QoS extremo a extremo, etc. (Huawei Technologies Co., 2010)

II.6.3 Evolución de la arquitectura IMS

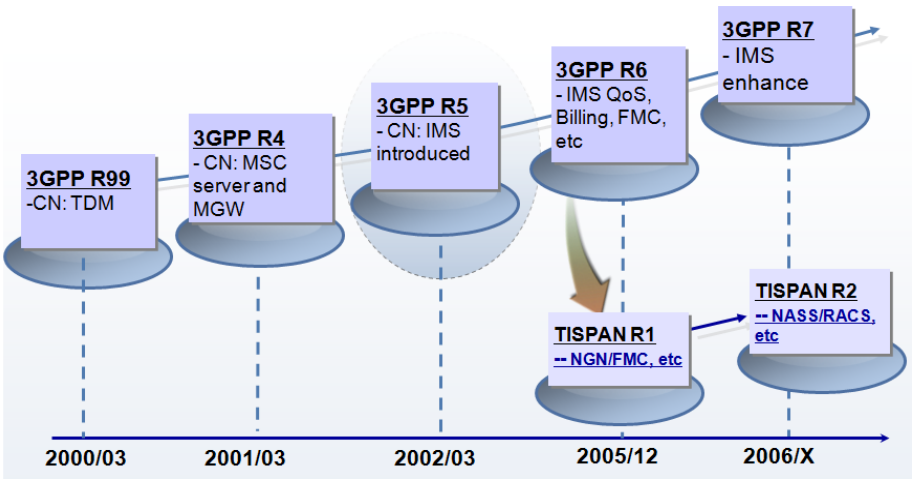


Figura 8: Evolución de la arquitectura IMS

Fuente: (Huawei Technologies Co., 2010)

El Instituto de Estandarización Europeo de Telecomunicaciones (pos sus siglas en ingles ETSI), fue la organización de estandarización que definió GSM (*Global System for Mobile Communications*), durante las décadas de los años 80 y 90, al igual que definió la arquitectura de la red GPRS (*General Packet Radio Service*). El último estándar de GSM se produjo en 1998, y en ese mismo año la 3GPP (*Third Generation Partnership Project*) fue fundada por grupos de estandarización de Europa, Japón, Corea del Sur, USA y China para especificar un sistema 3G (*Third Generation*) de telefonía móvil que integre la tecnología de acceso WCDMA (*Wideband Code Division Multiple Access*) y la TD-CDMA (*Time Division Code Division Multiple Access*) en un 'core' GSM. La 3GPP preparó las especificaciones para una primera versión (*release*), comenzando con la versión 99. -

II.6.3.1 *Release* 99

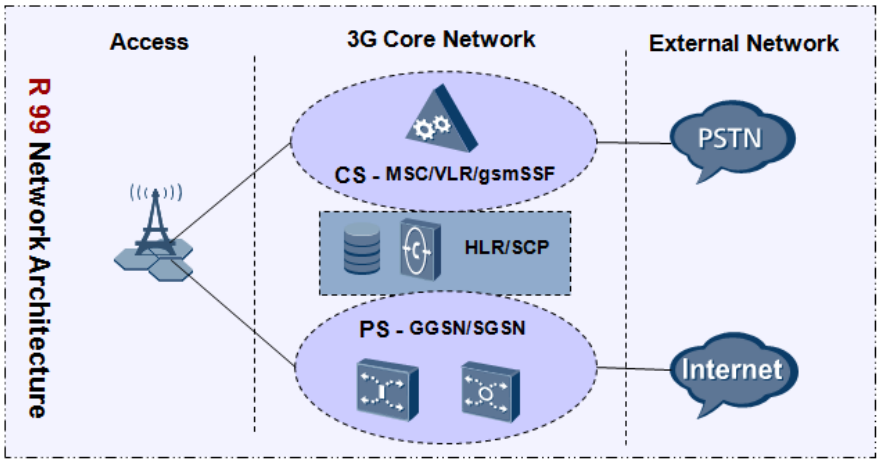


Figura 9: *Release* 99

Fuente: (Huawei Technologies Co., 2010)

La primera versión se obtuvo en 1999, debido a la ayuda en conjunto de dos organizaciones la 3GPP y la ETSI SMG (*Special Mobile Group*). La primera realizó el diseño de los servicios, la arquitectura del sistema, los accesos de radio por WCDMA y TD-CDMA, en un 'core' de red común. La ETSI SMG desarrolló el

acceso de radio EDGE (*Enhanced Data Rates for Global Evolution*). El acceso de radio WCDMA fue el aporte más significativo en la versión 99. También de introdujo el concepto de UTRAN (*UMTS Terrestrial Radio Access Network*). En la versión 99, la red 'core' 3G se separa en el dominio CS (*Circuit Switched*) y el dominio PS (*Packet Switched*), para la red PSTN e Internet respectivamente. (Huawei Technologies Co., 2010)

II.6.3.2 *Release* 4

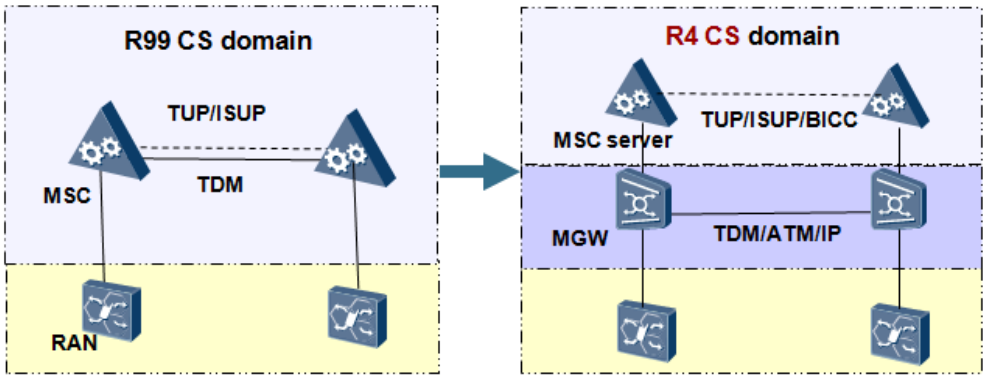


Figura 10: *Release* 4

Fuente: (Huawei Technologies Co., 2010)

En esta versión se incluye por primera vez las llamadas *All-IP*, lo que después se conoció como IMS. Como era una tecnología todavía inmadura, la 3GPP decidió completar la versión 4 sin IMS. En el *release* 4 la 3GPP incluye: MSC (*Mobile Switching Centre*), el concepto de MGW (*Media Gateway*), el transporte dentro de la red del 'core' mediante protocolos IP, LCS (*Location Services*) para el manejo de mensajes multimedia. Lo más relevante de la versión 4, fue que se separó el MSC en MSC *Server* y MGW; el control de llamadas se separa con la función de portador de los medios de comunicación. (Cabrejos & Cuesta, 2009)

II.6.3.3 *Release* 5

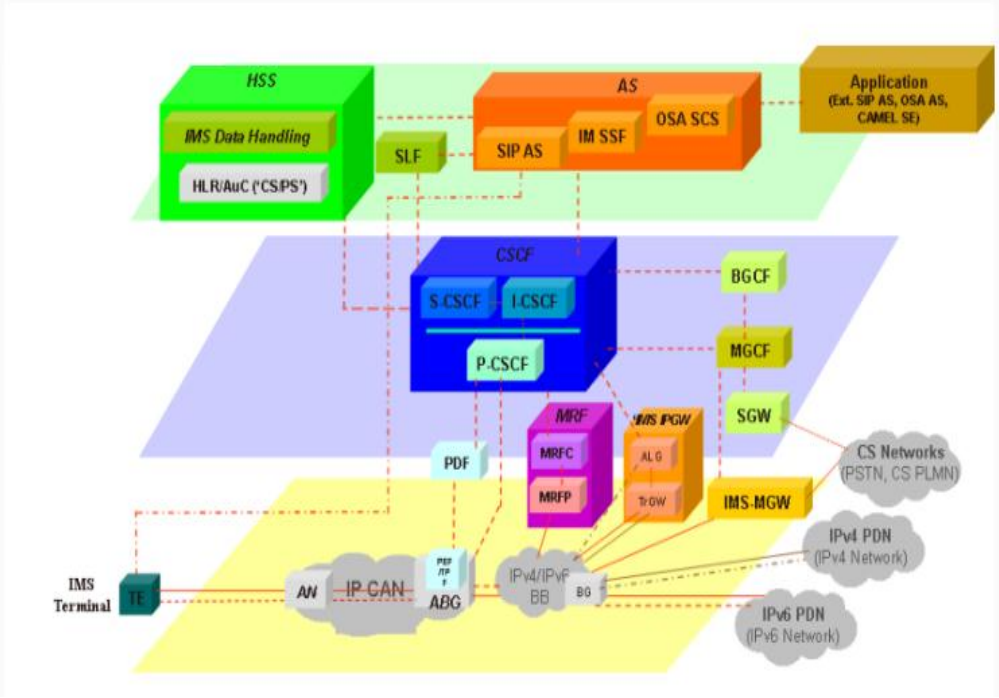


Figura 11: Evolución de la arquitectura IMS.

Fuente: (Normetn, 2007)

En la versión 5, la 3GPP finalmente introduce el concepto de IMS en sus especificaciones. Supone que es un estándar de acceso independiente de la arquitectura IP que interactúen con las redes de voz y datos, tanto fijo (por ejemplo, PSTN, ISDN, Internet) y móvil los usuarios (por ejemplo, GSM, CDMA). La arquitectura IMS hace posible establecer peer-to-peer de comunicaciones IP con todo tipo de clientes. Además de brindar la calidad requerida en los servicios y en la gestión de sesiones. La arquitectura IMS también se ocupa de funciones que son necesarias para la prestación de servicios completos (por ejemplo, registro, seguridad, carga, control de portador, *roaming*). Fue suspendida en marzo de 2002. (Huawei Technologies Co., 2010)

II.6.3.4 *Release* 6

En la versión 6 de la 3GPP, se continuó con el trabajo de la versión 5, se realizaron correcciones de las deficiencias presentes en cuanto a la IMS en la versión 5. La versión 6 fue completada en septiembre de 2005. En el *Release* 6 se incorpora el acceso para redes inalámbricas tales como WLAN y WIMAX. Es necesaria también la implementación de un Gateway para este tipo de acceso, el cual es llamado WAG (*Wireless Lan Gateway*), su función es hacer que los datos de la red de acceso sean entendidos por la red núcleo o 'core'. (Cabrejos & Cuesta, 2009)

II.6.3.5 TISPAN NGN *Release* 1

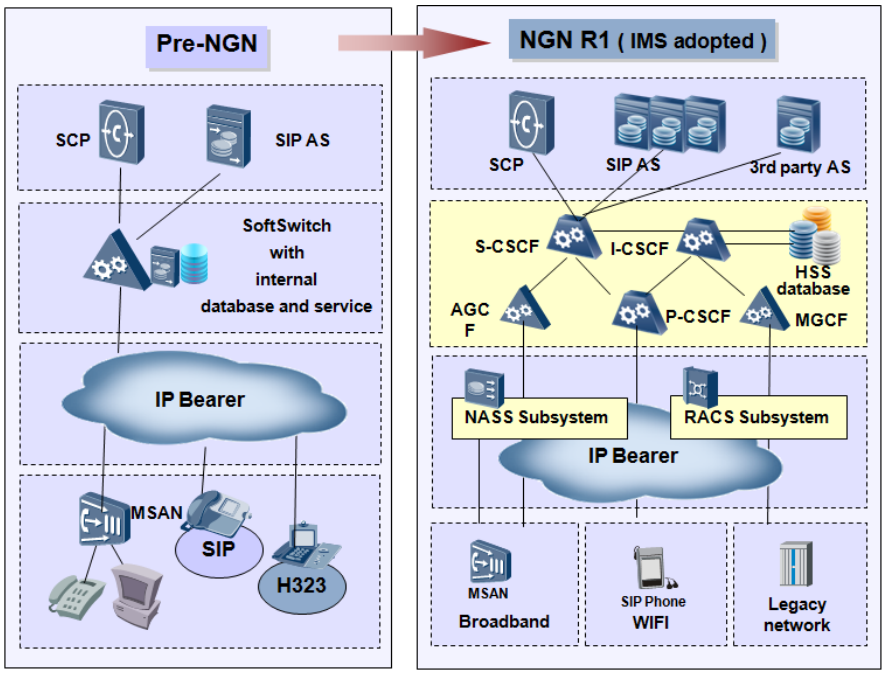


Figura 12: TISPAN NGN R1

Fuente: (Huawei Technologies Co., 2010)

En el dominio de la red fija, TISPAN adopta la arquitectura 3GPP R5 y re-define la Pre-NGN para NGN R1 con elementos de IMS. TISPAN diseñó dos nuevos

subsistemas (NASS y RACS), especialmente para acceder a la red fija y control de calidad de servicio (QoS) respectivamente. (Huawei Technologies Co., 2010)

II.6.3.6 *Release* 7

El *release* 7 nace de la colaboración entre la 3GPP, 3GPP2 y el *release* 1 de TISPAN. En este *release*, se implementa todo el acceso de las redes fijas, principalmente las redes DSL y Ethernet, para brindar mejores servicios de ancho de banda, servicios de voz continuos y servicios multimedia. Es necesario implementar un Servidor de Acceso de Banda Ancha (BAS) para comunicar los datos entre la red de acceso y la red 'core'. (Camarillo & García Martín, 2006)

II.6.4 Arquitectura de una red IMS

La arquitectura de una red IMS es un modelo en capas horizontales, donde convergen la telefonía móvil (GSM, WCDMA, EDGE, etc) y la telefonía fija (PSTN, ISDN, ATM, etc). A diferencia de los modelos tradicionales como el modelo OSI (*Open System Interconnection*) o el TCP/IP, el modelo en capas IMS consta de 3 capas como podemos observar en la figura. Las bases de datos y los servicios se encuentran en la misma plataforma, los usuarios pueden acceder de forma independiente al tipo de telefonía o tecnología que estén utilizando. A diferencia con las tecnologías antiguas, que era un modelo en capas verticales, donde el usuario y los servicios no se encuentran en la misma plataforma multiplicándose los costos para los proveedores, el nuevo modelo de capas horizontales de la arquitectura IMS reduce los costos de operación e integra todo en una misma plataforma. (Huawei Technologies Co., 2010)

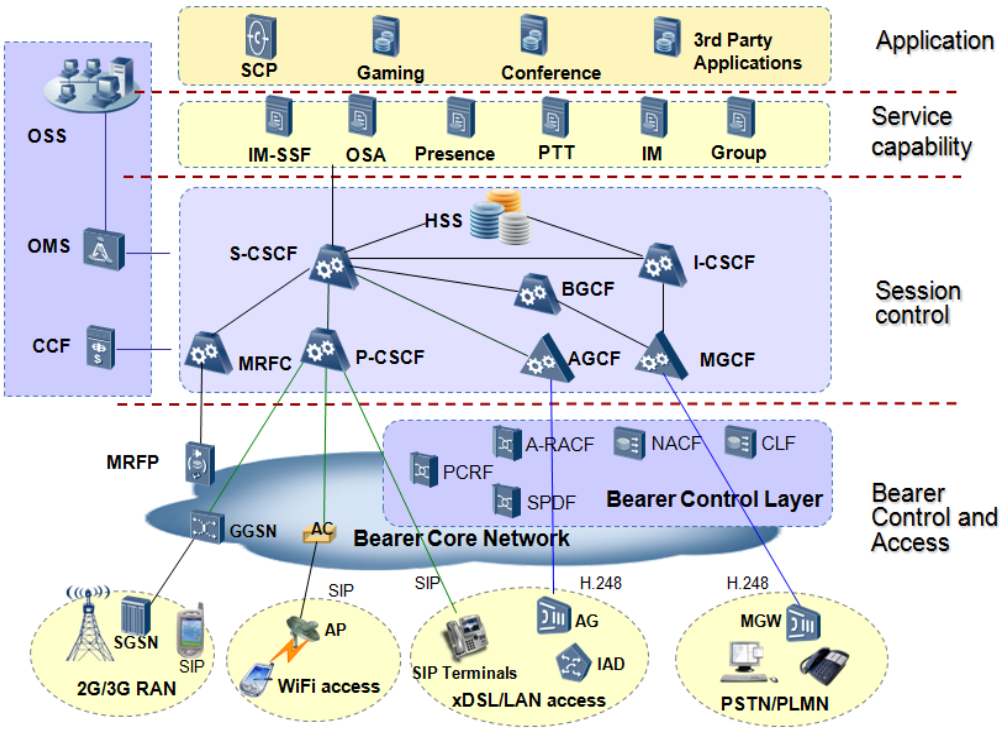


Figura 13: Arquitectura de una red IMS.

Fuente: (Huawei Technologies Co., 2010)

Como se puede observar en la figura 13, la primera capa que forma parte de la arquitectura de una red IMS es la capa de Acceso al Portador, donde se encuentran los usuarios y elementos de acceso a la red IMS. La segunda capa, o capa de Sesión de Control, es la capa más importante de la arquitectura IMS ya que es donde se encuentra el núcleo de la red, formada por controladores para el establecimiento y liberación de las sesiones, los cuales son los responsables de encaminar la señalización para el establecimiento de una llamada entre usuarios. Tiene como funciones principales el control de llamadas, gestión de usuarios, activación de servicios, control de recursos, entre otras funciones. Esta capa está formada por el elemento controlador fundamental de la red IMS, conocido como CSCF (*Call State Control Function*), además del AGCF/MGCF (*Media Gateway Control Function*) y el MRCF (*Media Resource Control Function*). Acceso al Portador (*Access and*

bearer), representa el acceso de los usuarios a través de tecnologías de alta velocidad de telefonía fija o móvil (UMTS, CDMA2000, xDSL, WiFi, redes de cable, etc.).

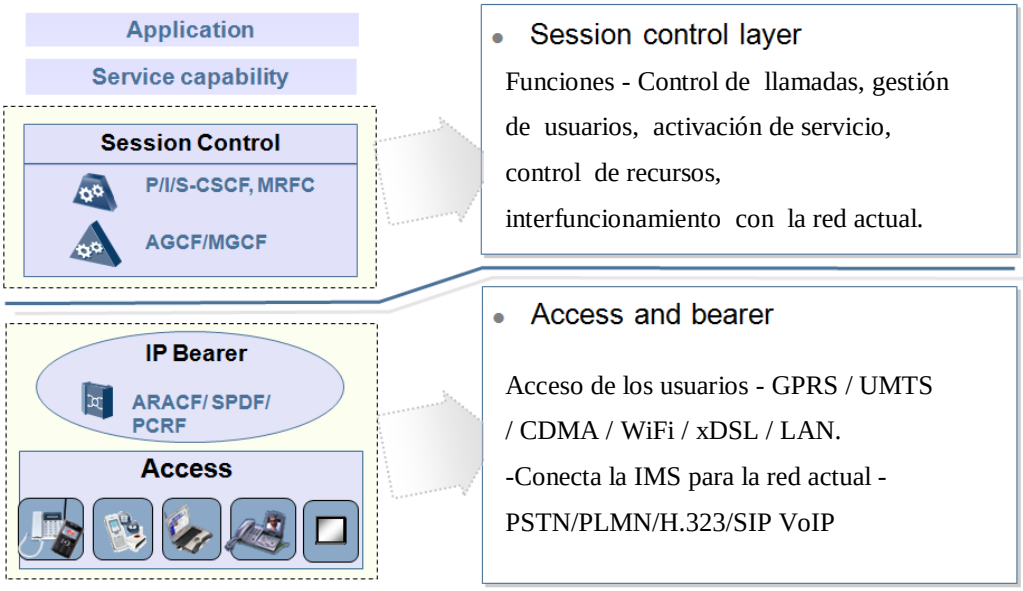


Figura 14: Capa Acceso / Portador.

Fuente: (Huawei Technologies Co., 2010)

A continuación tenemos las dos capas restantes que forman una arquitectura IMS, como son la capa de Servicio y la capa de Aplicación. La capa de Servicio ofrece la capacidad de distintos tipos de servicios a los clientes como presencia, telefonía general, VoIP, grupos, entre otros servicios. La capa de aplicación brinda a los clientes aplicaciones generadas por un tercero de confianza, como son los juegos, conferencias y chats, etc. La capa de Aplicación consiste en servidores de aplicación (*Application Server*) y MRF (*Multimedia Resource Function*) que son los servidores de media IP (*IP Media Server*).

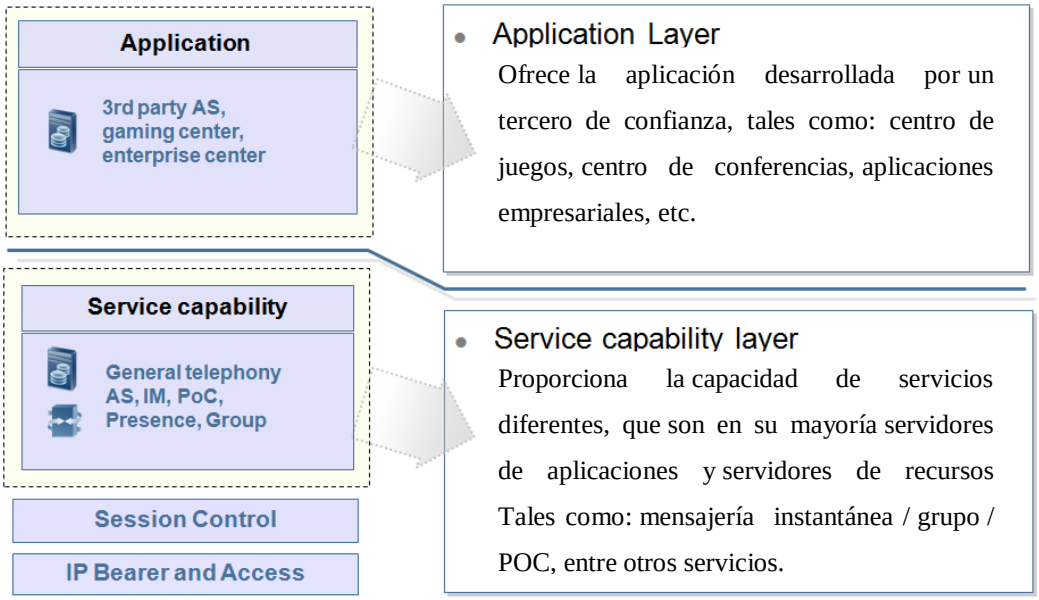


Figura 15: Capacidad de servicio y aplicación.

Fuente: (Huawei Technologies Co., 2010)

II.6.5 Elementos de la arquitectura IMS

Los elementos de red que conforman la arquitectura IMS, según (Huawei Technologies Co., 2010) se pueden observar en la tabla 4:

II.6.5.1 Capa de Control de Sesión

Función	Elemento	Función	Elemento
Control de Llamada (*Call Control*)	P-CSCF	Red de Interconexión (*Network Interworking*)	MGCF
	I-CSCF		IMS-MGW
	S-CSCF		BGCF
Gestión de Usuarios (*User Managment*)	HSS	Recursos Media (*Media Resources*)	MRFC
	SLF		MRFP

Tabla 4: Elementos de la Capa de Control de Sesión.

Fuente: (Huawei Technologies Co., 2010)

II.6.5.1.1 CSCF (*Call State Control Function*)

Es el elemento más importante dentro de la arquitectura IMS. Es el nodo encargado del control de la sesiones, realizando la correcta señalización a través del uso del protocolo SIP. Este elemento se divide en 3 subsistemas:

- **P-CSCF (*Proxy-Call State Control Function*):** en el plano de señalización, es el primer punto de contacto entre un terminal IMS (usuario) y el dominio de la red IMS. Es el elemento que controla el acceso a la red IMS, funcionando básicamente como un servidor proxy SIP. Dependiendo del usuario, se le asigna un P-CSCF distinto hasta que termine la sesión del mismo. El P-CSCF cumple funciones de control de seguridad, estableciendo varias asociaciones IPsec hacia el terminal IMS ofreciendo seguridad integral. Realiza funciones de control de NAT (*Network Address Translation*) seguro. El P-CSCF realiza la autenticación del usuario e informa al resto de los nodos de la red de la identidad del mismo, evitando futuras autenticaciones que ralenticen el proceso de señalización. El P-CSCF maneja de igual forma parámetros de calidad de servicio (QoS) y autoriza el uso de recursos, incluyendo un PDF (*Policy Decision Function*). (Cabrejos & Cuesta, 2009)

- **I-CSCF (*Interrogating-Call State Control Function*):** el I-CSCF funciona como un servidor proxy SIP, de igual forma que el P-CSCF, pero trabaja en el borde del dominio administrativo. Es la primera entrada a la red IMS por un transportista (*carrier*), teniendo información de la red en la que se encuentra el usuario. El I-CSCF tiene una funcionalidad conocida como THIG (*Topology Hiding Inter-Network Gateway*) o topología de la clandestinidad, para encriptar ciertas partes de los mensajes que sean de importancia para el usuario. El I-CSCF asigna el S-CSCF más apropiado dependiendo de la ubicación del usuario y realiza el enrutamiento para llegar al destino. El I-

CSCF interactúa con los servidores HSS (*Home Suscriber Servers*) y los SLF (*Suscriber Location Functions*) a través del uso del protocolo "Diameter".

- **S-CSCF (*Serving-Call State Control Function*):** es el elemento fundamental en la señalización. Es el nodo que permite la autenticación de usuarios registrados y el control de sesión de ruta (normal, interfuncionamiento, llamadas de emergencia). Funciona como un servidor SIP y provee servicios de enrutamiento SIP como función primordial. El S-CSCF es el encargado de inspeccionar todos los mensajes SIP y activar los servicios que requieren los usuarios. Toda la señalización SIP que los terminales IMS envíen o reciben, cursará por el S-CSCF designado. El S-CSCF, al igual que el I-CSCF, utiliza una interfaz con el servidor HSS haciendo uso del protocolo "Diameter", por las siguientes razones: (Cabrejos & Cuesta, 2009)

  - Obtener de los HSS los vectores de autenticación del usuario que desea acceder.
  - Informar a los HSS el S-CSCF designado durante el registro del usuario.
  - Obtener de los HSS el perfil del usuario, el cual incluye el perfil del servicio que informa al S-CSCF los servidores de aplicación de destino del mensaje SIP.

II.6.5.1.2 Bases de Datos

- **HSS (*Home Suscriber Servers*)**

Los HSS son un conjunto de servidores que contienen toda la información de suscripción relacionada al usuario requerida para el establecimiento de sesiones multimedia. Esta información incluye la identificación de los usuarios, numeración y correspondiente direccionamiento de la información, además de la información de seguridad de los usuarios (control de acceso de red para la autenticación y autorización), ubicación de los usuarios, el S-CSCF designado

para cada usuario y la información de perfil de cada usuario, que incluye el perfil de los servicios asignados.

- **SLF (*Suscriber Location Function*)**

Los SLF son nodos de bases de datos necesarios cuando los operadores de redes IMS poseen más de un servidor HSS debido a la gran cantidad de suscriptores que manejan. Los SLF permiten estos operadores de red, ubicar el servidor HSS que contiene toda la información del usuario correspondiente. Por lo general el SLF es combinado con el HSS, utilizando el protocolo "Diameter". (Cabrejos & Cuesta, 2009)

II.6.5.1.3 Nodos de Interconexión

PSTN/CS Gateway

El PSTN/CS Gateway permite a los terminales IMS enviar y recibir llamadas desde las redes basadas en conmutación de circuitos, como la red PSTN. Según (Mohammad & Syed, 2009), está formado por:

- **MGCF (*Media Gateway Control Function*)**

Es un elemento fundamental ya que es el elemento central del nodo PSTN/CS. Además controla el IMS-MGW para establecer, modificar y borrar canales de comunicación. Selecciona el I-CSCF correspondiente para las llamadas entrantes del nodo PSTN/CS. Es el encargado de realizar la conversión entre protocolos ISUP (usado para la red PSTN) y SIP. Utiliza el protocolo H.248 para comunicarse con el nodo IM-MGW.

- **IM-MGW (IMS-Media Gateway)**

Su función principal es la de terminar canales portadores de una red de conmutación de circuitos y flujos de datos multimedia desde una red de paquetes. Interconecta el plano multimedia de la red de conmutación de circuitos (PSTN). Este nodo envía y recibe datos multimedia a través del protocolo RTP (*Real-Time Transport Protocol*). Cuando el terminal IMS (usuario) no soporta el códec usado, este elemento se encarga de hacer transcodificación (*'transcoding'*) para que la información sea inteligible.

- **BGCF (*Breakout Gateway Control Function*)**

Este elemento se encarga de seleccionar el MGCF más adecuado para el interfuncionamiento con el dominio PSTN/CS. Es usado solamente en sesiones iniciadas por un terminal IMS, con destino a un usuario de la red de conmutación de circuitos, funcionando como un servidor SIP enrutando la llamada. (Mohammad & Syed, 2009)

II.6.5.1.4 Recursos Multimedia

- **MRFC (*Multimedia Resource Function Controller*)**

El nodo MRFC se encarga de controlar el flujo de recursos de los medios de comunicación en el MRFP (*Multimedia Resource Function Processor*). Este elemento tiene otra función, que es la de interpretar la información proveniente de un AS (*Aplication Server*) y S-CSCF (por ejemplo, un identificador de sesión) y un MRFP de control en consecuencia. Actúa como un SIP UA (*SIP-User Agent*) y posee una interfaz SIP con el S-CSCF correspondiente. **[** (Cabrejos & Cuesta, 2009)

- **MRFP (*Multimedia Resource Function Processor*)**

Este nodo proporciona recursos para ser controlados por el MRFC. Es el encargado de procesar los flujos de datos multimedia, ya sea realizando la transcodificación de los datos, analizando los medios de comunicación, etc. La MRFC controla los recursos en la MRFP, que es el elemento que implementa todas las funciones multimedia, a través de una interfaz H.248.

II.6.5.2 Capa de Acceso y Control al Portador

Función	Elemento	Función	Elemento
Control de Recursos (*Resource Control*)	PCRF	Cobrador(*Charging)*	CCF
	SPDF+A-RACF	Gestión de Elementos de Red (*NE Manage*)	OMS
Control de Acceso (*Access Control*)	NACF	SBC(*Session Border Controller*)	ABGF
	CLF	Nombre y dirección (*Naming and Address*)	DNC/ENUM

Tabla 5: Elementos de la Capa de Acceso y Control al Portador.

Fuente: (Huawei Technologies Co., 2010)

PCRF/SPDF

La función principal de este nodo, es la de realizar la función de calidad de servicio (QoS) en la red IMS (*policy control*).

NACF/CLF

Trabaja como DHCP (*Dynamic Host Configuration Protocol*) y la función del servidor AAA (*Autenthication, Authorization, Accounting*) para el usuario de la red de acceso fijo.

DNS/ENUM

Este nodo es el encargado de traducir las URL (*Uniform Resource Locator*) a una dirección IP para la sesión de enrutamiento (DNS); y la función ENUM (E.164 asignación de número URI) se utiliza para traducir el número URI (teléfono) a SIP URI.

NAT/SBC

Este nodo realiza funciones de NAT transversal, seguridad, conversión de IPv4/IPv6, etc. También trabaja como un Proxy para datos multimedia, control y seguridad de calidad de servicio para la red fija. (Cabrejos & Cuesta, 2009)

II.6.5.3 Capa de Capacidad de Servicio

Servidores de Aplicación AS (*Application Servers*)

Un AS ofrece servicios de mensajería instantánea y puede encontrarse en la red local del usuario o en una locación de terceros. Su principal función es procesar los mensajes SIP de la red IMS e iniciar los mensajes SIP, es decir, que son entidades que reciben y ejecutan servicios (Cabrejos & Cuesta, 2009). Dependiendo del servicio que ejecutan existen tres (3) clases de AS, los cuales se pueden observar en la figura 16:

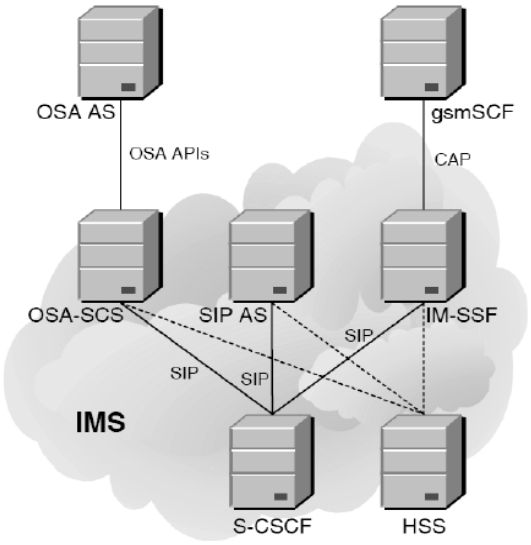


Figura 16: Servidores de Aplicación en IMS.

Fuente: (Huawei Technologies Co., 2010)

- **OSA-SCS (*Open Service Architecture-Service Capability Server*)**

  Este servidor de aplicación tiene la capacidad de acceder a la seguridad IMS desde redes externas. Funciona como un servidor de aplicación siendo un intermediario entre el S-CSCF y SIP, y también trabaja como una interfaz entre el OSA AS y el OSA API (*OSA Application Programming Interface*).

- **SIP AS (*SIP Application Server*)**

  Este servidor de aplicación es el que implementa un servicio para el usuario IMS. Este servidor recibe y ejecuta los servicios multimedia basados en el protocolo SIP.

- **IM-SSF (*IP Multimedia Service Switching Function*)**

  Permite volver a usar los servicios CAMEL (*Customized Applications for Mobile network Enhanced Logic*) que fueron desarrollados por GSM en IMS. El IM-SSF permite a la GSM SCF (*GSM Service Control Function*) controlar la sesión IMS. Actúa, por un lado como un servidor de aplicaciones (intermediario entre el S-CSCF con SIP), y por otro como un SSF (*Service*

Switching Function) con una interface hacia la GSM SCF basada en CAP (*CAMEL Application Part*). (Cabrejos & Cuesta, 2009)

II.6.6 Protocolos usados en IMS

II.6.6.1 SIP (*Session Initiation Protocol*)

SIP es un protocolo simple y flexible para crear, modificar y finalizar sesiones. Trabaja de manera independiente de los protocolos de transporte subyacente. Según (Huawei Technologies Co., 2010)**,** tiene las siguientes características:

- Simple – Estilo de texto, similar al HTTP y el protocolo SMTP.
- Extensible – Puede cooperar con otro protocolo, como el SDP / MSML.
- Flexible – Es capaz de soportar encabezados especiales.

Flujo básico del protocolo SIP en IMS

- Registro del usuario (UA)

En la figura 17, se puede observar el flujo de señalización para el registro de un usuario en IMS:

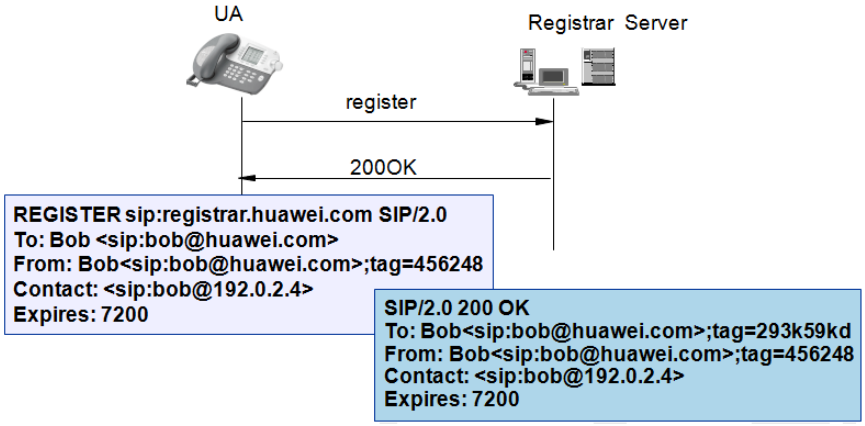


Figura 17: Registro del usuario (UA) SIP.

Fuente: (Huawei Technologies Co., 2010)

- Inicio de la sesión y liberación del flujo de datos

En la figura 18, se especifican los mensajes correspondientes al flujo de señalización para el inicio y liberación de una llamada cualquiera:

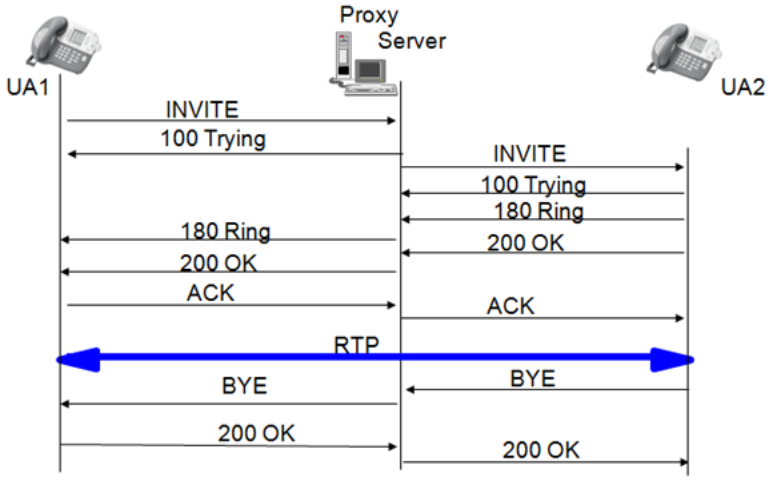


Figura 18: Inicio de la sesión del usuario SIP.

Fuente: (Huawei Technologies Co., 2010)

- Envío de una solicitud (INVITE)

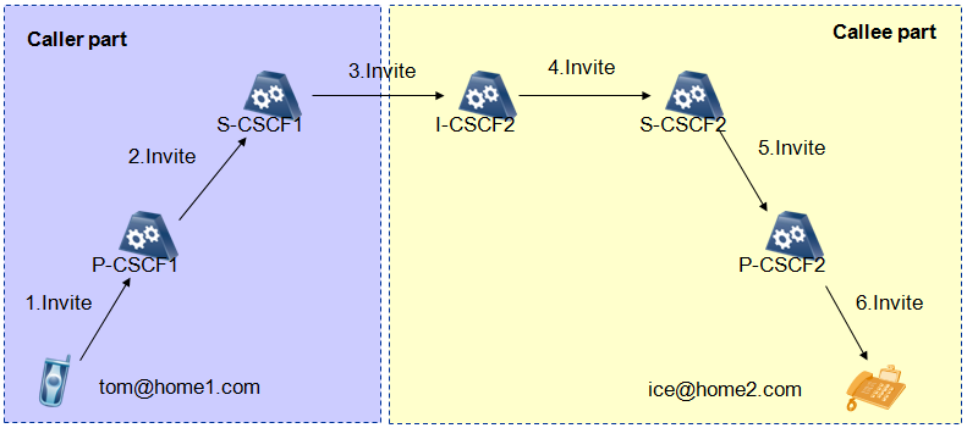


Figura 19: Señalización en IMS. Envío mensaje INVITE SIP.

Fuente: (Huawei Technologies Co., 2010)

Para el caso de enviar una solicitud para iniciar una llamada, el usuario que realiza la solicitud (*Caller*) tom@home1.com, envía un mensaje INVITE con el fin de establecer una llamada con el segundo usuario ice@home2.com. El

mensaje INVITE pasa por el P-CSCF (*Proxy-Call State Control Function*) el cual actúa como un servidor proxy para verificar el mensaje INVITE y realizar la autenticación del usuario. Una vez autenticado correctamente el usuario, el P-CSCF envía la información al S-CSCF1 (*Serving-Call State Control Function*), el cual es el nodo central en la señalización, encargado del control de la sesión. El mensaje INVITE pasa por el I-CSCF (*Interrogating-Call State Control Function*), el cual obtiene la información de la ubicación del usuario y enruta la petición al próximo nodo (S-CSCF2), después pasa por el otro P-CSCF2 hasta finalmente llegar al segundo usuario. El flujo se puede observar en la figura 20.

- Respuesta de la solicitud (respuesta 183) al mensaje INVITE

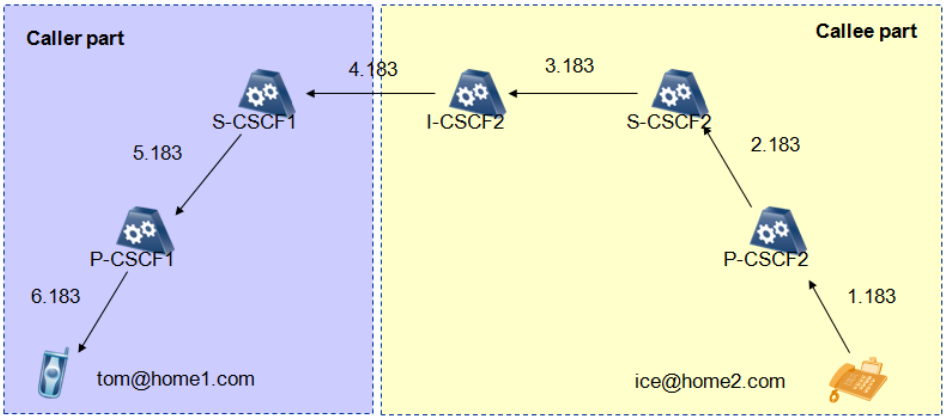


Figura 20: Respuesta del mensaje INVITE SIP.

Fuente: (Huawei Technologies Co., 2010)

En la figura 20, se observa la respuesta del segundo usuario ice@home2.com al llegar el mensaje INVITE, el teléfono comienza a repicar y se envía un mensaje de respuesta 183 (*Session Progress*) que indica que la sesión está en progreso a falta de autenticar el segundo usuario. El mensaje 1.183 informa al P-CSCF2 que el usuario es el correcto (ice@home2.com) e informa a todos los demás nodos de la red la identidad del usuario 2, el P-CSCF2 verifica la identidad del usuario y envía el mensaje 2.183 al S-CSCF2 para que controle y gestione el progreso de la sesión. El S-CSCF2 envía el mensaje 3.183 al I-

CSCF2 para que obtenga la información de la ubicación del usuario y enruta la petición al próximo nodo. Se repite el proceso pasando el mensaje del S-CSCF1 al P-CSCF1 hasta llegar al usuario que realizó la petición (tom@home1.com). La diferencia entre cada uno de los mensajes (1.183, 2.183, 3.183, etc.) radica en el campo 'via', dependiendo donde se encuentre el mensaje cada nodo debe agregar la dirección de cada nodo que debe atravesar el mensaje hasta llegar a su destinatario.

II.6.6.2 SDP (*Session Description Protocol*)

Es un protocolo de capa de aplicación para la descripción de las sesiones multimedia, presente en el cuerpo (*body*) de los mensajes SIP. Provee la suficiente información para la parte llamante (*caller*) y la parte llamada (*callee*), sobre las capacidades de ambos usuarios (estas capacidades pueden intercambiarse en el momento de negociación de la sesión o cuando se encuentre en curso); el protocolo SDP también incluye: tipo de data (información) a transmitir, destino de la información, nombre de la sesión y propósito, información de contacto. Los mensajes SDP, según (Cabrejos & Cuesta, 2009)**,** tienen 3 niveles de información:

- Descripción de la sesión de nivel: incluye identificador de la sesión y otros parámetros del nivel de sesión.
- Descripción del tiempo: tiempos de inicio y fin, y descripciones del nivel multimedia.
- Formato y tipo de sesión: protocolo de transporte, número de puerto y descripción del tipo de sesión multimedia.

II.6.6.3 RTP (*Real-Time Transport Protocol*)

Este protocolo es fundamental en el ámbito IMS, ya que permite el intercambio de la media (voz, video, datos, etc.) en tiempo real entre dos usuarios (end-to-end), identificar el tipo de códec, numeración secuenciada y monitorización de envío de la data. Este protocolo no provee calidad de servicio (QoS), para monitorear la QoS de la comunicación, RTP utiliza el protocolo de control RTCP (*Real-Time Transport Control Protocol*). El protocolo RTCP es fundamental para transmitir información de control de la sesión, transmitir el identificador de origen RTP y monitorear parámetros de QoS de la transmisión. (Huawei Technologies Co., 2010)

II.6.6.4 Diameter

Es un protocolo de red para brindar Autenticación, Autorización y Auditoría AAA (*Authentication, Authorization and Accounting*) en el acceso de los usuarios a la red IMS. Este protocolo se basa en el antiguo protocolo RADIUS, usado anteriormente para proveer servicios AAA. Dentro del entorno IMS, el protocolo Diameter se puede dividir en: el protocolo base Diameter, usado para negociar capacidades y para el manejo de errores; y las aplicaciones Diameter, que definen funciones especificas de cada aplicación disponible. En IMS se utilizan dos aplicaciones, Diameter SIP y DCC (*Diameter Credit Control*). Este protocolo es muy importante para la red IMS, ya que los servidores de bases de datos HSS y SLF se comunican a través de este protocolo, al igual que el I-CSCF para verificar con el HSS la identidad de un usuario. (Cabrejos & Cuesta, 2009)

II.6.6.5 MEGACO – H.248

Protocolo desarrollado en conjunto por la ITU y la IETF, que define el mecanismo de llamada para permitir al MGCF el control de puertas de enlace, a través del IMS-MGW, para el soporte de llamadas entre las redes PSTN-IP o IP-IP. Este protocolo es

fundamental para el entorno IMS, ya que es usado entre el IMS-MGW (*IMS-Media Gateway*) y el MGCF (*Media Gateway Controller Function*), para el manejo de la señalización la gestión de las sesiones multimedia. El MGCF utiliza el protocolo H.248 para controlar los recursos de la media en el IMS-MGW. El MGCF y el IMS-MGW guardan una relación maestro/esclavo. (Cabrejos & Cuesta, 2009)

II.6.6.6 COPS (*Common Open Policy Service*)

Este protocolo se utiliza en IMS para el intercambio de la información de política de la red, entre el PDP (*Policy Decision Point*) y los PEP (*Policy Enforcement Points*). (Huawei Technologies Co., 2010)

II.6.7 Beneficios de la tecnología IMS

Las razones estratégicas para que las operadoras implanten IMS en sus redes son, básicamente: una significativa reducción de los costos de la red tanto en personal como en infraestructuras, favoreciendo la escalabilidad y amortización más rápida de su red; la rápida implantación y proliferación de nuevos servicios más adaptados al cliente, ayudando a su fidelización; y un considerable incremento de las ventas y flujos de caja procedentes de los mismos. (Tejedor Millán, 2006)

En la estructura de red tradicional cada servicio tiene implementaciones separadas de funcionalidades comunes (facturación, presencia, gestión de grupos y listas de contactos, encaminamiento, provisión, etc.), y la estructura está replicada a lo largo de toda la red. IMS proporciona una serie de funciones comunes que son genéricas en su estructura e implementación, y que pueden ser reutilizadas por todos los servicios de la red. Por ejemplo, el sistema de facturación IMS registra los datos relacionados con la sesión IMS, tales como los usuarios implicados, la duración, los componentes multimedia empleados y la calidad de servicio (QoS) autorizada; y permite facturar cualquier tipo de servicio tanto en postpago como en prepago, según su duración, contenidos, volumen de datos, destino de la sesión o las diferentes combinaciones de

los anteriores. Esto además facilita y acelera el proceso de creación y suministro de servicios, la reutilización de infraestructura de transporte de red y de servidores de aplicaciones, y minimiza el inmovilizado fijo y la necesidad de personal técnico en todas las áreas (provisión, operación y mantenimiento, facturación, etc.). (Tejedor Millán, 2006)

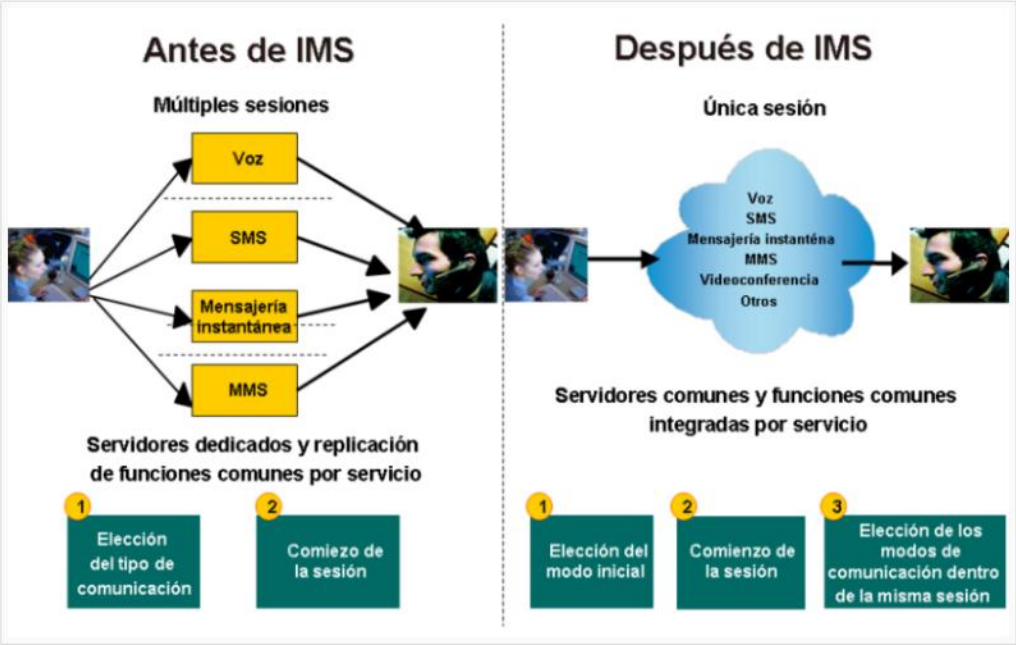


Figura 21: Estructura general de la tecnología IMS.

Fuente: (Tejedor Millán, 2006)

La posibilidad de ofrecer paquetes de servicios es muy importante para las operadoras de telecomunicación. Por ejemplo, la ventaja tradicional de las operadoras de cable frente a los antiguos ex-monopolios telefónicos, era la posibilidad de ofrecer una oferta integrada de telefonía, Internet y televisión. Ahora que la amenaza son los nuevos proveedores de servicios que son capaces de ofrecer aplicaciones gratuitas o a bajo coste sobre su infraestructura de red. De esta forma, empresas como Skype pueden ofrecer VoIP de bajo costo a sus usuarios empleando una arquitectura P2P, sin tener que pagar al proveedor de acceso a Internet por ofrecer dicho servicio y sin tener que asumir el mantenimiento de ninguna infraestructura de red y siendo

tan sólo necesarios unos pocos servidores. No obstante, estas empresas no son capaces de ofrecer el catálogo de servicios que podría ofertar una operadora con IMS. Además, las operadoras podrán gracias a IMS ir entrando en el mundo de los servicios informáticos, permitiendo a sus clientes empresariales disfrutar de muchas de sus aplicaciones actuales bajo el modelo de pago por uso, sin tener que realizar constantes inversiones en hardware y software, ya que será más rentable y eficiente distribuirlas en red. (Tejedor Millán, 2006)

La telefonía móvil e Internet han demostrado que los usuarios están cada vez más interesados en servicios de comunicación más allá de la voz, como demuestra el éxito de los SMS y de la mensajería instantánea, respectivamente. Pero los usuarios de telecomunicación actuales están cada vez más informados y son más exigentes, y se ha demostrado con iniciativas como los servicios 3G, que no siempre se cumplen las expectativas creadas por las operadoras y suministradores de infraestructura de telecomunicación. Para que los servicios multimedia tengan éxito, no basta con que sean útiles, también es necesario que sean sencillos de utilizar, baratos y accesibles en cualquier momento y lugar. Para los usuarios, los servicios basados en IMS permiten la comunicación persona a persona y persona a contenido en gran variedad de modos (incluyendo voz, texto, imágenes y vídeo, o una combinación de todas ellas) de una forma altamente personalizada y mucho más sencilla, porque el servicio es independiente del tipo de terminal o red de acceso que emplee en ese momento. Los usuarios se verán así beneficiados por servicios más adaptados a sus necesidades y fáciles utilizar, precios más competitivos, única factura, y mayor sencillez en las gestiones de incidencias. (Real Martín, 2008)

IMS abre nuevas perspectivas para los operadores de red. Sin embargo, varias técnicas y los desafíos de negocios se tienen que enfrentar con el fin de permitir la adopción generalizada de esta prometedora tecnología. Cuestiones comerciales: IMS lleva los operadores de redes a desempeñar un papel central en el servicio de distribución de los servicios. Esto implica que las compañías se han para obtener el contenido. El papel de los operadores en la facturación de los servicios prestados por

terceros también tiene que aclararse. Con IMS un solo cliente puede suscribirse a los servicios de varios proveedores. IMS tanto, lleva la red operadores en una competición con jugadores de la Internet en el mundo. La decisión de desplegar IMS es estratégica. Cuestiones técnicas: El extremo a extremo, modelo adoptado en IMS introduce varios problemas técnicos, por ejemplo, en materia de calidad de servicio (QoS), privacidad y la facturación. La cuestión tecnológica principal está relacionada con la interoperabilidad. IMS mezcla los puntos de vista de la IP, telefonía fija, telefonía móvil y los operadores de redes. Por último, que utiliza algunos protocolos recientes como Diameter que no han sido ampliamente desplegados. Por todas estas razones, la interoperabilidad puede ser difícil de conseguir en las redes IMS. (Poikselka, Mayer, Khartabil, & Niemi, 2006)

Capítulo III
Marco Metodológico

Este capítulo contempla la metodología utilizada para la ejecución del Trabajo Especial de Grado. En esta sección se encuentran definidas, las actividades realizadas y los procedimientos requeridos para la investigación, durante cada una de las fases establecidas para el cumplimiento de los objetivos planteados en el presente proyecto.

III.1 Tipo de Investigación

El Tipo de Investigación del presente Trabajo Especial de Grado es considerada de Campo, ya que se reúne la información necesaria a partir del contacto directo con los hechos que se encuentran en estudio, ya sea que estos hechos ocurran de manera ajena al investigador o sean provocados por éste con un adecuado control de las variables que intervienen en dichos fenómenos.

Adicionalmente es considerada una investigación de tipo Experimental, ya que se introducen cambios de manera controlada y sistemática dentro de los sistemas que se encuentran en estudio, para así observar las consecuencias de dichas alteraciones, en otras palabras, el investigador produce cambios en una o varias variables independientes para conocer los efectos que se generan en una o mas variables dependientes que son de interés en el estudio. Se manipulan variables como la cantidad de llamadas por segundo, porcentaje de uso del CPU, duración de las llamadas, longitud de mensajes, entre otras.

Y finalmente se puede decir que también es una investigación del tipo Documental ya que se reúne la información necesaria para la realización del trabajo recurriendo fundamentalmente a fuentes de datos en los que la información ya se encuentra

registrada, tales como libros, revistas especializadas, archivos, informes de investigaciones ya realizadas, etc. (Moreno Bayardo, 1987)

III.2 Descripción de Procedimientos y Actividades

En esta parte del capítulo se definen los pasos realizados para llevar a cabo el presente Trabajo. Para hacer más sencillo el entendimiento de los procedimientos y actividades para el logro de los objetivos propuestos, se decidió seguir una metodología dividida en cuatro fases bien demarcadas y definidas para la realización de este Trabajo Especial de Grado. (Ver, Figura 23)

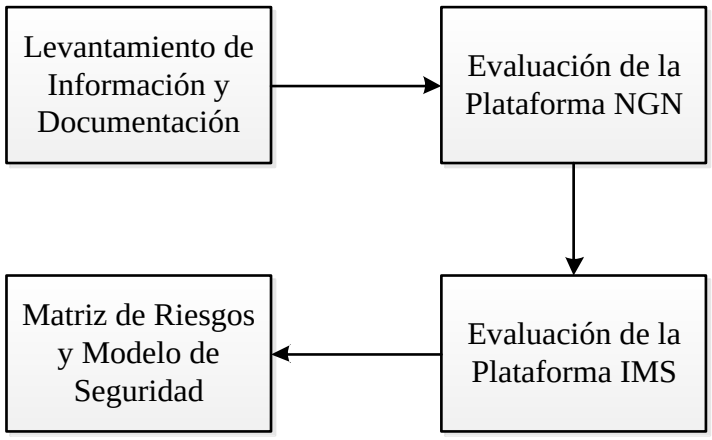


Figura 22: Esquema fases marco metodológico.

Fuente: [Elaboración propia]

III.2.1 Fase 1- Levantamiento de Información y Documentación

Se requiere realizar una investigación exhaustiva basada en la información teórica necesaria referente a los conceptos, aplicaciones, topologías, protocolos y servicios de las plataformas NGN (*Next Generation Networks*), así como también acerca de la tecnología IMS (*IP Multimedia Subsystem*) para con esto conocer sus funcionalidades e identificar fortalezas y riesgos que sirvieron de base para la posterior elaboración

del Modelo. Para esto, se necesita recaudar información de distintas fuentes, tales como libros, textos, artículos, manuales, publicaciones en Internet e informes técnicos, además de otras Tesis de Grado.

III.2.2 Fase 2- Evaluación de la Plataforma NGN

Se realizó una evaluación profunda, mediante investigación y pruebas de seguridad de la operación y servicios de la capa de control de la plataforma NGN de CANTV, con este estudio se busca conocer sus vulnerabilidades para así buscar posibles soluciones o mecanismos de defensa y mitigación. Las pruebas realizadas fueron en el laboratorio ubicado en el piso 6 del edificio Equipos II del Centro Nacional de Tecnología de CANTV, donde se disponía de los elementos principales, ejecutando protocolos de prueba y herramientas de análisis de seguridad.

III.2.3 Fase 3- Evaluación de la Plataforma IMS

Se realizó evaluación de la plataforma IMS en el laboratorio ubicado en el piso 6 del edificio Equipos II del Centro Nacional de Tecnología de CANTV, para detectar vulnerabilidades o fallas presentes y de esta forma proponer posibles requerimientos que garanticen la seguridad de la plataforma. Las pruebas se realizaron de forma directa en dicho laboratorio donde se disponía de los elementos principales, ejecutando protocolos de prueba y herramientas de análisis de seguridad.

III.2.4 Fase 4- Matrices de Severidad de Riesgos y Modelo de Seguridad

Se documentaron dos matrices de severidad de riesgos de las tecnologías NGN e IMS respectivamente, con las vulnerabilidades y amenazas detectadas en las pruebas realizadas de ambas plataformas. En base a los resultados obtenidos se elaboraron dichas matrices, clasificando las vulnerabilidades por la consecuencia que puede llegar a ocasionar en caso de presentarse, probabilidad de ocurrencia y severidad del riesgo detectado, para poder dar sustento a la generación del modelo de seguridad, elaborando los documentos conceptuales, diseño de arquitectura conceptual,

especificaciones técnicas que se deben cumplir para proporcionar la seguridad necesaria para el aseguramiento de la plataforma IMS de CANTV.

Capítulo IV
Desarrollo

En este capítulo se explican detalladamente todos los pasos realizados para la elaboración del presente Trabajo Especial de Grado. Empezando por la documentación y levantamiento de información de las tecnologías NGN e IMS, la evaluación de las plataformas NGN e IMS, y finalmente una Matriz de Riesgos que permitirá la elaboración del Modelo de Seguridad que es el principal objetivo de este Trabajo.

IV.1 Levantamiento de Información y Documentación

Esta fase inicial consistió en investigar detallada y exhaustivamente la información necesaria para poder llevar a cabo el proyecto, empezando las redes basadas en conmutación de circuitos, como las Redes Telefónicas Publicas Conmutadas (PSTN), las redes basadas en conmutación de paquetes, o redes "*All-IP*" como son las Redes de Próxima Generación (NGN). Se realizó una investigación exhaustiva sobre la plataforma NGN, los elementos que la conforman, protocolos de señalización utilizados por esta tecnología, ventajas de este tipo de redes, etc. Se realizaron búsquedas electrónicas a través de Internet en libros, revistas, servidores dedicados, tesis de grado anteriores y documentación proporcionada por la empresa donde se desarrolló el proyecto. Se realizaron numerosas visitas y entrevistas a personas expertas del área de seguridad y de gestión de la red NGN de CANTV, para conocer la arquitectura y elementos presentes en la misma. La información más relevante se encuentra documentada en el marco teórico del presente documento.

Para finalizar esta primera fase del trabajo, al igual que para la plataforma NGN se realizó una investigación exhaustiva acerca de la tecnología IMS, como su arquitectura y los elementos que la conforman, los protocolos de señalización

utilizados, y los beneficios de la implementación de esta tecnología. Para esto también se realizaron búsquedas electrónicas en libros, revistas electrónicas y tesis de grado anteriores, así como entrevistas con personal de la empresa conocedores de la tecnología IMS.

IV.2 Evaluación de la Plataforma NGN

Para esta segunda fase se inició con la evaluación de la plataforma NGN en laboratorio de CANTV. Se estudió a profundidad la plataforma NGN de CANTV, sus ventajas y desventajas, a partir de la documentación y toda la información recopilada, para determinar puntos vulnerables o posibles brechas presentes, a nivel de seguridad de la operación, que puedan atentar contra la plataforma NGN o contra los servicios ofrecidos a los usuarios finales. Se realizaron numerosas consultas con diferentes personalidades, expertos, en elementos y dispositivos NGN, y personal del laboratorio, para la realización de las pruebas. Se sostuvo una reunión con el Ingeniero Francisco Lagos el día 19/12/2012, en el 'Centro de Operaciones de la Red' de CANTV Los Palos Grandes, para determinar arquitectura y elementos que posee la red actual NGN de CANTV. El Ingeniero mostró su total interés y aprobación a la elaboración de una arquitectura de Seguridad IMS previa a la implementación de cualquier servicio o tecnología. La arquitectura actual de la red NGN de CANTV, está conformada como se puede observar en la figura 23:

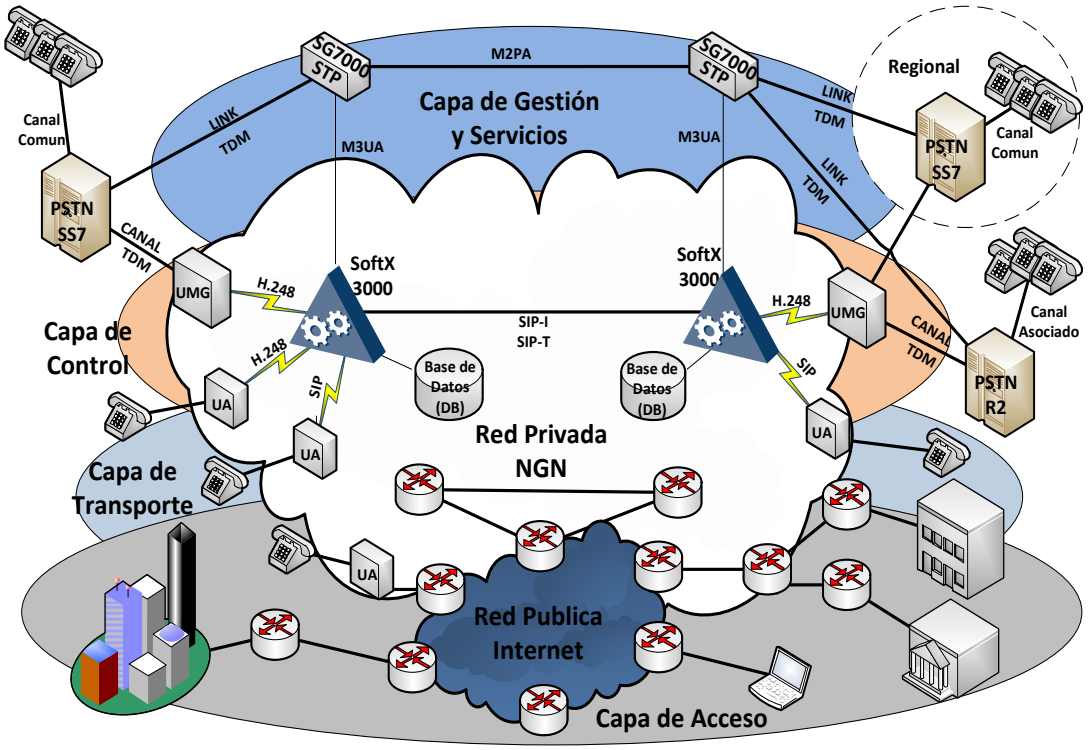


Figura 23: Plataforma NGN (*Next Generation Network*).

Fuente: [Elaboración propia].

A continuación se procedió a elaborar un protocolo de pruebas, con los aspectos a evaluar necesarios para determinar los riesgos presentes o potenciales en la plataforma que puedan ocasionar la degradación o negación de los servicios. Las pruebas se fundamentaron en dos (2) protocolos principalmente; el protocolo SIP (*Session Initiation Protocol*), encargado de iniciar, mantener y finalizar las llamadas; y el protocolo H.248/MEGACO, que está definido para la señalización y la gestión de las sesiones, y para la comunicación entre elementos de control de la red NGN. Un técnico de Huawei (empresa proveedora de los equipos) sirvió de apoyo en la realización de las pruebas, para la configuración de los parámetros y características necesarias para iniciar las pruebas y establecer trazas para capturar la señalización correspondiente. Se configuraron las variables de monitoreo a tener en consideración durante la evaluación, en cuanto a comportamiento del servicio, licencias requeridas,

porcentaje de uso del CPU del *Softswitch*, RAM y tráfico de red. Las pruebas propuestas se ejecutaron en su totalidad aproximadamente en dos (2) semanas.

El protocolo de pruebas para la plataforma NGN, fue dividido en seis grupos dependiendo del área a la que estaban enfocadas; el primer grupo estaba formado por pruebas de funcionamiento básico de VoIP, entre las cuales se pueden nombrar cursar llamadas utilizando diferentes códec de voz (G.711u, G.711a, G.723, G.726, G.729a), llamadas con y sin autenticación contra el Softswitch. Para el primer grupo de evaluaciones se utilizó un dispositivo de tráfico de llamadas conocido como *SmartClass* TPS (*Triple Play Services*), con el cual se generaron reportes, verificando parámetros de calidad de servicio de las llamadas y capturando los paquetes correspondientes a la señalización. El segundo grupo de pruebas, estaba enfocado a posibles fraudes y vulnerabilidades como la generación de llamadas SIP entre dos abonados con la misma identidad (duplicidad), validación de autenticación para elementos de acceso SIP y H.248, intento de suplantación de identidad (*spoofing*) a través de su dirección física y/o dirección IP, entre otras pruebas; el segundo grupo de pruebas se ejecutaron con una herramienta de tráfico de paquetes con cabeceras modificadas, según el RFC 4475.

Para el siguiente grupo de pruebas, se validaron aspectos de seguridad y cifrado en la señalización y el flujo RTP (voz), conteniendo diferentes tipos de pruebas entre las cuales se encuentran validar encriptación de la carga útil (*payload*), validación AAA (*Autorization, Authentication and Accounting*), modificación de parámetros de cabecera de los mensajes INVITE SIP (longitud, IP origen, IP destino, números origen y destino, etc.), verificando protección del *Softswitch* frente a la inundación de paquetes maliciosos; para este grupo de pruebas se utilizó un software de tráfico de paquetes para el descubrimiento de dispositivos SIP, según el RFC 3261. El cuarto grupo englobó todo lo relacionado a ataques de negación/degradación de servicios, incluyendo pruebas como generación de flujo de llamadas a números no existentes y números incompletos, para elementos SIP y H.248, determinar rendimiento del

Softswitch frente a la inundación de paquetes TCP/UDP y ataque de señalización SIP contra nodo de acceso; para este grupo se utilizó una herramienta *Exploit Toolkit* para la generación de llamadas bajo el protocolo SIP, según el RFC 2833.

El siguiente grupo corresponde a las pruebas de rendimiento de la red NGN, como verificar procesamiento del *Softswitch* frente al envío de múltiples solicitudes de mensajes SIP, simulando tráfico de llamadas en hora pico o BHCA (*Busy Hour Call Attempts*); se realizaron las pruebas según una herramienta de tráfico de llamadas bajo los protocolos SIP, H.248 y Diameter.

El último grupo de pruebas está conformado por otras funcionalidades de la plataforma NGN, como el manejo de CAC (*Call Admitance Control*), autenticación e integración de elementos no Huawei, conocer si es posible evitar generación de CDR (*Call Detail Record*) para un abonado o grupo de abonados y capacidad de bloqueo de un usuario por parte de un elemento de control de la red debido a comportamiento irregular o fraudulento.

Las configuraciones previas al inicio de las pruebas se pueden observar a continuación:

- Dirección Lógica (IP) del *Softswitch*: 172.16.80.42/26.
- Dirección Lógica (IP) del Usuario 1: 172.16.74.51.
- Dirección Lógica (IP) del Usuario 2: 172.16.74.52.
- Máscara de Red (Usuarios): 255.255.255.240.
- Puerta de enlace predeterminada (*Default Gateway*): 172.16.74.1.

Se realizaron varias entregas del protocolo con el tutor y se elaboró el documento definitivo. Se elaboró el escenario de pruebas basado en la interconexión de la plataforma NGN presente en el laboratorio. El escenario para la evaluación de la plataforma, se puede observar en la figura 24:

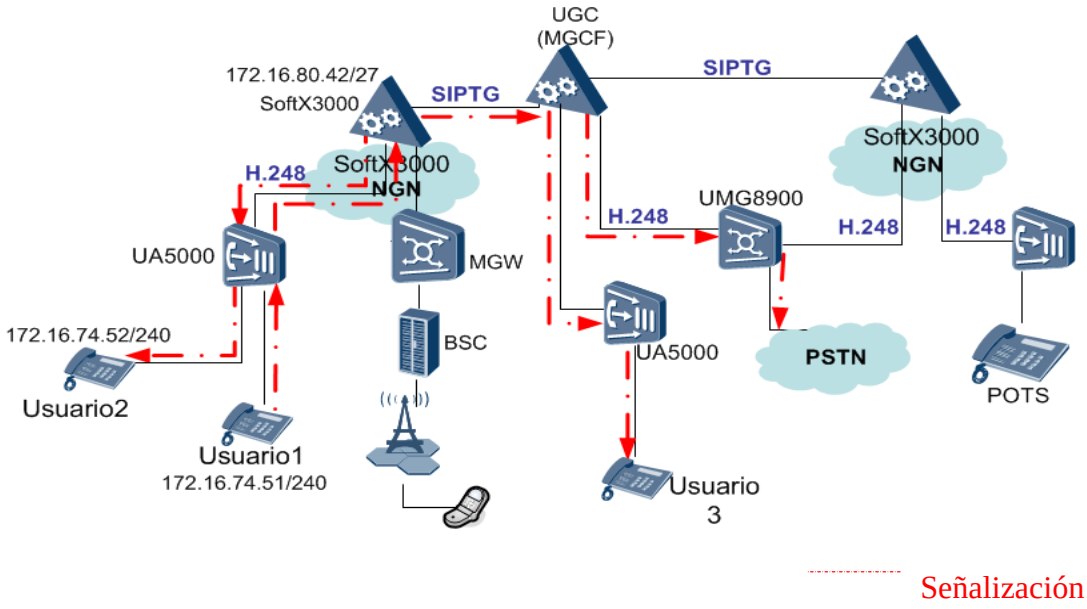


Figura 24: Escenario de pruebas protocolo NGN.

Fuente: [Elaboración propia].

Los resultados obtenidos en cada prueba se encuentran documentados en el protocolo NGN. Los riesgos identificados se pueden observar en el capítulo V, correspondiente a Resultados, del presente documento.

IV.3 Evaluación de la Plataforma IMS

Para esta tercera fase se inició con la evaluación de la plataforma IMS ubicada en el laboratorio de CANTV. Se estudió a profundidad la plataforma, elementos que la conforman (P-CSCF, I-CSCF, S-CSCF, HSS, BGCF, MRFC, etc.), ventajas y desventajas que ofrece la tecnología, a partir de la documentación y toda la información recopilada, para determinar puntos vulnerables o posibles brechas presentes, a nivel de seguridad de la operación, que puedan atentar contra la plataforma IMS o contra los servicios ofrecidos a los usuarios finales. Se realizaron numerosas consultas con diferentes personalidades expertos en elementos y dispositivos IMS, y con el personal del laboratorio, para plantear los posibles escenarios para la realización de las pruebas. Se mantuvo una reunión con Antonieta

Lobo el día 10/11/2012, para determinar el proceso para la elaboración de una arquitectura conceptual y especificaciones técnicas, en este sentido para lograr conocer la metodología empleada por CANTV, y como orientación para el desarrollo del modelo de Seguridad de la plataforma IMS. De igual forma se obtuvo la conformidad de la Ingeniero en la elaboración del presente trabajo de tesis, como documento inicial de seguridad para una posible implementación de la tecnología en CANTV.

El diagrama lógico de los equipos IMS presentes en el laboratorio de CANTV, se puede observar en la figura 25. La plataforma IMS en laboratorio, está formado en su totalidad por equipos Huawei.

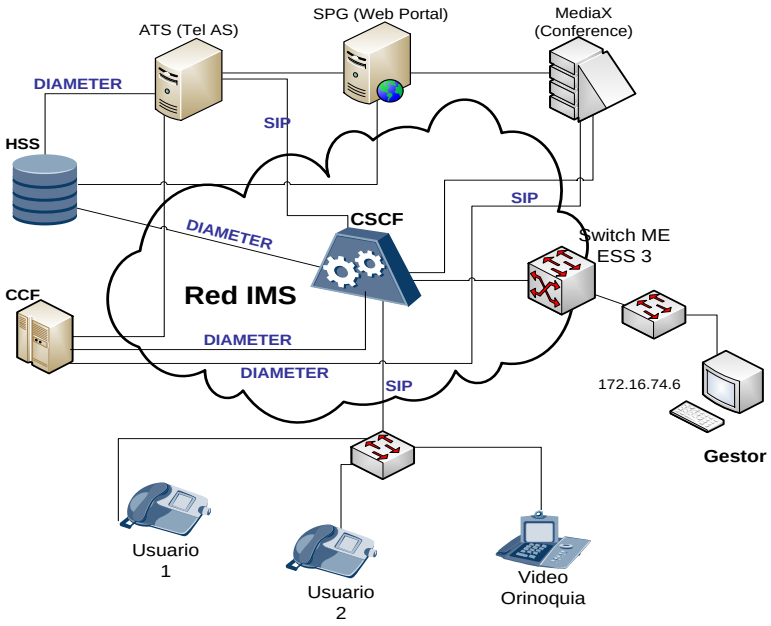


Figura 25: Esquema red IMS. Maqueta laboratorio de CANTV.

Fuente: [Elaboración propia].

Se determinaron capacidades de cada dispositivo que conforman la plataforma IMS de CANTV, las cuales se pueden observar en la tabla 6:

Elemento	Función	Licencias	Versión Sw
MediaX3600	Servidor de Conferencia	830 puertos	V3R5
MRP6600	Servidor de Media	702 canales	V1R2
CSC3300	CSCF/MRFC	2000 subscriptores	V1R6
HSS9820	HSS	2000 subscriptores	V9R6
iCG9815	CCF	30k CDR/hora	V3R2
ATS9900	Servidor de Telefonía	2000 subscriptores	V1R2
UGC3200	MGCF	92 Erl	V2R8

Tabla 6: Capacidades por dispositivo de la plataforma IMS instalada en Laboratorio. Fuente: (Compañía Anónima Nacional Teléfonos de Venezuela. CANTV, 2010).

Finalizado el estudio de la plataforma IMS en maqueta de CANTV, se procedió a elaborar un protocolo de pruebas, con las evaluaciones necesarias para determinar los riesgos presentes en la plataforma que puedan ocasionar la degradación o negación de los servicios. Las pruebas se fundamentan en tres (3) protocolos principalmente; el protocolo SIP (*Session Initiation Protocol*), encargado de iniciar, mantener y finalizar las llamadas; el protocolo Diameter, protocolo AAA (*Authorization, Authentication and Accounting*) para usuarios con conexión remota y sirve de comunicación entre elementos de control de la red IMS (CSCF, HSS, ATS, CCF); y el protocolo H.248/MEGACO, que está definido para la señalización y la gestión de las sesiones. De la misma forma que para la evaluación de la plataforma NGN, sirvió de apoyo un técnico de Huawei (empresa proveedora de los equipos) para la realización de las pruebas, en cuanto a la configuración de los parámetros y características necesarias para iniciar las pruebas y establecer las trazas para capturar la señalización correspondiente. Se configuraron las variables de monitoreo a tener en consideración durante la evaluación, en cuanto a comportamiento del servicio, licencias requeridas, porcentaje de uso del CPU del *Softswitch*, RAM y tráfico de red. Las pruebas propuestas se ejecutaron en su totalidad aproximadamente en tres (3) semanas.

El protocolo de pruebas para la plataforma IMS, fue dividido en seis (6) grupos dependiendo del área a la que estaban enfocadas; el primer grupo de pruebas lo conformaban las correspondientes a pruebas de funcionamiento básico de VoIP e interoperabilidad con la plataforma NGN, entre las cuales se pueden nombrar cursar llamadas utilizando diferentes códec de voz (G.711u, G.711a, G.723, G.726, G.729a), llamadas con y sin autenticación contra el *CSCF*, intento de llamadas entre un usuario NGN y un usuario IMS (interoperabilidad). Para el primer grupo de evaluaciones se utilizó un dispositivo de tráfico de llamadas conocido como *SmartClass TPS* (*Triple Play Services*), con el cual se generaron reportes, verificando parámetros de calidad de servicio de las llamadas y capturando los paquetes correspondientes a la señalización.

El segundo grupo de pruebas estaba enfocado a fraudes y vulnerabilidades, como el intento de llamadas entre dos abonados SIP con la misma identidad (duplicidad), intento de suplantación de identidad (*spoofing*) a través de su dirección IP, intento de llamadas con modificación de IMPI/IMPU (*IP Multimedia Identity*) usando el protocolo Diameter; el segundo grupo de pruebas se ejecutaron con dos (2) herramientas: la primera es una herramienta de tráfico SIP según el RFC 4475, y un instrumento de pruebas, generador de trafico que maneja múltiples protocolos (H.248, Diameter), orientado principalmente a pruebas sobre redes IMS.

Para el siguiente grupo de pruebas, se validaron aspectos de seguridad y cifrado en la señalización y el flujo RTP (voz), conteniendo diferentes tipos de pruebas entre las cuales se encuentran validar encriptación de la carga útil (*payload*), modificación de parámetros de cabecera de los mensajes INVITE SIP (longitud, IP origen, IP destino, números origen y destino, etc.) verificando protección del *P-CSCF* frente a la inundación TCP/UDP de paquetes malformados; para este grupo de pruebas se utilizó un software de tráfico de paquetes para el descubrimiento de dispositivos SIP, según el RFC 3261.

El cuarto grupo englobó todo lo relacionado a ataques de negación/degradación de servicios, incluyendo pruebas como generación de flujo de llamadas a números no existentes y números incompletos, para elementos SIP y H.248, determinar rendimiento del *P-CSCF* y ataques de señalización SIP contra nodos de acceso; para este grupo se utilizó una herramienta *Exploit Toolkit* para la generación de llamadas bajo el protocolo SIP, según el RFC 2833.

El siguiente grupo corresponde a las pruebas de rendimiento, como verificar porcentaje o nivel de procesamiento del *P-CSCF* frente al envío de múltiples solicitudes de mensajes SIP (INVITE, REGISTER, etc.), simulando tráfico de llamadas en hora pico o BHCA (*Busy Hour Call Attempts*); se llevaron a cabo las pruebas con un instrumento de pruebas, generador de trafico que maneja múltiples protocolos (H.248, Diameter), orientado principalmente a pruebas sobre redes IMS y una herramienta de trafico de solicitudes SIP, según el RFC 2833.

El último grupo de pruebas estaba conformado por otras funcionalidades de la plataforma IMS, como el manejo de CAC (*Call Admitance Control*), autenticación e integración de elementos no Huawei (tanto elementos de control de señalización y gestión de seguridad), evitar generación de CDR (*Call Detail Record*) por un abonado o grupo de abonados, manejo de listas negra/blanca y gestión de bloqueos de usuarios fraudulentos.

Se realizaron varias entregas del protocolo con el tutor y se elaboró el documento definitivo. Se elaboró el escenario de pruebas basado en la red IMS ubicada en el laboratorio de CANTV y su conexión con la plataforma NGN. El escenario de pruebas, para la evaluación de la plataforma IMS se presenta en la figura 26:

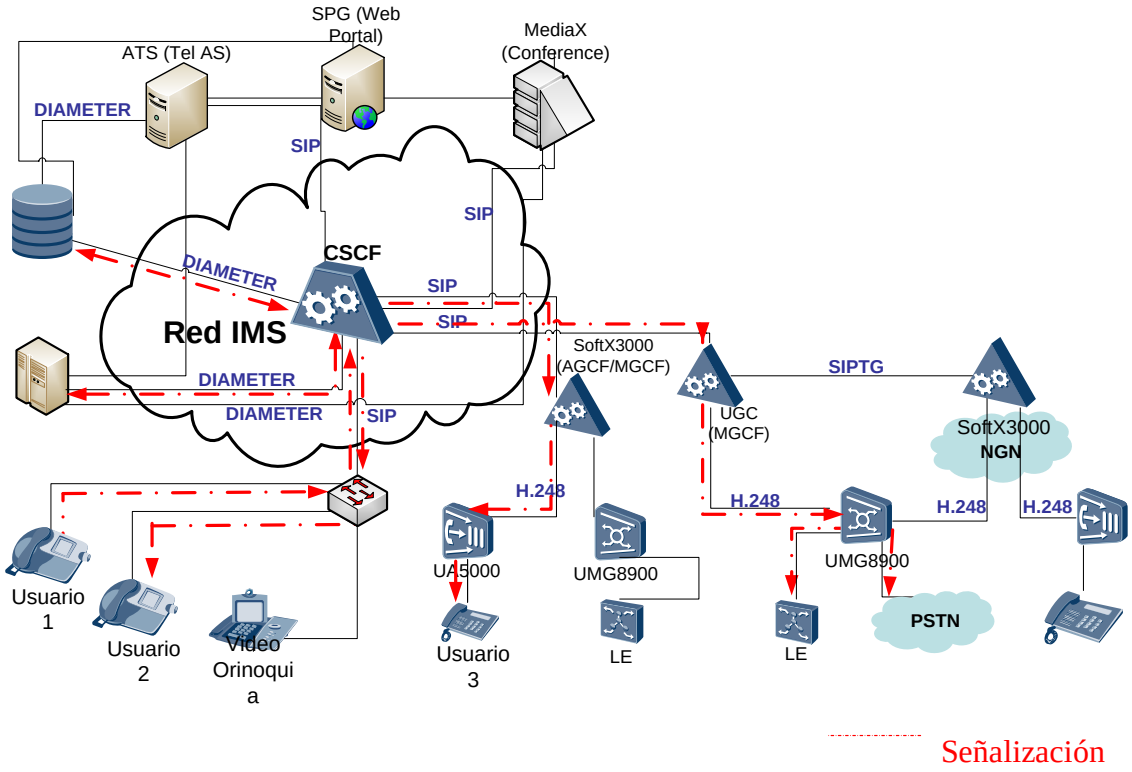


Figura 26: Escenario de pruebas red IMS y NGN laboratorio de CANTV.

Fuente: [Elaboración propia].

IV.4 Matrices de Severidad de Riesgos y Modelo de Seguridad

En base a las pruebas realizadas donde fueron empleados los protocolos de pruebas para las plataformas NGN e IMS de CANTV, se detectaron y documentaron los riesgos más importantes que afectan o afectarán ambas plataformas. Se procedió a elaborar dos (2) matrices de severidad de riesgos, una para cada plataforma, que contienen los riesgos detectados producto del estudio previo de ambas plataformas, como también de la ejecución de los protocolos de evaluación y de las entrevistas realizadas a personal de la empresa experto en el tema. Cada una de las matrices de severidad contiene una matriz de riesgo inherente, una matriz de riesgo controlado y una matriz de riesgo tratado. La matriz de riesgo inherente contiene la evaluación de las vulnerabilidades y riesgos inherentes sin controles que tiene cada plataforma, la matriz de riesgo controlado va referida a los riesgos y vulnerabilidades tomando en

cuenta los controles existentes para mitigar dichos riesgos, y finalmente la matriz de riesgo tratado se refiere a la evaluación de las vulnerabilidades teniendo planes de acción y medidas de mitigación. Además estas matrices contienen los diagramas de calor, dependiendo de su severidad, para cada uno de los riesgos detectados según la consecuencia que acarrean y la probabilidad de ocurrencia de las mismas. Dichos diagramas facilitan la comparación de la severidad entre los distintos riesgos, detectándose fácilmente cuales son los de mayor probabilidad de ocurrencia y mayor consecuencia.

Para la ponderación de la consecuencia se toman en cuenta ciertos criterios establecidos por la empresa, cada uno de estos criterios tienen asignado un campo según su grado de afectación. La ponderación consiste en asignarle un valor del uno (1) al cinco (5) a cada uno de los criterios, esto para indicar el grado de afectación de de cada riesgo, siendo uno (1) grado de afectación insignificante y cinco (5) grado de afectación catastrófico. Para cada criterio se encuentra definido lo que representa cada grado del uno (1) al cinco (5). Dichos criterios son: clientes, financiero, duración (acción requerida), calidad de servicio, importancia estratégica, elementos de red, imagen corporativa, complejidad y posibilidad. Los cuales serán definidos a continuación:

- **Clientes:** este criterio se refiere al grado de afectación del cliente de acuerdo al riesgo presentado. Los valores van desde 1-"Baja cantidad de reclamos de los clientes" hasta 5- "Pérdida de clientes a gran escala".
- **Financiero:** este criterio va referido al nivel de pérdidas de ingresos que podría generarse de acuerdo a los riesgos. Los valores van desde 1- "Posible pérdida de ingresos" a 5- "Pérdida de ingresos a gran escala".
- **Duración (acción requerida):** este criterio se refiere al tipo de acción que es requerida para la mitigación de los riesgos presentados, en cuanto al tiempo en que debe ejecutar dicha acción. Los valores van desde 1- "Acción a muy largo plazo" hasta 5- "Acción inmediata".

- **Calidad de Servicio:** el siguiente criterio especifica el grado de afectación del servicio para los riesgos presentados. Los valores van desde 1- "No afecta el servicio" hasta "Negación total del servicio".
- **Importancia Estratégica:** este criterio indica el grado de importancia estratégica para la corporación del riesgo presentado. Los valores van desde 1- "Importancia muy baja" hasta 5- "Muy importante".
- **Elementos de red:** el presente criterio va referido al grado de afectación de los elementos de red. Los valores van desde 1- "Posible pérdida de elementos" a 5- "Pérdida de elementos de red a gran escala".
- **Imagen Corporativa:** este criterio se refiere al grado de afectación del riesgo sobre la imagen corporativa. Los valores van desde 1- "No Afecta la imagen" a 5- "Gran afectación de la imagen".
- **Complejidad:** el siguiente criterio va referido al grado de dificultad para conseguir la solución del riesgo. Los valores van desde 1-"Muy simple" a 5- "Muy complejo".

Así como existen los criterios de consecuencia, también son definidos los criterios de probabilidad, en esta ocasión solo fue utilizado el criterio de posibilidad:

- **Posibilidad:** este criterio representa la posibilidad de que se materialice el riesgo. Los valores van desde 1-"Prácticamente imposible que ocurra" a 5- "Ocurre en todas las veces".

Una vez asignada la ponderación a cada criterio se calcula el valor promedio de todos los criterios de consecuencia, para obtener un valor total de consecuencia. Luego con el valor total de consecuencia y con el valor de probabilidad, se procede a calcular el nivel de severidad de cada riesgo, dicho nivel puede ser extremo, alto, moderado o bajo. Los diferentes niveles de severidad que pueden tener los riesgos son descritos a continuación:

- **Extremo:** se requiere acción inmediata y tratamiento tipo contingencia.
- **Alto:** se requiere atención de la Gerencia General y Gerencias propietarias del riesgo con planes de acción a corto plazo.

- **Moderado:** se debe especificar responsables de la gestión con planes de acción a mediano y largo plazo.
- **Bajo:** se administra con procedimientos de rutina.

Además, en las matrices correspondientes a cada plataforma, se encuentran definidas brevemente cada una de las vulnerabilidades o riesgos indicando datos relevantes de cada uno de ellos, también indicando las acciones a ejecutar o medidas de mitigación recomendadas para cada uno de los riesgos. Tanto los criterios de consecuencia como los criterios de probabilidad y niveles de severidad fueron previamente definidos por la empresa. Las matrices de severidad se pueden encontrar en la sección VII, correspondiente a Apéndices o Anexos.

Una vez completadas las matrices de severidad, se procedió a analizar los resultados obtenidos, ya que proporcionan una idea general de la orientación, limitaciones y alcances del modelo de seguridad IMS para el aseguramiento de la plataforma y los servicios ofrecidos a los usuarios finales. Seguido a esto se continuó con el diseño del modelo de seguridad, donde se determinaron las estrategias a seguir, basadas en los puntos débiles identificados de las plataformas.

Para el planteamiento del modelo, una vez elaboradas las matrices de severidad, se procedió a elaborar una arquitectura conceptual, así como la descripción técnica de la arquitectura de red del modelo, que incluye esquema de conectividad físico y lógico de la plataforma. Se determinaron capacidades de la capa de transporte de la actual arquitectura NGN ya que en caso de implementar en un futuro la tecnología IMS, es necesario conocer si es capaz de soportar la gran demanda de clientes con servicios que requieren una calidad de servicio considerable. Se determinaron especificaciones técnicas de la plataforma, al igual que de los equipos necesarios para darle robustez al modelo de seguridad. Los riesgos detectados, la arquitectura conceptual y especificaciones técnicas de la plataforma, y el planteamiento del modelo, se pueden observar en el Capitulo V, que corresponde a la sección de Resultados.

Capítulo V
Resultados

V.1 Análisis de los Resultados de la Investigación y Evaluación de las Plataformas NGN e IMS

La correcta realización de las pruebas fue un factor determinante para la detección de fallas y riesgos en la actual plataforma NGN de CANTV. Una acertada identificación de riesgos trae como consecuencia una adecuada selección de mecanismos de prevención, detección y corrección. Esto se resume en un documento que contenga la arquitectura conceptual, especificaciones técnicas, riesgos, diagnósticos, diagramas y soluciones tentativas, para una posible implementación de la tecnología IMS o servir de guía para la elaboración de distintos proyectos a futuro en CANTV. Dentro del marco de esta protección y en base a los resultados obtenidos en las pruebas, la investigación, conocimientos adquiridos de las visitas con diferentes personalidades de CANTV, el análisis de la plataforma NGN y la plataforma IMS en laboratorio de CANTV, se han identificado los riesgos más importantes requiriendo de mecanismos de seguridad robustos.

La incorporación de una nueva tecnología que presenta mayor innovación a lo presente actualmente, requiere estudio y entendimiento, así como determinar fortalezas y debilidades. Para el caso de IMS, es precisamente esta situación, y para CANTV en caso de surgir como proyecto y su posterior implementación, es fundamental garantizar su operación, calidad del servicio y fórmula de negocio. La actual red NGN, se puede considerar una plataforma 'Pre-IMS', ya que el 70% de la actual plataforma maneja la información de control y media (data) en paquetes. En caso de adoptar este conjunto de especificaciones nuevas es necesario integrar la actual plataforma NGN con la nueva IMS, para soportar la telefonía, tanto móvil como fija, y los servicios multimedia a través de IP. En la siguiente figura se puede

observar un esquema de la interconexión de la actual red NGN e IMS en caso de una eventual implementación, solamente ilustrativa:

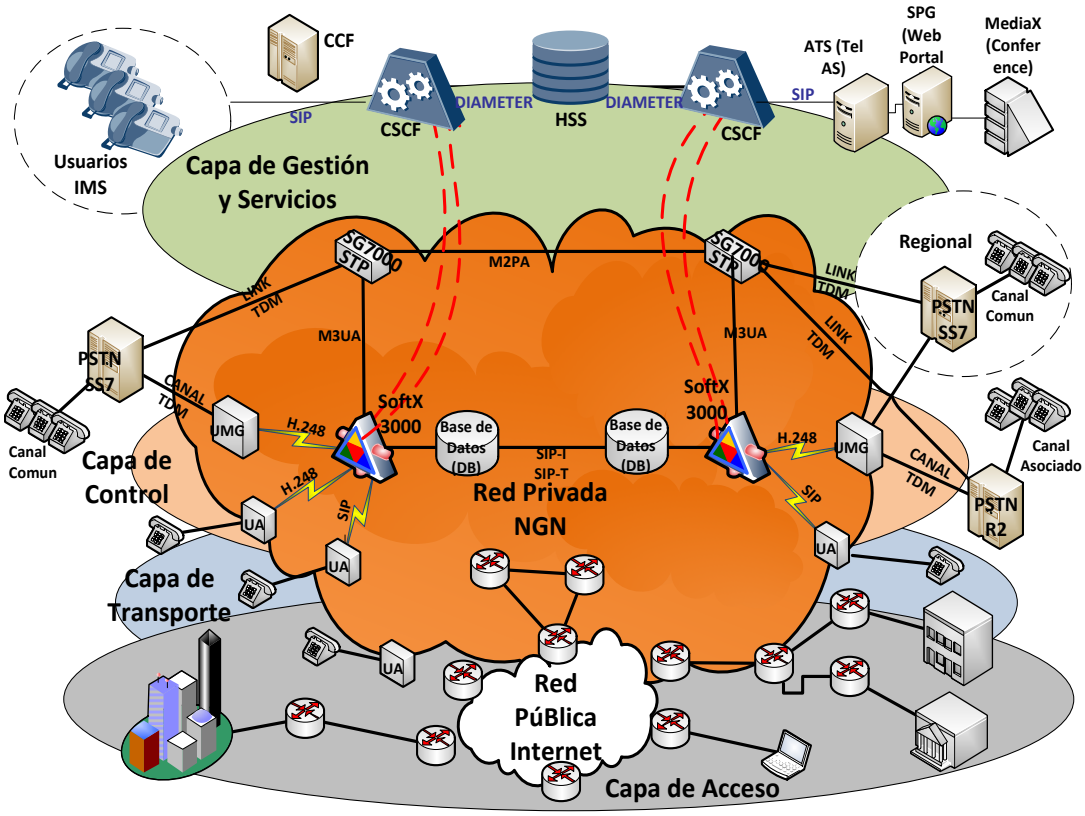


Figura 27: Implementación tecnología IMS sobre la plataforma NGN de CANTV.
Fuente: [Elaboración propia].

En la figura 27, se puede apreciar la interconexión de la plataforma NGN con la red IMS. A primera instancia, se puede llegar a pensar en desechar por completo la red actual NGN y migrar todo hacia una nueva tecnología como IMS, sin embargo, es obvio que es una pérdida de recursos y dinero, dado que es preferible el aprovechamiento de la infraestructura actual para abaratar costos, y es así como CANTV está utilizando sus centrales digitales para conectarlas a la red NGN, proceso que denominan paquetización, para contar con todos los elementos en una plataforma unificada. Es importante tener en cuenta que la red IMS se ubicaría en la capa superior a la actual red NGN, pasando los elementos actuales NGN al control de la nueva capa IMS. Dado que IMS es una tecnología para la convergencia de la

telefonía móvil con la fija y brindar servicios de calidad a sus clientes, es normal y fundamental que esta se encuentre en una capa superior.

En la red privada NGN de CANTV, el paquete H.248 es transportado sobre el protocolo UDP (*Unit Datagram Protocol*), ya que al ser un protocolo no orientado a conexión, las velocidades de transmisión de los paquetes son muy rápidas y no se utilizan tantos recursos de la red de transporte, quedando la seguridad en el envío y recepción de los paquetes por las características de ser una red privada, ya que no cuenta con ningún tipo de encriptación. La debilidad más resaltante detectada se determinó cuando un usuario usando el protocolo H.248, intenta realizar una llamada a otro usuario cualquiera. La comunicación puede establecerse, pero la vulnerabilidad se detecta ya que actualmente los usuarios H.248 no poseen ningún tipo de autenticación originando un riesgo de seguridad. Se determinó este riesgo entre los elementos de control de la red NGN, y los elementos de acceso a la red. En este sentido, la situación ocurre debido a que existen equipos que se encuentran lógicamente conectados directamente a la capa de control de NGN sin autenticación, como por ejemplo: el dispositivo UA5000; Por lo que pueden presentarse situaciones de fraude a través de suplantación de identidad. Lo descrito anteriormente se ilustra en la figura 28:

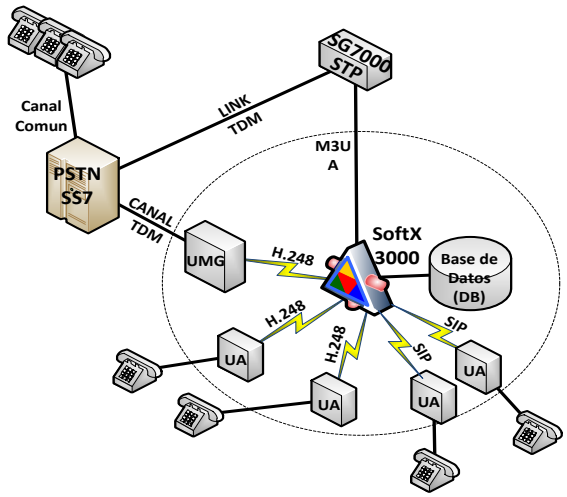


Figura 28: Red Privada CANTV (sin redundancia).

Fuente: [Elaboración propia].

La problemática se presenta como asegurar los equipos en entornos privados que se suponen seguros, sin embargo, están sujetos a ataques internos. Por ejemplo, una persona interna a CANTV, conocedor de políticas de seguridad de la empresa, puede tener acceso a la gestión de cualquier dispositivo de la red interna o realizar llamadas no autorizadas sin facturación. El mayor de los riesgos a nivel de seguridad de la actual plataforma se observa en el hecho de que las credenciales H.248 no se encuentran activas, por lo que no se manejan protocolos de autenticación, facilitando técnicas de fraude interno. La única protección que posee la capa de control de la red NGN radica en el hecho de ser una red privada, con *Firewalls*, *Proxys* y otros dispositivos de seguridad que bloqueen usuarios no autorizados de redes externas. El problema es que los *Firewalls* y *Proxys*, filtran paquetes y puertos, segmentando la red y protegiéndola contra entes externos gestionando bloqueos basados en direcciones IP. El problema surge cuando un individuo en la red interna de gestión, que conozca direcciones IP de los dispositivos de la plataforma, realice un ataque falsificando una dirección IP e intente obtener recursos, servicios, cuentas de usuario de la base de datos del *Softswitch*, atacar algún dispositivo para colapsar la red (DoS/DDoS), o algún otro fin malicioso.

Otra vulnerabilidad detectada fue la ausencia de protocolos de validación AAA (*Authentication, Authorization and Accounting*) de elementos de capa de control de la plataforma NGN como el SoftX3000, el UMG8900, el SG7000, UA5000, entre otros elementos. Este riesgo de seguridad es considerable ya que puede ocasionar una manipulación no autorizada en la gestión de los elementos, u obtener recursos sin autorización, estableciendo múltiples llamadas sin facturación. Es necesaria la automatización del manejo de protocolos AAA para todos los dispositivos de la capa de control y acceso. Otro factor detectado en las evaluaciones de la plataforma NGN, fue la ausencia de manejo de algunos códec por parte del *Softswitch*, lo que trae como consecuencia que la llamada no pueda establecerse y el *Softswitch* consumirá recursos intentando decodificar los paquetes para el establecimiento de la comunicación,

utilizando procesamiento del CPU y quedando expuesto a ataques como una inundación de paquetes TCP/UDP.

La capacidad de usurpación de identidad (duplicidad) de un usuario registrado en la base de datos del *Softswitch*, para intentar desviar recursos y establecer llamadas es posible, ya que la autenticación de los usuarios se puede realizar de tres (3) formas: dirección lógica (IP) del usuario, *login/password* del usuario o utilizando ambas, la dirección lógica y el *login/password* del usuario. La debilidad en la plataforma se encuentra cuando un usuario facilita su cuenta y clave a otro usuario, o el segundo usuario utilizando algún método malicioso adquiere la cuenta del usuario legítimo, y a su vez este conoce el rango de direcciones IP permitidas para obtener recursos de la red. El *Softswitch* responde todas las solicitudes entrantes, sean usuarios registrados o no, consumiendo recursos de procesamiento innecesariamente, no cuenta ni con un mecanismo de defensa para descartar los paquetes de forma automatizada ni con un dispositivo de borde y control que proteja la capa de control.

Validación de elementos de acceso por *login/password*, sin proporcionar contraseña al usuario. Es necesario contar con un mecanismo de protección, teniendo la contraseña cazada con el dispositivo para un determinado servicio. De esta forma no se utilizan innecesariamente recursos de procesamiento, ya que actualmente la plataforma proporciona una dirección IP al usuario y luego verifica el ID (*Identification*) del usuario. La falta de un mecanismo de generación de claves automatizado e integrado al dispositivo, puede permitir fraudes de suplantación de identidad debido a que las claves son conocidas tanto por el usuario como por el personal de la empresa.

Se detectó otra debilidad como resultado de las evaluaciones sobre la plataforma NGN, como la ausencia de cifrado de la información por parte de los equipos UA5000, debido a que estos equipos sólo manejan el protocolo Telnet, que es un protocolo de acceso remoto inseguro, ya que las claves de los usuarios viajan sin

ningún tipo de cifrado (señalización plana), pudiendo ser usurpada información importante de los usuarios. El *Softswitch* no maneja protocolos de cifrado para el transporte seguro de la información como TLS (*Transport Layer Security*), solamente maneja IPsec (*IP Security*).

En la ejecución de la prueba descubrimiento de dispositivos SIP, se detectó un riesgo crítico ya que el *Softswitch* y otros elementos de la red NGN, no se identifican como elementos de control de la red, pero proporcionan su dirección IP al inundar la red de paquetes maliciosos, quedando vulnerable a ataques o intentos de fraude por elementos internos a la red. En la figura 29 se puede observar una captura de pantalla de los resultados obtenidos en la prueba:

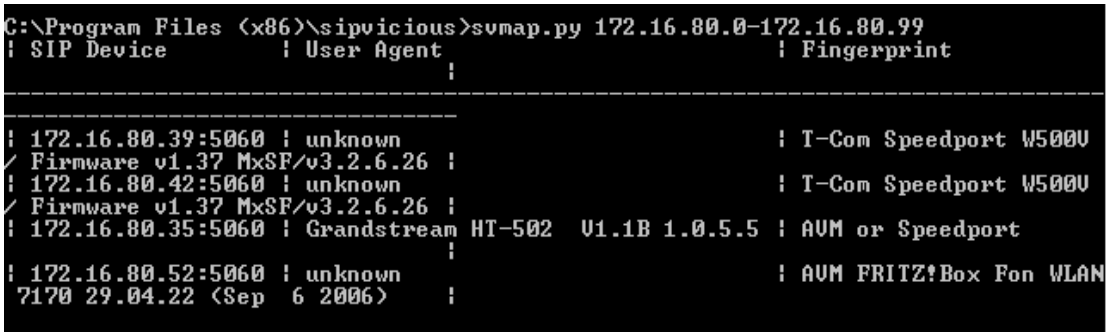


Figura 29: Captura descubrimiento de dispositivos (Protocolo SIP).

Fuente: [Elaboración propia].

Para la prueba de rendimiento del *Softswitch* frente al envío de múltiples solicitudes de mensajes SIP (INVITE, REGISTER) se observó una vulnerabilidad, ya que el dispositivo deja de enviar respuestas a las solicitudes recibidas. Aproximadamente el dispositivo colapsa con 400 solicitudes por segundo, dejando la red vulnerable. Actualmente el *Softswitch* no cuenta con un dispositivo que brinde protección y sirva de soporte para el procesamiento de solicitudes, por lo que el modelo se incluirá una solución para mitigar este riesgo. En la figura 30 se puede observar el resultado de la prueba:

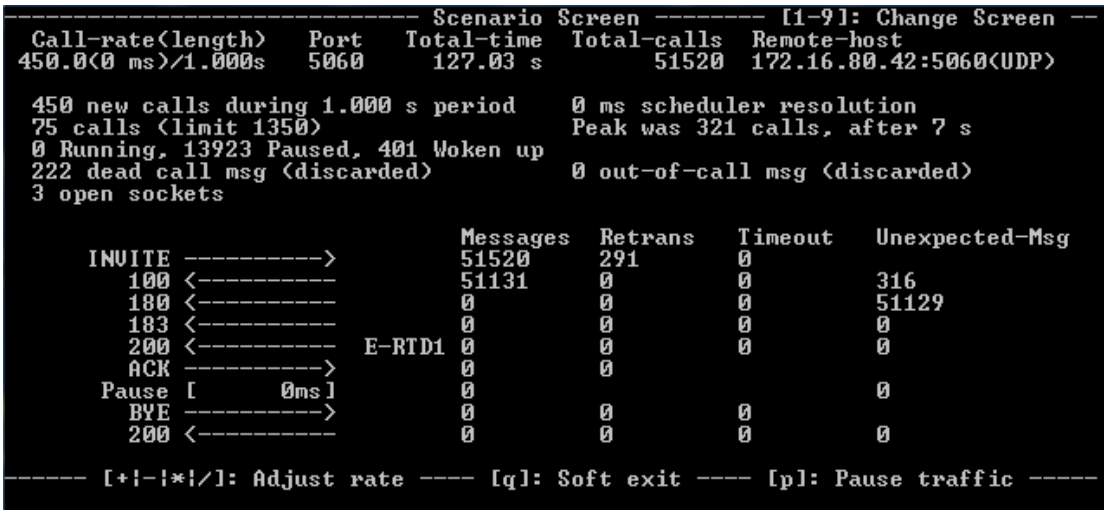


Figura 30: Captura prueba rendimiento SoftX3000.

Fuente: [Elaboración propia].

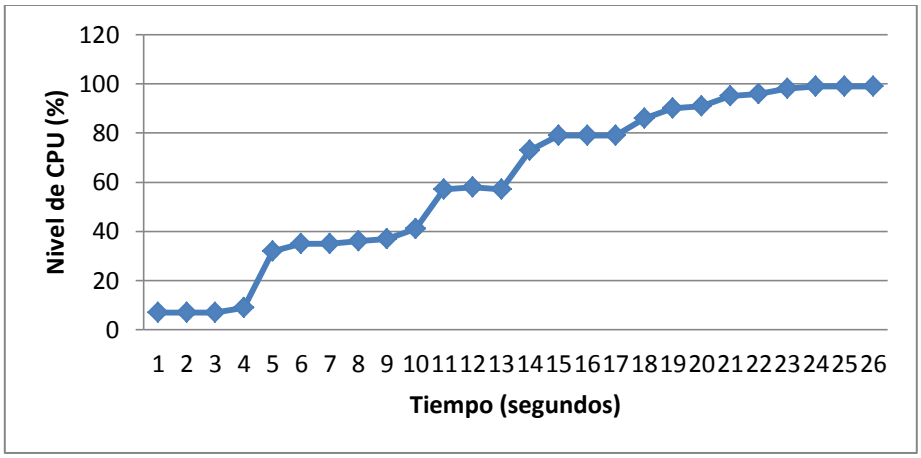


Figura 31: Prueba rendimiento (rampa) plataforma NGN.

Fuente: [Elaboración propia].

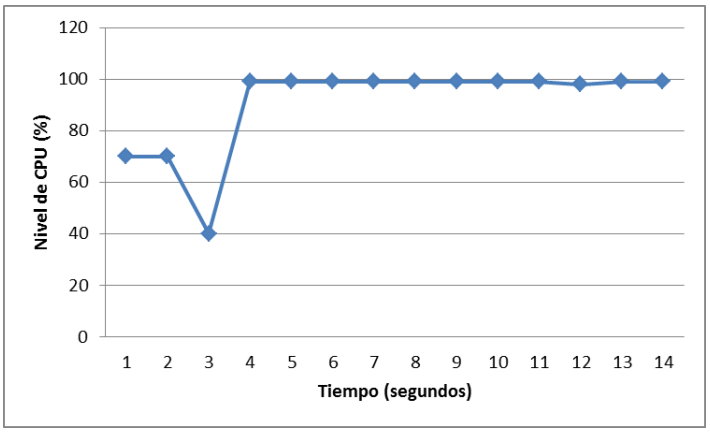


Figura 32: Prueba rendimiento (disparo) plataforma NGN.

Fuente: [Elaboración propia].

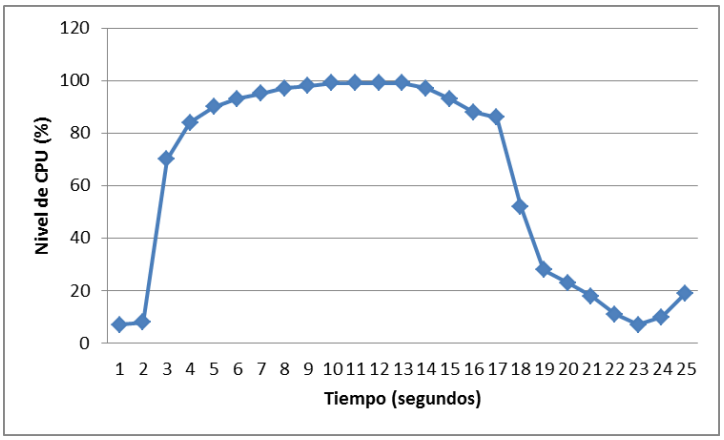


Figura 33: Prueba rendimiento (hora pico, BHCA) plataforma NGN.

Fuente: [Elaboración propia].

La ausencia o falta de un sistema alterno automatizado de notificación y detección de fallas. Actualmente CANTV cuenta con un gestor que emite alarmas en caso de cualquier falla, debido al colapso de algún dispositivo o falla en la red de transporte, pero no proporciona la causa de la falla. Es necesario un mecanismo de seguridad en la prevención y detección de las fallas que garantice la continuidad del servicio. Esta vulnerabilidad puede estar intrínsecamente relacionada a la incapacidad de integración de elementos de proveedores distintos a Huawei, para la gestión de seguridad de la red, lo que genera grandes limitaciones en sistemas integrales de

seguridad aplicables a la red. Es permitida la integración de elementos de otros proveedores a nivel de capa de control de la red.

Los aspectos identificados de seguridad en la actual plataforma NGN, están relacionados a la falta de segmentación de la red a través de un dispositivo de control que sea capaz de gestionar la seguridad. Las capas de seguridad, control y servicios se encuentran en el mismo nivel lógico, por lo cual la seguridad se puede ver comprometida ya que en caso de existir una intrusión por un elemento fraudulento, pueden verse afectadas todas las capas. La incapacidad de bloqueos automatizados de usuarios con comportamientos irregulares (como número de llamadas, numerosas llamadas internacionales, múltiples intentos de servicios especiales, etc.), por parte del *Softswitch* u otro elemento de control, lo que genera consumo de recursos al procesar las solicitudes.

Otra vulnerabilidad importante encontrada en la plataforma NGN, radica en la falta de una base de datos centralizada. En el presente, no existe una base de datos que contenga la información de las cuentas de usuarios y los servicios que poseen cada uno de ellos, mediante la cual se realice la autenticación de los usuarios. Cada pareja de *Softswitch* (activo/pasivo) posee su propia base de datos con el contenido de los usuarios asignados a administrar por cada *Softswitch*, por lo que la seguridad debe ser más minuciosa y las probabilidades de fraudes aumentan, ya que es necesario el control de mayor número de bases de datos. Con la tecnología IMS se mitiga este riesgo, ya que solamente existe una base de datos conocida como HSS (*Home Subscriber Server*) capaz de almacenar gran cantidad de usuarios detallando los servicios a los que pueden acceder cada uno de ellos.

Las vulnerabilidades detectadas en la evaluación de la plataforma NGN son fundamentales ya que serán heredadas por IMS en caso de una posible implementación en CANTV. En la evaluación de la plataforma IMS se detectaron varios riesgos a nivel de seguridad de importancia. En la ejecución de una prueba, se

realizaron llamadas con y sin autenticación, detectando que actualmente no existe un sistema de autenticación que verifique inequívocamente el usuario legítimo, permitiendo el registro de dos usuarios distintos acceder a los servicios de una misma cuenta registrada en el HSS, negando el servicio del usuario legítimo. El mecanismo de mitigación de esta brecha, seria la segmentación de la red permitiendo autenticación de los usuarios por un rango de direcciones lógicas (IP), validando cuenta y contraseña (*login/password*), verificando la identidad del usuario evitando de esta forma posibles ataques de negación o degradación de los servicios.

En la realización de la prueba rendimiento del CSC3300 frente al ataque de múltiples solicitudes INVITE utilizando protocolos TCP/UDP, se detectó una falla del dispositivo P-CSCF, ya que el equipo respondía todas las solicitudes entrantes, llegando a colapsar dejando vulnerable la red privada de la plataforma IMS. El P-CSCF responde todos los mensajes que llegan, válidos o no. El P-CSCF colapsa alrededor de las 2000 solicitudes por segundo, a diferencia del *Softswitch*, que a partir de las 450 solicitudes por segundo el dispositivo comienza a descartar paquetes, colapsando y negando las solicitudes para el establecimiento de nuevas llamadas (negación/degradación del servicio). En la figura 34 se puede observar el rendimiento del P-CSCF frente a la inundación de paquetes TCP/UDP:

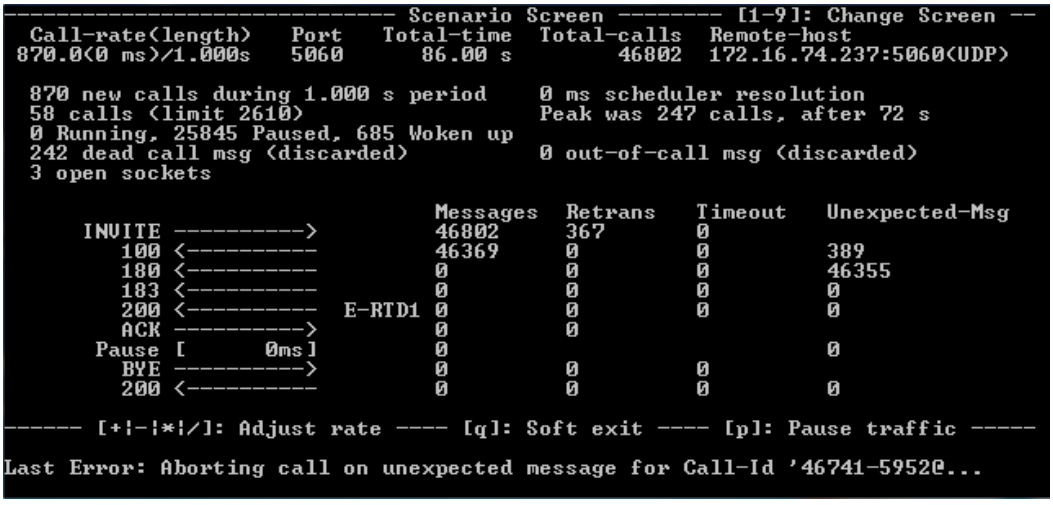


Figura 34: Captura prueba rendimiento P-CSCF. Plataforma IMS.

Fuente: [Elaboración propia].

A continuación, en la figura 35 se observan los resultados obtenidos en la ejecución de la evaluación de rendimiento del CSC3300 modelando un tráfico de llamadas tipo rampa:

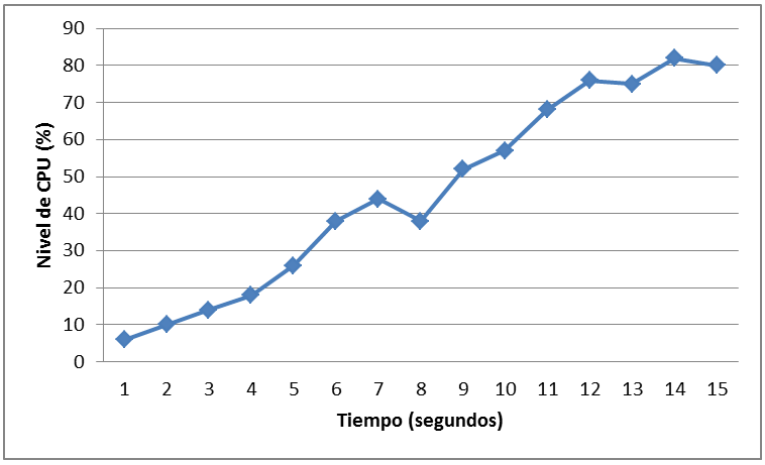


Figura 35: Prueba de rendimiento (rampa) plataforma IMS.

Fuente: [Elaboración propia].

A continuación, en la figura 36 se observa el porcentaje de uso de CPU durante la ejecución de la evaluación de rendimiento modelando un tráfico de llamadas tipo disparo:

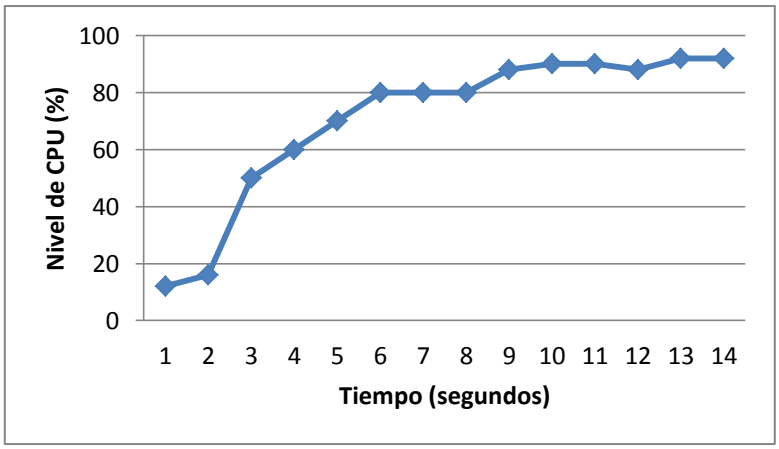


Figura 36: Prueba de rendimiento (disparo) plataforma IMS.

Fuente: [Elaboración propia].

Otra vulnerabilidad detectada en las evaluaciones de la plataforma IMS, fue la capacidad de detectar paquetes provenientes de la señalización previa al establecimiento de una llamada cualquiera, ataque MitM (*Man in the Middle*). Al modificar direcciones IP para intentar redireccionar los paquetes, el P-CSCF rechazaba los paquetes protegiendo la red frente al ataque en curso. Los mensajes estaban encriptados, resultando más difícil descifrar la información contenida en los paquetes. La falta de manejo de varios códec por parte del CSCF, puede ser interpretado como una vulnerabilidad, ya que el P-CSCF agota recursos intentado codificar/decodificar la información con un códec que no es soportado por el dispositivo, malgastando procesamiento del equipo.

Para la prueba descubrimiento de dispositivos bajo el protocolo SIP, se observó que el P-CSCF no se identifica como un equipo de control y seguridad, pero proporciona su dirección lógica (IP) quedando vulnerable frente a un ataque de degradación o negación del servicio. En la figura 37 se pueden observar los resultados obtenidos para esta evaluación:

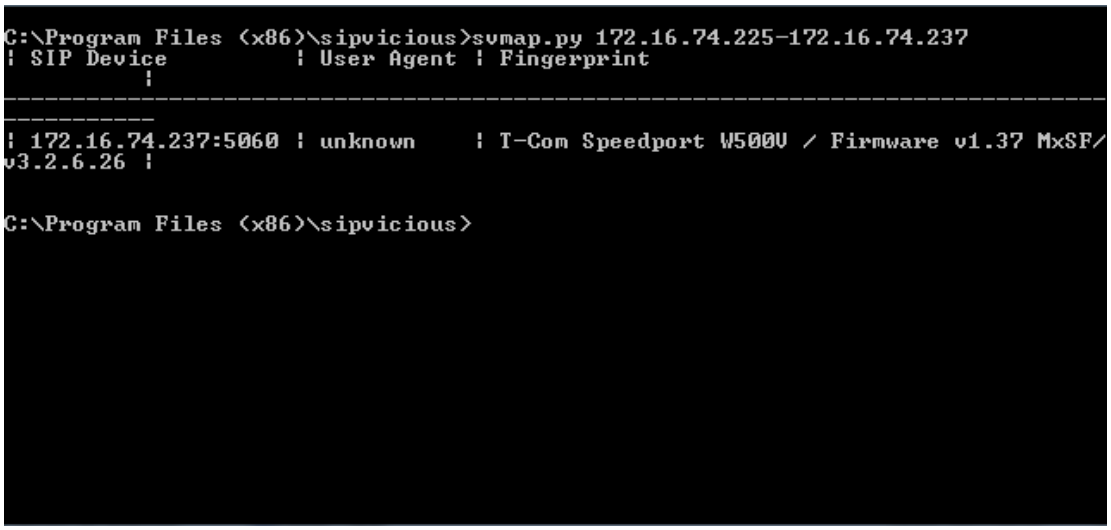


Figura 37: Captura prueba descubrimiento SIP. Plataforma IMS.

Fuente: [Elaboración propia].

Como se pudo observar en los resultados obtenidos de las evaluaciones sobre las plataformas NGN e IMS de CANTV, existen numerosos riesgos de seguridad a nivel

de capa de control que son necesarios mitigar para evitar la falla de los servicios y comprometer la calidad del servicio ofrecido a los usuarios. Comparando ambas plataformas, salta a la vista las mejoras sustanciales de la implementación de IMS ya que mejora en muchos aspectos la actual plataforma NGN, como por ejemplo cuenta con un dispositivo controlador (P-CSCF) que protege el CSCF frente a cualquier ataque, en NGN existen abonados conectados a través de los UA5000 directamente al *Softswitch* siendo el escenario perfecto para un fraude interno; IMS ofrece el concepto del HSS como base de datos centralizada para tener mayor control sobre la información de importancia y brindar robustez a la plataforma, ausencia de un sistema (servidor) automatizado generador de claves de seguridad (NGN), la falta en la plataforma NGN de autenticación de usuarios multimedia, entre otros riesgos.

A continuación se presenta un resumen de los riesgos y vulnerabilidades encontrados tanto en la plataforma NGN como en la de IMS.
Para la plataforma NGN se detectaron un total de 19 riesgos, distribuidos de la siguiente manera, indicando el porcentaje sobre 100% que representa cada grupo:

- 6 Riesgos a nivel de Acceso (31,58%)
- 3 Riesgos a nivel de Transporte (15,79%)
- 7 Riesgos referentes a Negación o Degradación de servicios (36,84%)
- 3 Riesgos en Gestión de Seguridad (15,79%)

Adicionalmente, para la plataforma IMS se detectaron un total de 9 riesgos, distribuidos de la siguiente manera, indicando el porcentaje sobre el 100% que representa cada grupo:

- 3 Riesgos a nivel de Acceso (33,33%)
- 1 Riesgo a nivel de Transporte (11,11%)
- 4 Riesgos referentes a Negación o Degradación de servicios (44,44%)
- 1 Riesgos en Gestión de Seguridad (11,11%)

V.2 Arquitectura Conceptual del Modelo de Seguridad IMS para el Aseguramiento de Plataforma Y Servicios

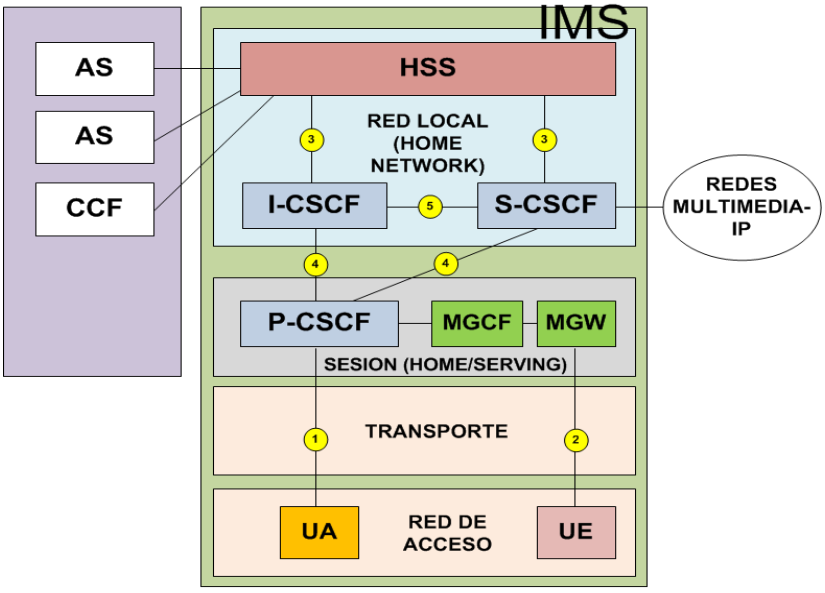


Figura 38: Arquitectura de seguridad IMS.
Fuente: (Wong, 2003)

En la figura 38, se ilustra configuración básica a nivel de seguridad, para la protección de la plataforma IMS. Para el flujo de señalización en esta red multiprotocolo, es indispensable determinar puntos críticos de seguridad para ubicar mecanismos robustos de prevención que eviten fraudes o riesgos que impacten el servicio. Existen cinco (5) mecanismos de protección, que se deben implementar al adoptar la tecnología IMS, que le dan protección y aseguran el servicio.

1. Es necesario establecer protocolos AAA (*Authentication, Authorization and Accounting*) entre el UE (*User Equipment*) y el S-CSCF, para el control de acceso de los usuarios a la red privada. El proceso de autenticación de los suscriptores corresponde al S-CSCF (*Serving-CSCF*), el usuario accede a la red con cualquier tecnología de acceso, a través del P-CSCF (*Proxy-CSCF*) y el I-CSCF (*Interrogating-CSCF*) valida la cuenta del usuario con el HSS

(*Home Suscriber Server*), que es el encargado de almacenar las cuentas de los suscriptores y generar las claves públicas para el acceso de los mismos a la red. Es necesario almacenar la clave asociada con el IMPU (*Public User Identities*) del usuario ya que es la que proporciona al usuario utilizar los servicios correspondientes y de esta forma identificar inequívocamente el usuario legítimo asociado a la cuenta.

2. La razón de utilizar un P-CSCF (*Proxy-CSCF*) es segmentar la red pública de la red privada, brindando un enlace seguro y una asociación de seguridad entre el UE y el P-CSCF para la protección de la red interna. Es necesario proporcionar autenticación de los datos de origen para corroborar identificación del usuario (punto de referencia Gm).

3. Es necesario proveer seguridad en el dominio de la red interna entre el HSS y el I-CSCF (*Interrogating-CSCF*), que es el encargado de obtener cuenta, credenciales y servicios para cada usuario a través del protocolo Diameter. Es necesario implementar todas las características de seguridad que ofrece el protocolo Diameter para brindar la protección necesaria.

4. Proporcionar seguridad entre los nodos centrales de control de la plataforma IMS (*I/P/S-CSCF*), a través del protocolo SIP. Es necesario blindar la comunicación entre estos tres (3) nodos, ya que es fundamental para la plataforma la confidencialidad de la información de control para el establecimiento, gestión y culminación de las sesiones de los usuarios. Se propone la utilización de un método de autenticación distinto al HTTP Digest (utilizado por SIP). Se pueden implementar protocolos AAA que blinden los dispositivos I-CSCF y S-CSCF, ya que en caso de colapsar el P-CSCF estos dispositivos quedan vulnerables a posibles ataques.

5. El I-CSCF es el encargado de obtener la IMPU del usuario que realiza la solicitud al HSS respectivo, para posteriormente asignar el S-CSCF correspondiente para el establecimiento de la sesión. Es necesario un nivel de seguridad robusto, ya que este punto proporciona la comunicación entre el P-CSCF y otras redes de servicios SIP, cuando el UE se encuentra operando en la HN (*Home Network*). La propuesta de seguridad sería implementar una capa de borde, que controle y gestione el acceso y operación de los UE en la capa de control, entre el P-CSCF y la capa de acceso de la red NGN.

Como ya se mencionó anteriormente, la actual red NGN de CANTV juega un papel fundamental en el advenimiento de la nueva tecnología IMS. Por ello, se evidencia que las debilidades o riesgos de la plataforma NGN pueden tener una estrecha relación con respecto a IMS, es decir, herencia de riesgos. Como complemento a las vulnerabilidades detectadas en las evaluaciones realizadas a las plataformas NGN e IMS, se realizó un estudio avanzado sobre las capacidades y especificaciones técnicas de equipos de la actual plataforma NGN (UA5000, SG7000, UMG8900, SOFTX3000).

El diagrama de bloques de la arquitectura conceptual del modelo de seguridad IMS se muestra en la figura 39:

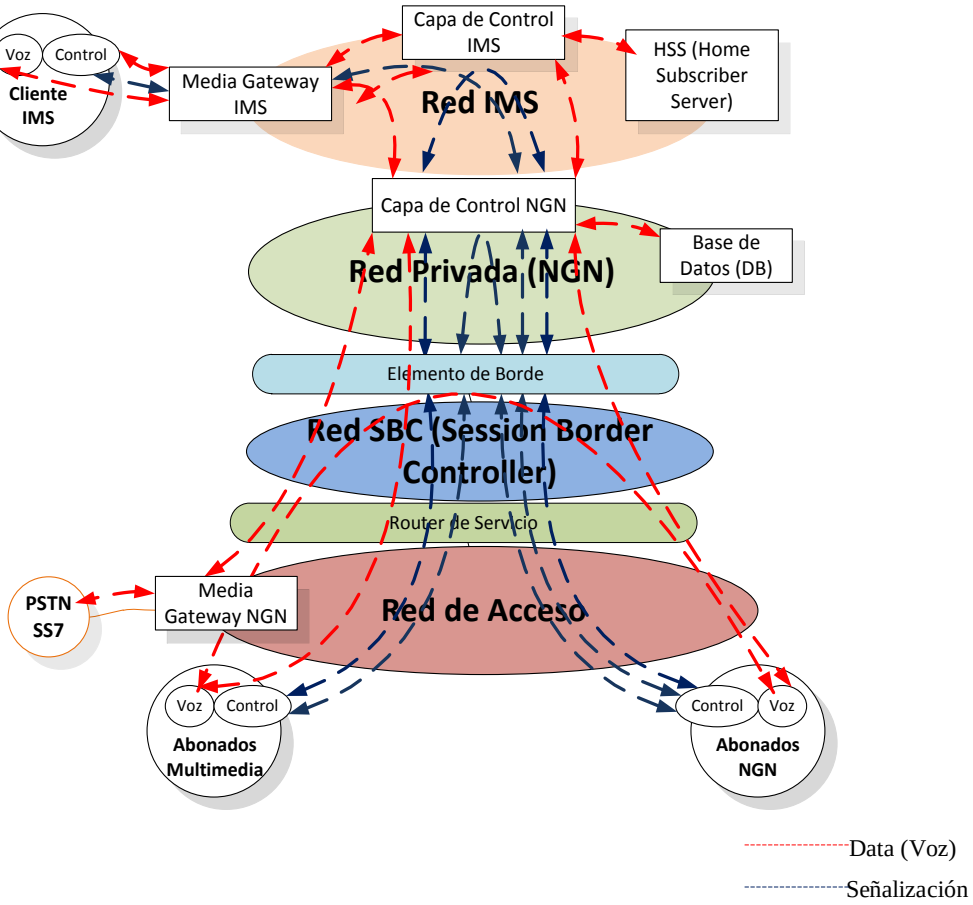


Figura 39: Diagrama de Bloques Arquitectura Modelo IMS.

Fuente: [Elaboración Propia].

Actualmente, en la red operativa los elementos NGN poseen direcciones IP de *backbone* para conectarse al *Softswitch*. Una persona interna de la compañía con el acceso correspondiente puede tener acceso a la gestión de estos dispositivos de la red interna o realizar llamadas no autorizadas sin facturación. La mayor brecha a nivel de seguridad de la actual plataforma se observa en el hecho de que las credenciales H.248 no se encuentran activas, por lo que no se manejan protocolos AAA (*Authentication, Authorization and Accounting*), facilitando técnicas de fraude 'interno'. La protección que posee la capa de control de la red NGN, radica en el hecho de ser una red privada, con elementos barrera como *Firewalls*, *Proxys* y otros dispositivos de seguridad que impiden el acceso a usuarios no autorizados. El

problema es que los *Firewalls* y *Proxys*, filtran paquetes y puertos, segmentando la red y la protegen contra entes externos, gestionando bloqueos basados únicamente en direcciones físicas (MAC) y lógicas (IP). En este sentido, es de gran importancia aplicar controles que aseguren la señalización, aspecto de gran importancia en redes del tipo NGN o IMS, permitiendo administrar y controlar el acceso a los elementos y uso del servicio. La autenticación de los elementos H.248 debe estar soportada por un sistema de autenticación automatizado.

Aquellos elementos que señalizan contra la capa de control NGN en protocolo SIP, presentan riesgos de seguridad al igual que los dispositivos que se comunican con protocolo H.248. Elementos de la capa de control de la red NGN no cuentan con un dispositivo que gestione y controle las conexiones de los usuarios y troncales SIP, quedando vulnerable a intentos de fraude o ataques de negación de servicios. Según el RFC 3261, elaborado por la IETF proponen ciertos mecanismos de seguridad para proporcionar robustez al protocolo. Existen dos mecanismos de seguridad: TLS (*Transport Layer Security*) y S/MIME, y se utilizan para dar carácter confidencial a la señalización y comprobar la identidad entre clientes y servidores. Como TLS no proporciona seguridad extremo a extremo, surge el protocolo S/MIME el cual se propuso para lograr un nivel de verificación de identidad de extremo a extremo, así como la confidencialidad de los datos. Existen numerosos problemas en la forma en que los teléfonos SIP manejan certificados de TLS. Si el *Softswitch* no verifica los certificados no tiene ningún sentido el uso de una sesión TLS, ya que el uso de claves es obsoleto porque no se comprueba la identidad del usuario. TLS demuestra la ruta segura de señalización hasta el servidor y S/MIME proporciona la seguridad extremo a extremo entre (dispositivos) y su señalización. Una vez establecido el canal seguro para la señalización, según el RFC 3329, se recomienda usar el protocolo RTCP (*Real-Time Control Protocol*) que ofrece una vía para la codificación del medio de transporte de datos en tiempo real, entre dos extremos. El problema es el intercambio de las claves de cifrado de forma segura, usando TLS, en la corriente de los medios de comunicación. Todos los servidores intermedios en la ruta de llamada tendrán

acceso a las claves de cifrado, representando un riesgo de seguridad para que un tercero obtenga la clave y decodifique la información.

El planteamiento de una capa de SBC (*Session Border Controller*) mitiga estas vulnerabilidades, estableciendo una capa de borde entre los dispositivos y la capa de control NGN, formando esto parte de la arquitectura lógica de seguridad que brinde protección a las capas de control NGN e IMS. La funcionalidad de la capa SBC es el manejo de toda la señalización para el establecimiento, gestión y control de las sesiones multimedia, blindando las capas de control de las plataformas. Los SBC mezclan seguridad de redes, procesamiento de solicitudes para el establecimiento de llamadas y transporte seguro, a través del control de segmentos IP. La capa SBC brindará diversas funciones como control de acceso para los usuarios, protección de la red contra virus y gusanos, funcionalidades NAT (*Network Address Translation*), manipulación de números telefónicos y de URIs (Uniform Resource), enrutamiento basado en calidad de los enlaces, entre otras funciones. Además esta capa de SBC mitiga problemas de ausencia de manejo de ciertos códec por parte del *Softswitch*, ya que posee esta funcionalidad. La función del SBC de *topology hiding* (ocultamiento de la topología) de la red NGN e IMS, es la que va a proporcionar protección interna a la red privada y la mitigación de ataques de negación o degradación de servicio (DoS).

La plataforma NGN permite una segmentación limitada de servicios, contrario a su sucesor IMS, el cual busca la convergencia y fácil manejo de los servicios y su aprovisionamiento. Sin embargo, dada la estructura jerárquica, sistemas de Tecnología de Información y de negocios de la red actual de CANTV, se dificulta proporcionar servicios específicos dependiendo de las necesidades de los usuarios, sin depender de otros. Esto ocasiona riesgos importantes de negocio, operativos y de seguridad. En este sentido, por ejemplo, puede existir consumo de recursos innecesarios, tendencia a la utilización de recursos de forma gratuita o fraude, aunque existen diversos mecanismos que permiten su detección. Normalmente, en redes de

datos con DSLAM/BRAS, donde no existe una integración de servicios y del acceso de forma segura, se pueden dar recursos al cliente (IP, QoS, etc.) sin una validación previa de su perfil como cliente en las plataformas, sin estar cazado a una identificación. De esta forma, es necesaria la implementación de mecanismos de seguridad y acceso que permitan la auditoría y control de recursos según perfiles de usuario, unificado para diversos servicios, por ejemplo '*Triple play'*. Para acceder a los servicios, se puede proporciona un mapa de códigos a los usuarios para su autenticación que garantice su identidad. Se debe garantizar la autenticación y cifrado en los elementos que señalicen H.248 contra la capa de control.

De igual forma es necesario contar con un dispositivo SBC para controlar el acceso y evitar robo de credenciales o algún otro tipo de fraude, así como garantizar la calidad de servicio y trazabilidad, protegiendo la capa de control de intentos maliciosos de obtención de información, servicios u ataques. La implementación de SBC corresponde con el hecho de proporcionar un elemento de borde en la misma red privada de operación, de CANTV, controlando el flujo tanto de señalización como de voz, para el establecimiento de las sesiones multimedia y protección de la información de ataques internos y fraude, evitando que la capa de control señalice con otros equipos directamente. La capa SBC proporcionaría, no sólo la seguridad necesaria para la protección de la red, sino que también mejoraría el desempeño del (*Softswitch*), aumentando su eficiencia y ahorrando procesamiento para las funciones que debe ejecutar.

Con la tecnología IMS se mitigan diversos riesgos identificados en la actual plataforma NGN de CANTV. Por ejemplo, por cada *Softswitch* existe una base de datos que almacena un grupo determinado de usuarios, mientras que IMS soluciona el problema de aprovisionamiento de los usuarios, ya que existe lo que se conoce como HSS (*Home Subscriber Server*) servidor que centraliza la información de todos los usuarios, disminuyendo la complejidad de la red y aplicando las políticas de seguridad respectivas. El *Softswitch* no tiene la funcionalidad de validar la

información del abonado origen. El SBC es el dispositivo encargado de consultar al HSS, cuentas, servicios y política aplicativa a cada usuario que accede a la red, validando la información de origen y protegiendo la red en caso de un ataque de negación o degradación del servicio.

V.2.1 Esquema de Conectividad de Ubicación y Respaldo de la Plataforma IMS

A continuación, en la figura 40 se puede observar el diseño de la placa integrada de los elementos de la red IMS, en la figura siguiente:

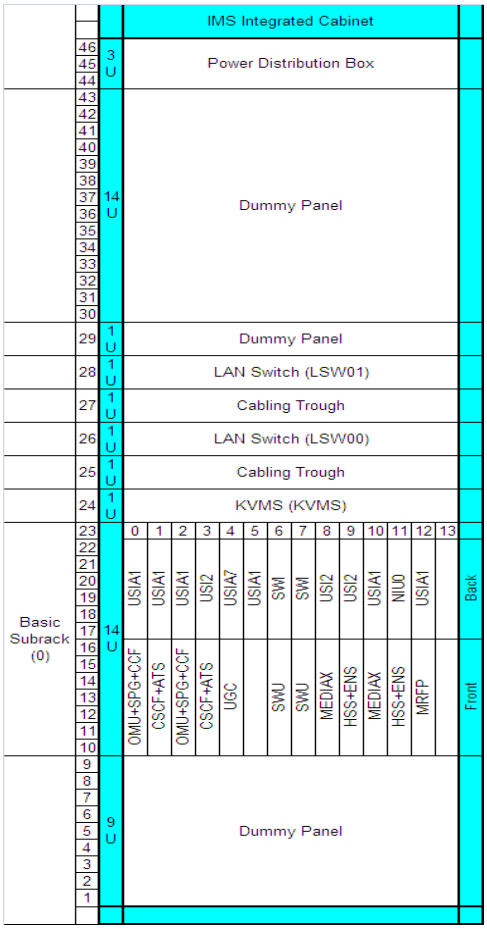


Figura 40: Gabinete físico plataforma IMS.

Fuente: [Documento facilitado por CANTV].

Capacidades Técnicas de la actual plataforma IMS proveedor HUAWEI (maqueta) en laboratorio de CANTV:

- Huawei ATCA Hardware Platform.
- MediaX3600 V3R5 (830 ports).
- MRP6600 V1R2 (702 channels).
- CSC3300 V1R6 (2K subs).
- HSS9820 V9R6 (2K subs FE, 2K subs BE).
- iCG9815 V3R2 (30K CDR/hour).
- SPG2800 V1R2 (2K subs).
- OMS2600 V1R6 (2K subs).
- ATS9900 V1R2 (2K subs).
- UCG3200 V2R8 (92 erl).

Actualmente el tráfico de voz es manejado por seis (6) parejas de *Softswitch* a nivel nacional. Cada pareja de *Softswitch* se encuentra en configuración activo/pasivo, cada *Softswitch* tiene su respectiva base de datos (activo/pasivo). Para la red SBC se propone la implementación de tres (3) SBC marca Acmepacket Net-Net 9000, un (1) SBC para cada pareja de *Softswitch* en la región capital, configuración activo/activo (Nodo principal). El SBC Acmepacket Net-Net 9000 posee redundancia por sí solo. De igual forma se plantea el despliegue de tres (3) SBC marca Acmepacket Net-Net 9000, un (1) SBC para cada pareja de *Softswitch* para la región del interior del país, donde se encuentran el resto de los *Softswitch* que funcionan como redundancia (Nodo secundario). Los SBC deben estar situados en nodos de distribución de la red de '*backbone*' NGN (red troncal), dependiendo de la energía disponible en el '*Data Center*' y capacidad física de alojar los equipos, en las localidades de Caracas y Barquisimeto (activo/pasivo). En la figura 41 se puede observar el SBC (*Session Border Controller*) marca Acmepacket Net-Net 9000:

Figura 41: SBC marca Acmepacket Net-Net 9000.

Fuente: [Documento facilitado por CANTV].

Es mandatorio migrar toda la información de los usuarios y los servicios de las bases de datos NGN a los servidores HSS, por un tema de seguridad, para el control de las cuentas y credenciales de los usuarios, centrando la seguridad en un solo elemento, mitigando de esta forma posibles ataques. Los servidores HSS deben estar en puntos de distribución o '*core*' (red IP/MPLS). Para los nodos externos (*outdoor*), con acceso directo a la red troncal o de '*backbone*', es necesaria la implementación de un SBC para el tráfico de voz y mitigar ataques de negación o degradación del servicio.

En la figura 42, se puede observar el diagrama de conectividad de ubicación y respaldo del modelo de seguridad IMS:

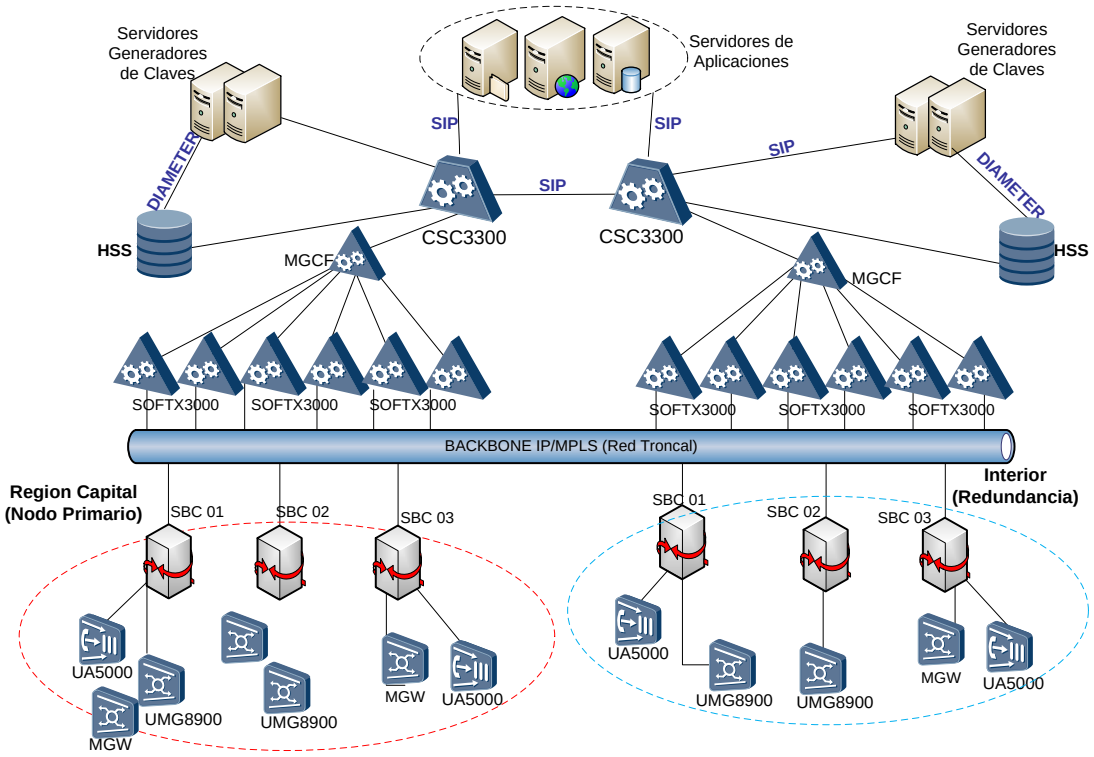


Figura 42: Diagrama de conectividad de ubicación y respaldo del modelo de seguridad IMS.
Fuente: [Elaboración propia].

Los SBC 01/02/03 corresponden a los SBC primarios, cada uno de ellos posee su propia redundancia, configuración activo/activo. Los SBC de la región del interior es la redundancia. Cada SBC dispondrá de dos (2) interfaces de 1Gbps ópticas:

- Una (1) interfaz pública o externa, conectada a los equipos que funcionan como puerta de enlace para el acceso de los usuarios NGN y abonados multimedia.
- Una (1) interfaz privada o interna, conectada a la red privada (IP/MPLS) de CANTV.
- Adicionalmente los equipos SBC pueden requerir una o dos interfaces *Ethernet* 10/100/1000 Mbps para interconectarse directamente con su pareja, para el funcionamiento del mecanismo de redundancia activo pasivo.

Los servidores generadores de claves son los encargados de proporcionar las contraseñas a los usuarios para acceder a la red privada, autenticando la IMPU del usuario a través del HSS (protocolo Diameter) y obteniendo la IMPI del usuario respectiva. Los servidores van a estar conectados al CSC3300 a través del protocolo SIP, con una interfaz 10 Gbps (fibra). Se deben tener en consideración todas las características de seguridad que ofrece cada uno de los protocolos para brindar robustez a la plataforma.

V.2.2 Esquema de conectividad lógico de la Plataforma.

La interconexión de los abonados POTS a la red NGN de CANTV, se realizará a través de Nodos de Acceso que manejan protocolo H.248, y troncales TDM a través del UMG8900 H.248. De igual forma, los abonados multimedia accederán a la red NGN de CANTV, a través de una sesión SIP que se establecerá directamente entre los usuarios y los equipos SBC, utilizando el algoritmo de compresión UIT-T G.723. Los equipos SBC (*Session Border Controller*) estarán interconectados a su vez a la capa de control de la NGN (*Softswitch*) a través de troncales SIP, utilizando el mismo algoritmo de compresión UIT-T G.723. La razón de utilizar el algoritmo G.723 es para el ahorro en ancho de banda. Ante una llamada, el SBC se encargará de enviar la señalización al *Softswitch* correspondiente de la red privada NGN y aplicará las políticas de seguridad y control en la cantidad de llamadas permitidas por elemento (CAC) sobre el tráfico de señalización SIP y voz RTP para su posterior entrega a la red IMS (en caso de comunicación con un cliente IMS), la capa de los SBC señaliza la llamada sin necesidad de acceder a una capa de orden superior.

Se debe encriptar campos claves en la información de señalización para evitar ataques de usurpación de identidad o desvío de la información. Se debe configurar un mecanismo de redundancia en esquema activo/pasivo entre las interfaces privadas de cada pareja de equipos SBC, con el objeto de que uno de ellos asuma el rol de SBC activo y el otro asuma el rol de SBC pasivo. El mecanismo debe permitir una dirección IP virtual o flotante entre los equipos SBC. El mecanismo debe garantizar

que al momento de fallar alguna de las interfaces (privadas o públicas) del equipo SBC activo, el equipo SBC pasivo debe asumir el rol de activo para ambas interfaces (privadas o públicas) los elementos pasivos deben estar ubicados en una localidad diferente a los activos. Para el enrutamiento desde la pareja de equipos SBC se deben configurar rutas estáticas, estableciendo como '*default gateway*' la dirección de la interfaz privada del SBC correspondiente. El esquema mencionado anteriormente se encuentra representado en la figura 43.

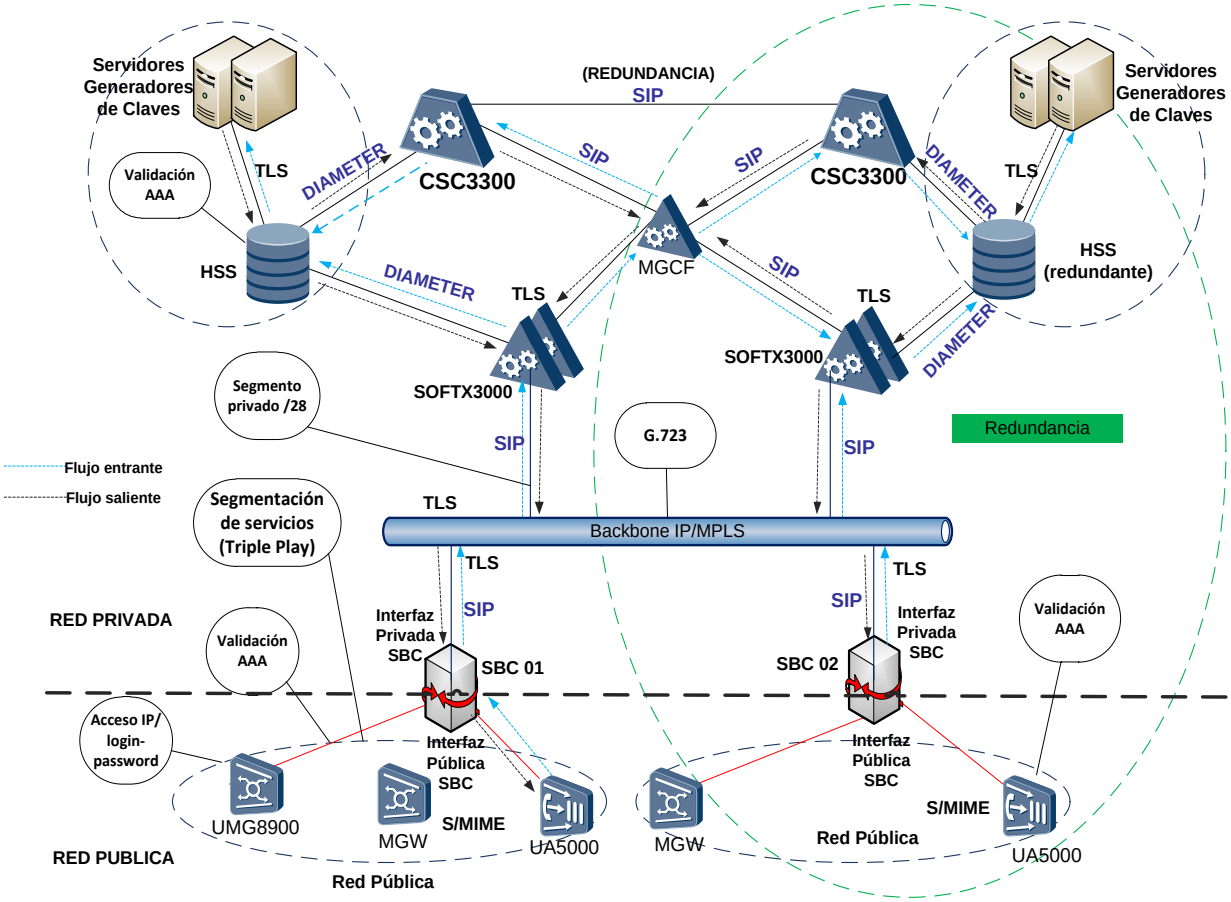


Figura 43: Diagrama de conectividad lógico del modelo de seguridad IMS.

Fuente: [Elaboración propia].

Para la red privada de CANTV, es necesario implementar direcciones privadas /28 para proteger la red, para evitar conexiones entrantes/salientes a Internet y proteger la red privada, y al tener direcciones privadas los dispositivos conocen el rango de

direcciones IP permitidas para recibir y enviar paquetes de forma segura. El SBC segmenta la red y funciona como el elemento controlador de borde entre la red pública (usuarios) y la red privada de control. Es indispensable la encriptación de la información de intercambio de los elementos de control de la plataforma (CSC3300, SOFTX3000, Servidores de claves, etc.). Es necesario un mecanismo de seguridad a nivel de capa de control, específicamente para los elementos bajo el protocolo H.248, ya que al no existir un mecanismo de autenticación, el ambiente es propenso para la creación de llamadas sin facturación. En este sentido, es necesario proteger la media, encriptando la voz para evitar ataques de interferencia (*eavesdropping*). Según el RFC 2401 y el RFC 2411, propuestos por la IETF define el mecanismo de seguridad propuesto para este protocolo cuando es transportado sobre redes IP es el IPsec (*Internet Protocol Security*).

Según el RFC 3525 de la IETF, que corresponde al protocolo H.248 (*Gateway Control Protocol*), es necesaria la seguridad para las conexiones de los dispositivos que usen este protocolo. Proponen varias características (*Features*) de seguridad, como el uso de dos cabeceras para el manejo de claves manuales de seguridad.

Para ello plantean la creación de una cabecera de autenticación AH (*Autenticación Header*) para proporcionar mayor seguridad a la red, ya que permite la autenticación del origen de los datos, integridad sin conexión y protección opcional en los mensajes de señalización entre los dispositivos de control de la red (MGW, MGWC, SG7000). Implementaciones de la cabecera AH requieren del soporte de dos algoritmos, para la verificación de la integridad en el uso de claves manuales, los cuales son:

- HMAC con MD5 [MG97a].
- HMAC con SHA-1 [MG97b].

Adicionalmente se propone una cabecera opcional denominada ESP (*IP Encapsulating Security Payload*), la cual proporciona confidencialidad de los mensajes (RFC 2406). Para el uso de la cabecera ESP, es que requiere un conjunto

mínimo de algoritmos para la comprobación de la integridad y el cifrado. Para una correcta implementación de ESP, es necesario el apoyo de ciertos algoritmos los cuales se citan a continuación:

- DES en modo CBC [MD97].
- HMAC con MD5 [MG97a].
- HMAC con SHA-1 [MG97b].
- Algoritmo de autenticación NULL.
- Algoritmo de cifrado NULL.

Estas implementaciones de cabeceras de seguridad para el manejo de claves públicas, deben usar el protocolo IKE (*Internet Key Exchange*). El protocolo para Intercambio de Claves en Internet es el encargado, en la infraestructura IPSec, de proporcionar un entorno previo seguro para la compartición de una clave secreta y autenticación de los extremos. El protocolo IKE utiliza el puerto 500 de UDP para establecer el intercambio de mensajes pertinente. Por lo general se implementa como una aplicación en espacio de usuario, al no formar parte del núcleo de muchos sistemas operativos.

V.3 Resumen Arquitectura Modelo de Arquitectura IMS

- Manejo de protocolos AAA, para la autenticación de los usuarios y equipos.
- La implementación de una capa SBC, para segmentar la red pública de la red privada, controlando el acceso de los usuarios y ocultando la topología privada de la red, brindando la seguridad y calidad de servicio requerida.
- Implementación de protocolos de compresión G.723 para las llamadas, y ahorrar ancho de banda y mejorar el rendimiento de los elementos controladores.
- Permitir acceso de los usuarios a través de dirección lógica (IP), cuenta y contraseña (*login/password*), así como dirección MAC ADDRESS de ser posible para la validación de usuarios legítimos y mitigar intrusiones a la red.

- Es necesario implementar todas las características (*features*) de seguridad ofrecidos por los protocolos SIP, H.248, H.323 y Diameter, involucrados en el modelo propuesto.
- Autenticación de los elementos H.248 debe estar soportada por un sistema de autenticación automatizado.
- Implementar protocolos de encriptación para el transporte seguro de la información como TLS y S/MIME, al igual que el protocolo RTCP para el control de la media (RTP) durante una transmisión.
- El planteamiento de una capa de SBC (*Session Border Controller*), estableciendo una capa de borde entre los dispositivos y la capa de control NGN, formando esto parte de la arquitectura lógica de seguridad que brinde protección a las capas de control NGN e IMS.
- Implementación de mecanismos de seguridad y acceso que permitan la auditoría y control de recursos según perfiles de usuario, unificado para diversos servicios, por ejemplo '*Triple play'*.
- Implementación de un HSS (*Home Subscriber Server*) servidor que centraliza la información de todos los usuarios, para el control de las cuentas y credenciales de los usuarios, centrando la seguridad en un dispositivo.
- Implementación de servidores generadores de claves integrados al HSS, encargados de proporcionar las contraseñas a los usuarios para acceder a la red privada.
- Los abonados multimedia accederán a la red NGN de CANTV, a través de una sesión SIP que se establecerá directamente entre los usuarios y los equipos SBC, y utilización del algoritmo de compresión UIT-T G.723.
- Los equipos SBC (*Session Border Controller*) estarán interconectados a su vez a la capa de control de la NGN (*Softswitch*) a través de troncales SIP, utilizando el mismo algoritmo de compresión UIT-T G.723.
- Encriptar campos claves de los paquetes correspondientes a la señalización para la mitigación de ataques.

- Encriptación de la media (voz) para evitar ataques de *eavesdropping*.
- Establecer ambas interfaces correspondientes a cada SBC, en la red privada segura de la plataforma.
- Implementación de direccionamiento privado /28, para evitar conexión con Internet y para tener las direcciones IP justas para la cantidad de dispositivos en el segmento de red.
- Implementar protocolos SIP y H.248 sobre protocolos de encriptación como IPsec (*IP Security*).
- Implementar cabecera opcional ESP (*IP Encapsulating Security Payload*) para la encriptación de la data (*payload*), utilizando protocolo IPsec.
- Utilizar protocolo IKE (*Internet Key Exchange*) para el intercambio seguro de las claves públicas y privadas.

Capítulo VI
Conclusiones

Cada vez se hace mas imperativo el hecho de que las empresas proveedoras de servicios de telecomunicaciones emigren hacia nuevas tecnologías para satisfacer las necesidades de sus usuarios ofreciendo más y mejores servicios, esto implica el aumento de la complejidad en las redes y el surgimiento de nuevos riesgos de seguridad, por lo que es imprescindible la realización de una evaluación de seguridad acerca de la tecnología que se desea implementar, para con esto obtener una visión preliminar de las ventajas y riesgos que pueda traer consigo una nueva tecnología en caso de una eventual implementación a futuro, y así evitar eventos que atenten contra la prestación de los servicios y posibles pérdidas a las empresas.

El estudio de las capacidades, elementos y funcionamiento de las plataformas de Próxima Generación (NGN), fue fundamental para determinar las ventajas de este tipo de redes. El logro de este objetivo trajo como consecuencia el manejo de los conocimientos necesarios para determinar posibles mecanismos de prevención, detección y corrección de fallas presentes o potenciales en la actual plataforma operativa NGN de CANTV.

Para la tecnología IMS fue imprescindible el estudio de los elementos que la componen así como de sus principales funcionalidades beneficios y ventajas de esta novedosa tecnología. De igual forma se obtuvieron los conocimientos necesarios para la elaboración del protocolo de pruebas de seguridad y posterior evaluación de la plataforma en laboratorio de CANTV.

En la evaluación de las plataformas NGN e IMS en laboratorio de CANTV, una vez elaborados ambos protocolos de seguridad, se ejecutaron cada una de las pruebas propuestas para la detección de los riesgos presentes o potenciales en ambas

plataformas. Los resultados obtenidos en las pruebas fueron fundamentales para la elaboración de las matrices de severidad ya que con estas se obtuvo una visión acerca del grado de afectación y la naturaleza de cada uno de los riesgos, necesaria para la elaboración del documento de arquitectura conceptual y especificaciones técnicas, que contenga estrategias a seguir y requerimientos de seguridad para una posible implementación a futuro por parte de la empresa.

En miras hacia la evolución de la actual red NGN de CANTV, la nueva tecnología IMS es la solución ideal para la convergencia de la plataforma y servicios, integrando las comunicaciones fijas con las móviles, además de proporcionar nuevas aplicaciones y servicios. Con esta nueva tecnología además es posible brindar servicios específicos a cada usuario, sin necesidad de proporcionar un servicio secundario, es decir, actualmente para proporcionar acceso a internet, es necesario contar con un servicio telefónico y posteriormente es solicitado el servicio de datos. Con IMS es posible tener un servicio de datos específico sin necesidad de un servicio básico para utilizar el servicio deseado.

Es necesario el estudio y elaboración de documentos conceptuales que aborden necesidades, ventajas, desventajas y beneficios de una nueva tecnología antes de abordar una implementación. Es mandatorio estudiar las capacidades técnicas de las plataformas y servicios actuales, para determinar escalabilidad dependiendo de la demanda de nuevos y mejores servicios.

La tecnología IMS puede valerse por sí sola y no necesita ser implementada sobre otra tecnología ya existente, por lo que los riesgos de seguridad serían los inherentes de dicha tecnología, pero en el caso CANTV puede ser implementada como una capa superior a la actual red NGN, por lo que las vulnerabilidades existentes en la red actual serían heredadas al efectuarse la eventual implementación de la nueva tecnología.

IMS proporciona mecanismos de seguridad independientes de la red de acceso, por lo cual si la seguridad de la red de acceso es vulnerada, IMS continuaría estando protegida por sus propios mecanismos de seguridad. En IMS, el uso de asociaciones de seguridad proporciona protección a la información, mediante mecanismos de cifrado e integridad. IMS utiliza el Protocolo de Seguridad de IP (IPsec) que proporciona las reglas para el establecimiento de asociaciones de seguridad, en el que se determinan los parámetros de seguridad (algoritmos y claves) para proteger la comunicación, proporcionando así seguridad al tráfico entre el equipo del usuario y el P-CSCF (*Proxy-CSCF*).

La implementación de una arquitectura de control de borde que gestione y autentifique la conexión de los usuarios con la red interna de CANTV proporcionaría niveles óptimos de seguridad, manteniendo aislada la capa de control de la red de elementos externos que puedan realizar posibles fraudes o ataques.

Es mandatorio proporcionar garantías de calidad de servicio a los usuarios finales, con el fin de cumplir con el ancho de banda y demás requisitos para las aplicaciones multimedia y demás servicio, fijados en los SLA (*Service Level Agreement*) entre el proveedor y el cliente. Por lo tanto es fundamental proporcionar arquitecturas seguras para garantizar la continuidad del negocio y cumplir con los parámetros de QoS establecidos. Es fundamental asegurar los servidores, dispositivos y elementos de control para la facturación y registro de los servicios, evitando fraudes y protegiendo los recursos de la empresa.

IMS crea una arquitectura modular que permite la segmentación y prestación de servicios únicos y distintos para cada tipo de usuario, dependiendo de sus necesidades. Ofrecer a los usuarios la misma cantidad y calidad de servicios, independientemente de la tecnología de acceso del mismo, es el gran reto de los

proveedores. Es necesario aplicar políticas de seguridad para la gestión de los equipos.

La arquitectura conceptual, especificaciones técnicas, dispositivos de seguridad planteados son los aspectos necesarios y de importancia en el Modelo de Seguridad. Algunos componentes y servicios, como *Firewalls*, SBCs y demás elementos, se plantean como soluciones a los riesgos detectados producto de la investigación y las evaluaciones realizadas.

Las puertas de enlace predeterminadas (*gateways*) son los elementos más vulnerables en la red IMS, ya que son los elementos que están expuestos a la red externa. Con la implementación de los SBC se mitiga este riesgo, protegiendo el acceso a la red privada y protegiendo los MGCF (*Media Gateway Control Function*), los MGW (*Media Gateway*) y el P-CSCF (*Proxy-CSCF*). Es fundamental el ocultamiento de la topología de la red interna de CANTV, para evitar ataques de negación o degradación del servicio, mitigando fraudes internos y externos. La plataforma NGN permite una segmentación limitada de servicios, contrario a su sucesor IMS, el cual busca la convergencia y fácil manejo de los servicios y su aprovisionamiento.

El presente documento conceptual representa el inicio o la base para las futuras evaluaciones de seguridad en cuanto a la plataforma IMS para su formalización y entrega al departamento de planificación de redes; unificando las estrategias a seguir y las especificaciones necesarias para su eventual implementación en CANTV.

Recomendaciones

- Realizar el estudio previo de la seguridad siempre que se desee adoptar alguna nueva tecnología, para con esto tomar las medidas de mitigación pertinentes y así evitar eventos de negación y degradación del servicio y fraudes. Es necesario un análisis conceptual de las tecnologías implicadas en el proceso, para determinar ventajas/desventajas y beneficios que trae consigo la implementación de la tecnología para soportar la inversión económica que debe realizar la empresa.

- Hacer uso de los protocolos AAA (*Authentication, Authorization and Accounting*) entre el UE (*User Equipment*) y el S-CSCF, para el control de acceso de los usuarios a la red privada. El protocolo Diameter es la solución para la autenticación de los usuarios y evitar ataques de negación o degradación del servicio.

- Establecer protocolos de encriptación para el transporte seguro de la información diferente a IPsec (*IP Security*) para evitar robo/desvío de la información o ataques de suplantación de identidad, que ocasionen degradación o negación de los servicios.

- Se recomienda integración del servidor generador de contraseñas con la base de datos de la plataforma IMS, el HSS (*Home Subscriber Server*). La integración se propone para brindar mayor seguridad a la plataforma, centrando la seguridad en un solo dispositivo, mejorando la eficiencia de la red ya que no existe la necesidad de encriptar la información entre el servidor y el HSS para el envío seguro de la información.

- Segmentar la red pública de la red privada, brindando un enlace seguro y una asociación de seguridad entre el UE y el P-CSCF para la protección de la red

interna. Es necesario proporcionar autenticación de los datos de origen para corroborar identificación del usuario.

- Es necesario proveer seguridad en el dominio de la red interna entre el HSS y el I-CSCF (*Interrogating-CSCF*), que es el encargado de obtener cuenta, credenciales y servicios para cada usuario a través del protocolo Diameter. Es necesario implementar todas las características de seguridad que ofrece el protocolo Diameter para brindar la protección necesaria.

- Proporcionar seguridad entre los nodos centrales de control de la plataforma IMS (*I/P/S-CSCF*), a través del protocolo SIP. Es necesario blindar la comunicación entre estos tres (3) nodos, ya que es fundamental para la plataforma la confidencialidad de la información de control para el establecimiento, gestión y culminación de las sesiones de los usuarios.

- Implementación de un sistema de autentificación automatizado que brinde la seguridad necesaria, por lo que se propone implementar servidores integrados generadores de contraseñas, para no suministrar a los usuarios multimedia ni al personal interno las contraseñas para la validación de las credenciales de los servicios. Se propone la creación de una rutina para estos servidores que, de forma automatizada, cambien semanalmente las contraseñas para los abonados multimedia.

- El planteamiento de una capa de SBC (*Session Border Controller*), para con esto proporcionar una capa superior a la capa de control de CANTV en la arquitectura lógica, para brindar mayor protección a las capas de control NGN e IMS, mediante el manejo de toda la señalización para el establecimiento, gestión y control de las sesiones multimedia, al igual que el manejo del flujo donde viaja la voz, blindando las capas de control de las plataformas. La capa SBC brindará diversas funciones como control de acceso para los usuarios, protección de la red

contra virus y gusanos, funcionalidades NAT (*Network Address Translation*), manipulación de números telefónicos y de URIs (Uniform Resource), enrutamiento basado en calidad de los enlaces, entre otras funciones. El uso de una capa de SBC es la medida de mitigación de numerosos riesgos presentes actualmente, dicha capa proporcionaría, no sólo la seguridad necesaria para la protección de la red, agregaría simplicidad a la capa de control de la red eximiendo de funciones a los elementos de control, aumentando la eficiencia de la red y ahorrando procesamiento de estos elementos para las funciones que debe ejecutar.

- En el presente trabajo de grado se plantea la implementación de una capa de seguridad, basada en SBCs (*Session Border Controllers*) para segmentar la red pública de la red privada y brindar la protección a la capa de control de la plataforma, esto como parte del modelo de seguridad expuesto. Se propone el estudio de las capacidades técnicas de la actual plataforma NGN de CANTV, a nivel de capa de transporte, para determinar soporta de la demanda de ancho de banda y calidad de servicio que se necesita para la posible implementación de la tecnología IMS. Determinar capacidades técnicas de los equipos controladores de borde (SBC) para determinar mejor proveedor, marca y modelo para brindar la seguridad necesaria a la plataforma.

- Es mandatorio migrar toda la información de los usuarios y los servicios de las bases de datos NGN a los servidores HSS. Los servidores HSS deben estar en nodos de distribución o '*core*' (red IP/MPLS). Con estos servidores se centraliza la información de todos los usuarios, disminuyendo la complejidad de la red y aplicando las políticas de seguridad respectivas.

- Es necesario realizar un estudio exhaustivo de las capacidades de la actual red de transporte de CANTV, para determinar si es capaz de manejar la gran demanda de

velocidades para proporcionar los servicios que ofrece IMS a los usuarios, con la calidad de servicio requerida.

- Antes de una posible implementación de la tecnología IMS, es imperativo determinar estrategias y tecnologías a seguir y adoptar, para ofrecer iguales servicios con velocidades semejantes tanto a los usuarios IMS como a los abonados que pertenecen a la red PSTN y abonados multimedia de la red NGN.

- Es de suma importancia plantear la búsqueda de un mecanismo alterno para proporcionar contraseñas a los clientes y sus servicios, para no facilitar la contraseña al cliente, quedando la incertidumbre para el proveedor de un intento de fraude facilitando la cuenta y la contraseña a otro usuario. Es mandatorio establecer contraseñas integradas con los dispositivos de última milla, para evitar fraudes internos o de usuarios que faciliten la información e intenten realizar llamadas y adquirir recursos de la red para utilizar los servicios ofrecidos al usuario legítimo.

- Se recomienda implementación de la última versión de IMS 3GPP / TISPAN. De igual forma, migrar o actualizar a la última versión de NGN TISPAN. Las versiones han sufrido modificaciones y mejoras, tanto a nivel funcional como seguridad, por ello se recomiendan las últimas versiones en caso de una posible implementación.

- Se recomienda que la tecnología IMS maneje aplicativos desarrollados para Software Libre, así como versatilidad para la implementación y políticas de seguridad y auditoria.

Bibliografía

1. Bertrand, G. (2007). *The IP Multimedia Subsystem in Next Generation Networks.* Recuperado el 8 de Febrero de 2011, de http://www.tele.pw.edu.pl/~mareks/auims/IMS_an_overview-1.pdf
2. Cabezas Pozo, J. D. (2007). *Sistemas de Telefonía.* Madrid: Thomson Paraninfo.
3. Cabrejos, C., & Cuesta, E. (2009). *Diseño de una Red IMS para la cuidad de Ica.* Lima: Pontificia Universidad Catolica del Perú.
4. Camarillo, G., & García Martín, M. (2006). *The 3G IP Multimedia Subsystem (IMS).* Chichester: John Wiley & Sons Ltd,.
5. Centro de Investigación para la Sociedad de la Información. (2009). *Integracion NGN.* Recuperado el 2 de Febrero de 2011, de http://www.imaginar.org/ngn/manuales/Integracion_NGN.pdf
6. Cisco Systems. (2006). *Comunicaciones y Tecnologias de Conectividad de Redes.* New Jersey: Prentice Hall.
7. Compañia Anonima Nacional Telefonos de Venezuela. CANTV. (2006). *NGN- Next Generation Networks.* Caracas: CANTV.
8. Compañía Anónima Nacional Teléfonos de Venezuela. CANTV. (2010). *Procedimiento de Gestion de Riesgos.* Caracas: CANTV.
9. Estrella Bonilla, D. (2007). *Diseño de un Prototipo de Red de Nueva Generación NGN (Next Generation Network), basado en una arquitectura MetroEthernet para proveer servicio de VoIP.* Quito: Escuela Politecnica Nacional.
10. García, E. (2003). *Estrategia de Migración de las Redes de voz alambricas, inalambricas y móviles a la arquitectura de Redes de Nueva Generación.* Cuernavaca: Centro Nacional de Investigación y Desarrollo Tecnológico.

11. Gil, P., Pomares, J., & Candelas, F. (2010). *Redes y Transmisión de datos.* Alicante: Universidad de Alicante.
12. Huawei Technologies Co. (2010). *IMS Network Architecture.*
13. Huawei Technologies. Co. (2010). *IMS System Protocol Overview.*
14. Huidobro, J., & Conesa, R. (2007). *Sistemas de Telefonía.* Madrid: Thomson Paraninfo.
15. Lopez Austin, A. (2005). *El modelo en la ciencia y la cultura.* Buenos Aires: Siglo xxi Editores.
16. Mohammad, I., & Syed, A. (2009). *IP Multimedia Subsystem (IMS) handbook.* Boca Raton: Taylor and Francis Group.
17. Moreno Bayardo, M. (1987). *Introducción a la metodología de la Investigación Educativa.* Moscú: Editorial Progreso.
18. Normetn, H. (2007). A Singel Killer App? Not in Today's Personalized World. *IMS Magazine*.
19. Poikselka, M., Mayer, G., Khartabil, H., & Niemi, A. (2006). *The IMS IP Multimedia Concepts and Services 2nd Edition.* Chichester: John Wiley & Sons Ltd,.
20. Ramos, I., & Armas, Y. (2009). *Tipos de Evaluacion segun las Diferentes Tipologias.* Valle de la Pascua: Universidad Experimental Simon Rodriguez.
21. Real Martín, L. (2008). *COITT.* Recuperado el 5 de Febrero de 2011, de http://coitt.es/res/revistas/05d_Arquitectura.pdf
22. Rios, J., & García, M. (2005). *Softswitch.* Caracas: Compañía Anónima Nacional Teléfonos de Venezuela.
23. Russell, T. (2007). *The IP Multimedia Subsystem (IMS): Session Control and Other Network Operations.* Columbus: McGraw-Hill.
24. Tejedor Millán, R. (2006). *Ramonmillan.com.* Recuperado el 4 de Febrero de 2011, de http://www.ramonmillan.com/tutoriales/ims.php
25. Wong, M. (2003). *IMS Security Framework.* Wippany: Third Generation Partnership Project.

Apéndices

Apéndice A

Extracto Protocolo de Pruebas Plataforma NGN

Proyecto: NGN CANTV.	Documento: Protocolo de pruebas del Softswitch de la plataforma NGN de CANTV.	Versión: 2.0
Descripción general de las pruebas: Pruebas SOS: Plataforma de Próxima Generación NGN.		Fecha: 30/11/2011.
Localidad: Edificio NEA. Caracas.	Tipo de pruebas: Laboratorio. Maqueta NGN.	Elementos: SOFTSWITCH NGN.

INDICE DE PRUEBAS DE SEGURIDAD DE LA OPERACIÓN PLATAFORMA NGN.

Proyecto: NGN CANTV.	**Documento:** Protocolo de pruebas del Softswitch de la plataforma NGN de CANTV.	**Versión:** 2.0
Descripción general de las pruebas: Pruebas SOS: Plataforma de Próxima Generación NGN.		**Fecha:** 30/11/2011.
Localidad: Edificio NEA. Caracas.	**Tipo de pruebas:** Laboratorio. Maqueta NGN.	**Elementos:** SOFTSWITCH NGN.

Identificación del Documento		
Nombre del archivo: Protocolo NGN V2.docx	Código del documento: EVA-GSOS-PLATNGN-CONTROL	Edición actual: Versión 2.0
Elaborado por: Eugenio Flores Ignacio Suarez Fernando Monegui	Unidad: Gerencia Corporativa de Seguridad de la Operación y Servicios.	Fecha: 02/02/2011.

Revisiones del documento			
Edición	**Responsable de modificación / revisión**	**Breve descripción de la modificación / revisión**	**Fecha de modificación / revisión**
1.0	Ignacio Suarez Fernando Monegui	Inicio del Protocolo.	16/12/2011
1.5	Ignacio Suarez Fernando Monegui	Modificaciones del Protocolo de Pruebas.	05/01/2012
2.0	Ignacio Suarez Fernando Monegui	Modificaciones del Protocolo de Pruebas.	30/01/2012

Proyecto: NGN CANTV.	**Documento:** Protocolo de pruebas del Softswitch de la plataforma NGN de CANTV.	**Versión:** 2.0
Descripción general de las pruebas: Pruebas SOS: Plataforma de Próxima Generación NGN.		**Fecha:** 30/11/2011.
Localidad: Edificio NEA. Caracas.	**Tipo de pruebas:** Laboratorio. Maqueta NGN.	**Elementos:** SOFTSWITCH NGN.

Personal involucrado en las Evaluaciones y Pruebas			
Nombre y Apellido	**Unidad**	**Función**	**Fecha de evaluación**
Eugenio Flores	CANTV	Evaluador/Revisor	16/12/2011
Ignacio Suarez	CANTV	Equipo de Pruebas	16/12/2011
Fernando Monegui	CANTV	Equipo de Pruebas	16/12/2011
Jody Gener	HUAWEI	Equipo de Pruebas	16/12/2011

Revisado por:	Eugenio Flores (CANTV)
	Eduardo Vásquez (Huawei)

Proyecto: NGN CANTV.	**Documento:** Protocolo de pruebas del Softswitch de la plataforma NGN de CANTV.	**Versión:** 2.0
Descripción general de las pruebas: Pruebas SOS: Plataforma de Próxima Generación NGN.		**Fecha:** 30/11/2011.
Localidad: Edificio NEA. Caracas.	**Tipo de pruebas:** Laboratorio. Maqueta NGN.	**Elementos:** SOFTSWITCH NGN.

No. de Prueba. 2.2	**Condiciones iniciales:** Todos los equipos conectados y funcionando correctamente.	**Nombre y Descripción de la prueba:** *Validación de autenticación SIP.* Verificar el funcionamiento de la autenticación. El análisis incluye: MAC Address, IP, login/password. Verificar la correcta autenticación revisando la señalización de un usuario cualquiera por diferentes métodos.
Equipos usados: JDSU TPS (Triple Play Services), Softphone Xlite v.4.1, Softswitch SOFTX3000. **Modelo / Versión:** Laptop HP Dv6. SoftX3000 v.300R010C05SPC100		
Procedimiento: 1. Crear usuario SIP en el Softswitch. 2. Registrar usuario en el Softswitch. 3. Capturar señalización. 4. Verificar la correcta autenticación del usuario por MAC Address, dirección IP, usuario y contraseña. 5. Analizar resultados.		**Escenario de prueba:** Diagrama 2.0
Resultados obtenidos: El UA se puede registrar con dirección IP (172.16.74.6) con su LOGIN/PASSWORD correspondiente, el SoftX3000 no permite el registro de otro UA con otra IP. Por dirección física (MAC) no se puede realizar la autenticación de un usuario. Se puede realizar la autenticación de un usuario registrado en el SoftX3000 con su LOGIN/PASSWORD. Para mayor seguridad, se puede realizar la autenticación SIP con la dirección IP del dispositivo y LOGIN/PASSWORD. Los resultados de esta prueba se pueden observar en los archivos: Prueba NGN_2.2 IP, Prueba NGN_2.2 Logpas, Prueba NGN_2.2 IPLogpas.		**Resultados Esperados:** Se espera la correcta autenticación y autorización del usuario registrado por MAC Address, IP y login/password. **Prueba satisfactoria:** Aprobado [V] Fallido [ ] Repetir [ ] **Aprobado por:** **Revisado por:**

Proyecto: NGN CANTV.	Documento: Protocolo de pruebas del Softswitch de la plataforma NGN de CANTV.	Versión: 2.0
Descripción general de las pruebas: Pruebas SOS: Plataforma de Próxima Generación NGN.		**Fecha:** 30/11/2011.
Localidad: Edificio NEA. Caracas.	**Tipo de pruebas:** Laboratorio. Maqueta NGN.	**Elementos:** SOFTSWITCH NGN.

No. de Prueba. 3.7	**Condiciones iniciales:** Todos los equipos conectados y funcionando correctamente.	**Nombre y Descripción de la prueba:** *Descubrir dispositivos SIP* Realizar un escaneo de direcciones IP, según la herramienta de auditoría de sistemas basados en SIP según el RFC 3261, para intentar descubrir dispositivos SIP.
Equipos usados: JDSU TPS (Triple Play Services), Softphone Xlite v.4.1, Softswitch SOFTX3000. **Modelo / Versión:** Laptop HP Dv6. SoftX3000 v.300R010C05SPC100		
Procedimiento: 1. Registrar dos (2) cuentas de usuario en el Softswitch. 2. Utilizar el comando para descubrir dispositivos SIP según la herramienta de auditoría de sistemas basados en SIP según el RFC 3261. 3. Verificar si el SoftX3000 se identifica como un dispositivo perteneciente a la red. 4. Verificar información proporcionada por el SoftX3000.		**Escenario de prueba:** Diagrama 2.0
Resultados obtenidos: El Softswitch no se protege eficazmente, frente al ataque realizado utilizando la herramienta de auditoría de sistemas basados en SIP según el RFC 3261. Al ejecutar el comando 'svmap' el Softswitch envía una respuesta al mensaje OPTIONS. El SoftX3000 da respuesta a los mensajes enviados pero no se identifica, solamente proporciona su dirección IP, por lo que puede ser vulnerable frente a un ataque para colapsar el dispositivo como un 'flooding' de mensajes. Los resultados de esta prueba se observan en la captura Descubrir Dispositivos SIP.		**Resultados Esperados:** Se espera que el Softswitch no proporcione ninguna información, protegiéndose frente a cualquier intento de fraude o degradación del servicio. **Prueba satisfactoria:** Aprobado [V] Fallido [ ] Repetir [ ] **Aprobado por:** **Revisado por:**

Apéndice B

Extracto Protocolo de Pruebas Plataforma IMS

Proyecto: IMS CANTV.	Documento: Protocolo de pruebas del CSCF de la plataforma IMS de CANTV.	Versión: 2.0
Descripción general de las pruebas: Pruebas SOS: Plataforma IMS (IP Multimedia SubSystem).		Fecha: 30/11/2011.
Localidad: Edificio NEA. Caracas.	Tipo de pruebas: Laboratorio. Maqueta IMS.	Elementos: CSCF (Call Session Control Function).

INDICE DE PRUEBAS DE SEGURIDAD DE LA OPERACIÓN PLATAFORMA IMS.

Proyecto: IMS CANTV.	Documento: Protocolo de pruebas del CSCF de la plataforma IMS de CANTV.	Versión: 2.0
Descripción general de las pruebas: Pruebas SOS: Plataforma IMS (IP Multimedia SubSystem).		**Fecha:** 30/11/2011.
Localidad: Edificio NEA. Caracas.	**Tipo de pruebas:** Laboratorio. Maqueta IMS.	**Elementos:** CSCF (Call Session Control Function).

Proyecto: IMS CANTV.	**Documento:** Protocolo de pruebas del CSCF de la plataforma IMS de CANTV.	**Versión:** 2.0
Descripción general de las pruebas: Pruebas SOS: Plataforma IMS (IP Multimedia SubSystem).		**Fecha:** 30/11/2011.
Localidad: Edificio NEA. Caracas.	**Tipo de pruebas:** Laboratorio. Maqueta IMS.	**Elementos:** CSCF (Call Session Control Function).

Identificación del Documento		
Nombre del archivo: Pruebas GSO v250811 IMS.docx	Código del documento: EVA-GSOS-PLATIMS-CONTROL	Edición actual: Versión 2.0
Elaborado por: Eugenio Flores Ignacio Suarez Fernando Monegui	Unidad: Gerencia Corporativa de Seguridad de la Operación y Servicios.	Fecha: 29/11/2011.

Revisiones del documento			
Edición	**Responsable de modificación / revisión**	**Breve descripción de la modificación / revisión**	**Fecha de modificación / revisión**
1.0	Ignacio Suarez Fernando Monegui	Inicio del Protocolo.	09/01/2012.
1.5	Ignacio Suarez Fernando Monegui	Modificaciones del Protocolo de Pruebas.	11/01/2012.
2.0	Ignacio Suarez Fernando Monegui	Modificaciones del Protocolo de Pruebas.	18/01/2012

Proyecto: IMS CANTV.	**Documento:** Protocolo de pruebas del CSCF de la plataforma IMS de CANTV.	**Versión:** 2.0
Descripción general de las pruebas: Pruebas SOS: Plataforma IMS (IP Multimedia SubSystem).		**Fecha:** 30/11/2011.
Localidad: Edificio NEA. Caracas.	**Tipo de pruebas:** Laboratorio. Maqueta IMS.	**Elementos:** CSCF (Call Session Control Function).

Personal involucrado en las Evaluaciones y Pruebas			
Nombre y Apellido	**Unidad**	**Función**	**Fecha de evaluación**
Eugenio Flores	CANTV	Evaluador/Revisor	27/01/2012.
Ignacio Suarez	CANTV	Equipo de Pruebas	09/01-27/01/2012.
Fernando Monegui	CANTV	Equipo de Pruebas	09/01-27/01/2012.
Eduardo Vasquez	HUAWEI	Equipo de Pruebas	09/01-27/01/2012.

Revisado por:	Eugenio Flores (CANTV)
	Eduardo Vásquez (Huawei)

Proyecto: IMS CANTV.	**Documento:** Protocolo de pruebas del CSCF de la plataforma IMS de CANTV.	**Versión:** 2.0
Descripción general de las pruebas: Pruebas SOS: Plataforma IMS (IP Multimedia SubSystem).		**Fecha:** 30/11/2011.
Localidad: Edificio NEA. Caracas.	**Tipo de pruebas:** Laboratorio. Maqueta IMS.	**Elementos:** CSCF (Call Session Control Function).

No. de Prueba. 2.5	**Condiciones iniciales:** Todos los equipos conectados y funcionando correctamente.	**Nombre y Descripción de la prueba:** *Generación de llamadas SIP, misma identidad.* Validar mecanismo del P-CSCF (Proxy-Call Session Control Function) para determinar el verdadero usuario, al intentar autenticarse dos usuarios distintos, que conocen los datos de una misma cuenta correctamente registrada en el HSS. El P-CSCF debe identificar el usuario perteneciente a la cuenta asociada para el establecimiento de una llamada.
Equipos usados: JDSU TPS (Triple Play Services), Softphone Xlite v.4.1, CSC3300 V1R6 (2k subs)_Master site. **Modelo / Versión:** Laptop HP Dv6.		
Procedimiento: 1. Registrar dos (2) usuarios en el HSS (Home Suscriber Server). 2. Realizar la autenticación de dos (2) usuarios diferentes con la misma cuenta registrada en el Softswitch (UAC). 3. Intentar establecer una llamada del UAC o Abonado A (usuario válido) al UAS o Abonado B. 4. Intentar establecer una llamada del UAC o Abonado A (usuario inválido) al UAS o Abonado B. 5. Verificar si se establecen ambas llamadas.		**Escenario de prueba:** Diagrama 2.0
Resultados obtenidos: Detectada una vulnerabilidad del P-CSCF, admite el registro de dos usuarios distintos con los datos de una misma cuenta registrada en el HSS. Se puede realizar un filtraje de grupos de IP en el P-CSCF, crear tabla con las direcciones IP validas y solamente ese grupo de IP son las que el HSS recibirá paquetes. El P-CSCF no permite realizar llamadas a dos usuarios diferentes con la misma cuenta. Vulnerabilidad detectada ya que un usuario válido registrado no puede realizar llamadas (DoS) debido al otro usuario (fraudulento) que se registró con la misma cuenta del usuario A.		**Resultados Esperados:** Se espera que el CSCF determine el verdadero usuario asociado a la cuenta registrada, rechazando la solicitud del segundo usuario evitando el establecimiento de la llamada. **Prueba satisfactoria:** Aprobado [V] Fallido [ ] Repetir [ ] **Aprobado por:** **Revisado por:**

Proyecto: IMS CANTV.	Documento: Protocolo de pruebas del CSCF de la plataforma IMS de CANTV.	Versión: 2.0
Descripción general de las pruebas: Pruebas SOS: Plataforma IMS (IP Multimedia SubSystem).		**Fecha:** 30/11/2011.
Localidad: Edificio NEA. Caracas.	**Tipo de pruebas:** Laboratorio. Maqueta IMS.	**Elementos:** CSCF (Call Session Control Function).

No. de Prueba. 6.2	**Condiciones iniciales:** Todos los equipos conectados y funcionando correctamente.	**Nombre y Descripción de la prueba:** *Autenticación e integración de elementos no HUAWEI. (Señalización y Gestión)*
Equipos usados: JDSU TPS (Triple Play Services), Softphone Xlite v.4.1, CSC3300 V1R6 (2k subs)_Master site. **Modelo / Versión:** Laptop HP Dv6.		Se espera la autenticación e integración de elementos propietarios a otros proveedores, tanto a nivel de señalización como a nivel de gestión.
Procedimiento: 1. Registrar ambos usuarios en el HSS. 2. Intentar autenticación de un UA no Huawei. 3. Intentar captación de información de gestión distinto al N2000 de Huawei. 4. Verificar autenticación e integración de estos elementos.		**Escenario de prueba:** Diagrama 2.0
Resultados obtenidos: A nivel de señalización es posible la integración de equipos de terceros (otro proveedor), siempre y cuando los protocolos sean estandarizados y no propietarios del tercero. A nivel de gestión, no es posible la integración de equipos de terceros a los gestores Huawei.		**Resultados Esperados:** Se espera integración de elementos Huawei, tanto a nivel de señalización como a nivel de gestión.
		Prueba satisfactoria: Aprobado [V] Fallido [ ] Repetir [ ]
		Aprobado por: **Revisado por:**

Apéndice C

Matrices de Severidad de Evaluación Plataforma NGN

Proyecto: NGN CANTV.	Documento: Protocolo de pruebas del Softswitch de la plataforma NGN de CANTV.	Versión: 2.0
Descripción general de las pruebas: Pruebas SOS: Plataforma de Próxima Generación NGN.		**Fecha:** 30/11/2011.
Localidad: Edificio NEA. Caracas.	**Tipo de pruebas:** Laboratorio. Maqueta NGN.	**Elementos:** SOFTSWITCH NGN.

INDICE DE PRUEBAS DE SEGURIDAD DE LA OPERACIÓN PLATAFORMA NGN.

Gerencia General de Seguridad Integral
Gerencia de Seguridad de la Operación y Servicios
Coordinación de Riesgos de Servicios y Antifraude

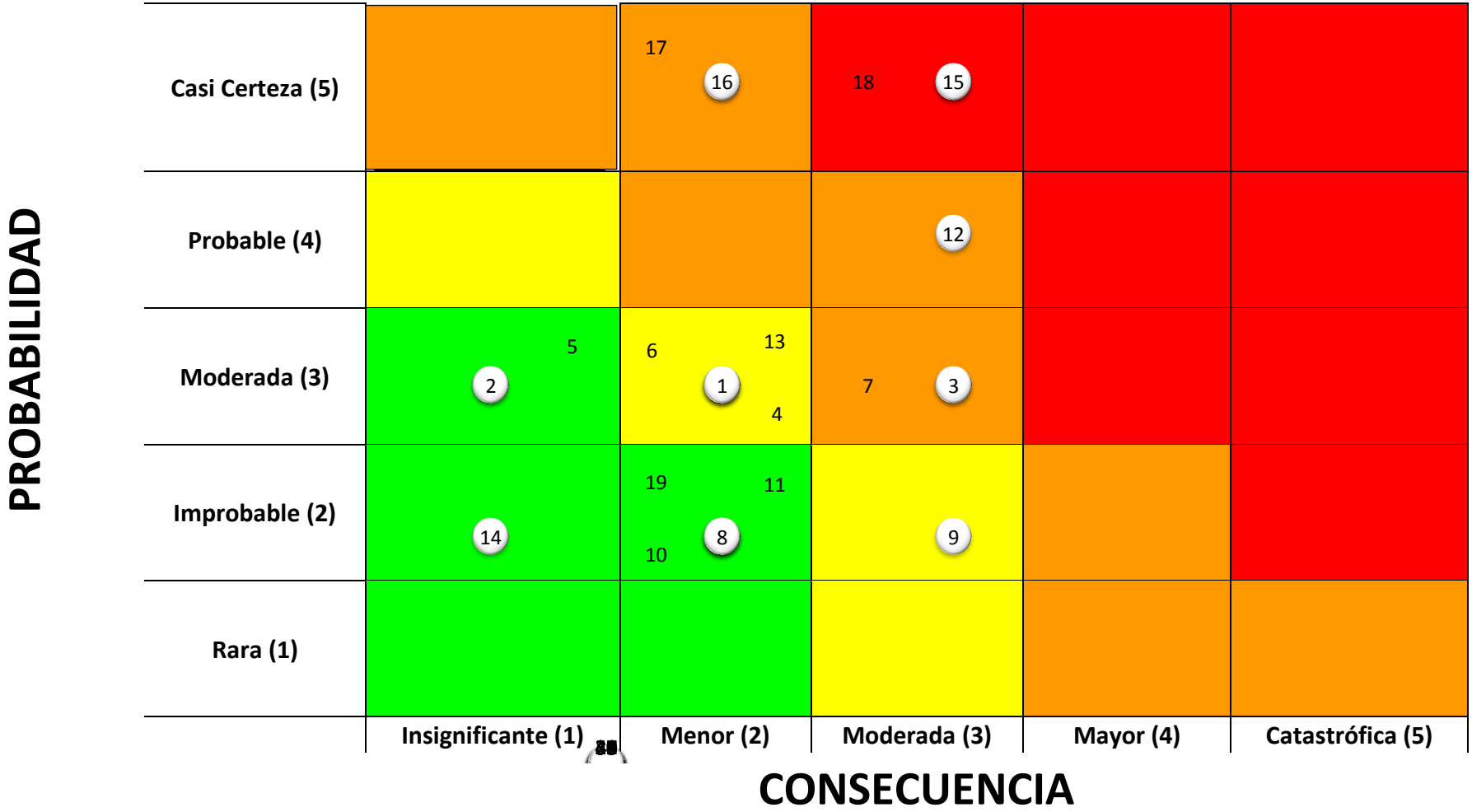
Modelo de Seguridad IMS para el Aseguramiento de Plataforma y Servicios - Fase Conceptual

30/11/2011

Pruebas SOS. Plataforma de Próxima Generación NGN

		CONSECUENCIA									PROBABILIDAD				
N°	IDENTIFICACIÓN DEL RIESGO	CLIENTES	FINANCIERO	DURACIÓN (ACCIÓN REQUERIDA)	CALIDAD DEL SERVICIO	IMPORTANCIA ESTRATEGICA	ELEMENTOS DE RED	IMAGEN CORPORATIVA	COMPLEJIDAD	TOTAL	Posibilidad	TOTAL	SEVERIDAD DE RIESGO (INHERENTE)	ESTATUS	RESPONSABLE
1	Seguridad comprometida por carencia de autenticación de los elementos que conforman la red NGN	1	1	5	1	5	1	1	2	2	3	3	MODERADA	Abierto	CANTV
2	Falta de manejo de algunos códec por parte del Softswitch	1	1	2	1	1	1	1	2	1	3	3	BAJA	Abierto	CANTV
3	Seguridad comprometida por conexión directa de los nodos NGN contra el Softswitch	1	1	5	1	5	3	1	3	3	3	3	ALTA	Abierto	CANTV
4	Seguridad comprometida debido a que el Softswitch da respuesta a todos los mensajes que recibe	1	1	5	3	2	4	1	2	2	3	3	MODERADA	Abierto	CANTV
5	Ausencia de cifrado de la información por parte de los equipos ua5000,	1	1	2	1	2	1	1	2	1	3	3	BAJA	Abierto	CANTV
6	Falta de manejo de protocolos de seguridad por parte del Softswitch	1	1	2	1	3	1	1	4	2	3	3	MODERADA	Abierto	CANTV
7	Entrega de dirección IP por parte del Softswitch	1	1	5	1	3	4	1	5	3	3	3	ALTA	Abierto	CANTV
8	Ausencia de validación de numero infinito	1	1	3	1	2	4	1	2	2	2	2	BAJA	Abierto	CANTV
9	Falta de capacidad de procesamiento del Softswitch	2	3	3	1	2	4	2	5	3	2	2	MODERADA	Abierto	CANTV
10	Ausencia de sistema de notificación de alarmas alterno	1	1	2	1	3	4	1	3	2	2	2	BAJA	Abierto	CANTV
11	Incapacidad de integración de elementos no Huawei para la gestión de seguridad de la red	1	1	2	1	3	1	1	3	2	2	2	BAJA	Abierto	CANTV
12	Seguridad comprometida por falta de segmentación de la red	1	1	5	1	4	4	1	5	3	4	4	ALTA	Abierto	CANTV
13	Incapacidad de bloqueo automatizado de usuarios	1	1	3	1	3	4	1	5	2	3	3	MODERADA	Abierto	CANTV
14	Comunicación insegura entre elementos de la capa de control	1	1	2	1	2	1	1	2	1	2	2	BAJA	Abierto	CANTV
15	Falta de autenticación entre UA y Softswitch	1	3	5	1	5	1	2	3	3	5	5	EXTREMA	Abierto	CANTV
16	Falta de una base de datos centralizada	1	1	5	1	4	3	1	3	2	5	5	ALTA	Abierto	CANTV
17	Ausencia de un sistema automatizado de generación de claves de seguridad integrado a la base de datos	1	1	5	1	4	1	1	3	2	5	5	ALTA	Abierto	CANTV
18	Falta de autenticación de usuarios multimedia	1	3	5	1	5	1	1	3	3	5	5	EXTREMA	Abierto	CANTV
19	Ausencia de mecanismo de protección para el reinicio automático de tarjetas del Softswitch	1	1	2	3	2	4	1	2	2	2	2	BAJA	Abierto	CANTV
										2		3	MODERADA		

MATRIZ DE RIESGOS INHERENTES
Modelo de Seguridad IMS para el Aseguramiento de Plataforma y Servicios - Fase Conceptual



#	IDENTIFICACIÓN DEL RIESGO	CONSECUENCIA	PROBABILIDAD	SEVERIDAD
1	Seguridad comprometida por carencia de autenticación de los elementos que conforman la red NGN	2	3	MODERADA
2	Falta de manejo de algunos códec por parte del Softswitch	1	3	BAJA
3	Seguridad comprometida por conexión directa de los nodos NGN contra el Softswitch	3	3	ALTA
4	Seguridad comprometida debido a que el Softswitch da respuesta a todos los mensajes que recibe	2	3	MODERADA
5	Ausencia de cifrado de la información por parte de los equipos ua5000,	1	3	BAJA
6	Falta de manejo de protocolos de seguridad por parte del Softswitch	2	3	MODERADA
7	Entrega de dirección IP por parte del Softswitch	3	3	ALTA
8	Ausencia de validación de numero infinito	2	2	BAJA
9	Falta de capacidad de procesamiento del Softswitch	3	2	MODERADA
10	Ausencia de sistema de notificación de alarmas alterno	2	2	BAJA
11	Incapacidad de integración de elementos no Huawei para la gestión de seguridad de la red	2	2	BAJA
12	Seguridad comprometida por falta de segmentación de la red	3	4	ALTA
13	Incapacidad de bloqueo automatizado de usuarios	2	3	MODERADA
14	Comunicación insegura entre elementos de la capa de control	1	2	BAJA
15	Falta de autenticación entre UA y Softswitch	3	5	EXTREMA
16	Falta de una base de datos centralizada	2	5	ALTA
17	Ausencia de un sistema automatizado de generación de claves de seguridad integrado a la base de datos	2	5	ALTA
18	Falta de autenticación de usuarios multimedia	3	5	EXTREMA
19	Ausencia de mecanismo de protección para el reinicio automático de tarjetas del Softswitch	2	2	BAJA

Gerencia General de Seguridad Integral
Gerencia de Seguridad de la Operación y Servicios
Coordinación de Riesgos de Servicios y Antifraude

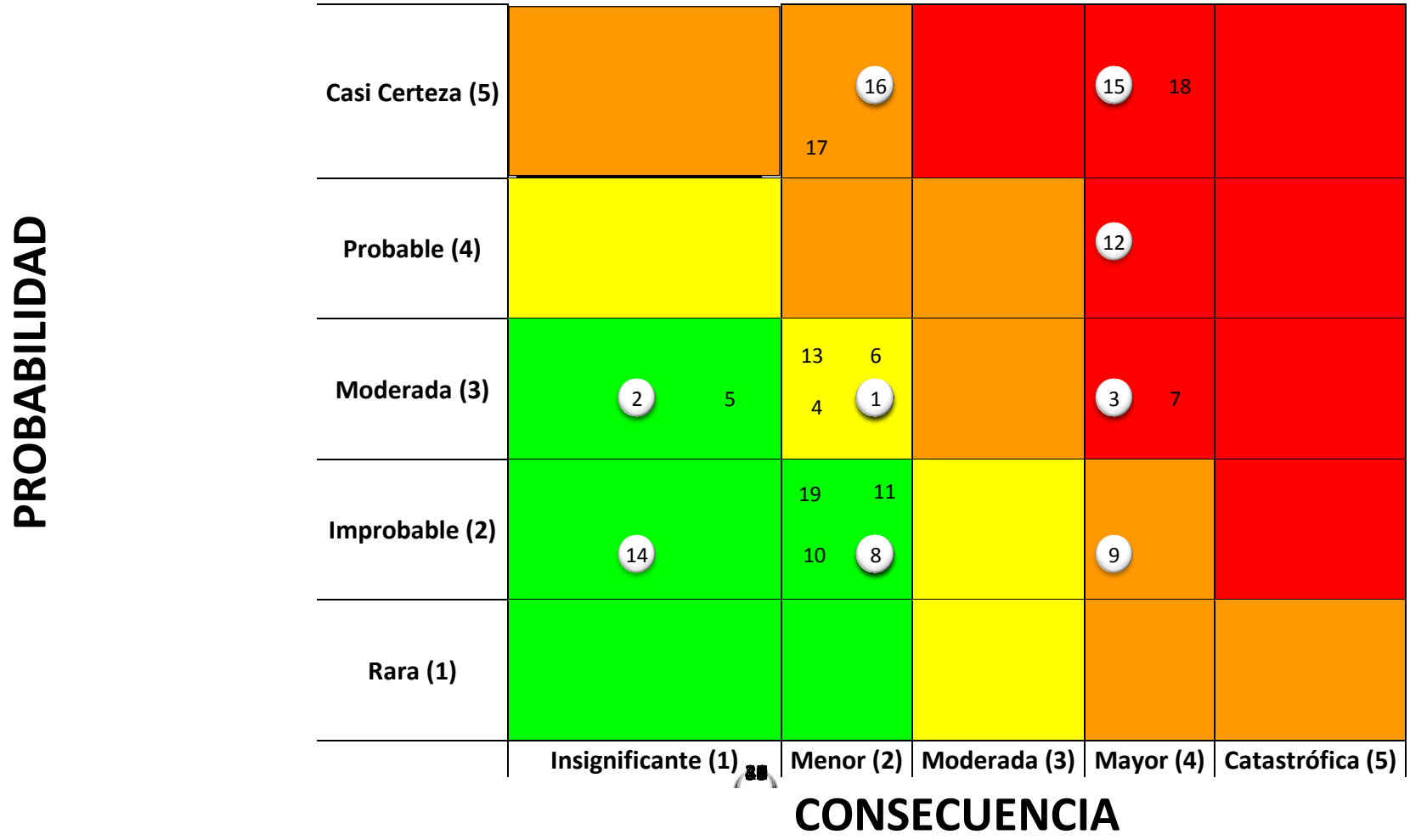
Modelo de Seguridad IMS para el Aseguramiento de Plataforma y Servicios - Fase Conceptual **10/01/2012**

Pruebas SOS. Plataforma de Próxima Generación NGN

30/11/2011

		CONSECUENCIA									PROBABILIDAD					
N°	IDENTIFICACIÓN DEL RIESGO	CLIENTES	FINANCIERO	DURACIÓN (ACCIÓN REQUERIDA)	CALIDAD DEL SERVICIO	IMPORTANCIA ESTRATEGICA	ELEMENTOS DE RED	IMAGEN CORPORATIVA	COMPLEJIDAD	TOTAL	Posibilidad	TOTAL	SEVERIDAD DE RIESGO (INHERENTE)	SEVERIDAD DE RIESGO (CONTROLADO)	ESTATUS	RESPONSABLE
1	Seguridad comprometida por carencia de autenticación de los elementos que conforman la red NGN	1	1	5	1	5	1	1	2	2	3	3	MODERADA	MODERADA	Abierto	CANTV
2	Falta de manejo de algunos códec por parte del Softswitch	1	1	2	1	1	1	1	2	1	3	3	BAJA	BAJA	Abierto	CANTV
3	Seguridad comprometida por conexión directa de los nodos NGN contra el Softswitch	1	1	5	1	5	3	1	3	3	3	3	ALTA	ALTA	Abierto	CANTV
4	Seguridad comprometida debido a que el Softswitch da respuesta a todos los	1	1	5	3	2	4	1	2	2	3	3	MODERADA	MODERADA	Abierto	CANTV
5	Ausencia de cifrado de la información por parte de los equipos ua5000,	1	1	2	1	2	1	1	2	1	3	3	BAJA	BAJA	Abierto	CANTV
6	Falta de manejo de protocolos de seguridad por parte del Softswitch	1	1	2	1	3	1	1	4	2	3	3	MODERADA	MODERADA	Abierto	CANTV
7	Entrega de dirección IP por parte del Softswitch	1	1	5	1	3	4	1	5	3	3	3	ALTA	ALTA	Abierto	CANTV
8	Ausencia de validación de numero infinito	1	1	3	1	2	4	1	2	2	2	2	BAJA	BAJA	Abierto	CANTV
9	Falta de capacidad de procesamiento del Softswitch	2	3	3	1	2	4	2	5	3	2	2	MODERADA	MODERADA	Abierto	CANTV
10	Ausencia de sistema de notificación de alarmas alterno	1	1	2	1	3	4	1	3	2	2	2	BAJA	BAJA	Abierto	CANTV
11	Incapacidad de integración de elementos no Huawei para la gestión de seguridad de la red	1	1	2	1	3	1	1	3	2	2	2	BAJA	BAJA	Abierto	CANTV
12	Seguridad comprometida por falta de segmentación de la red	1	1	5	1	4	4	1	5	3	4	4	ALTA	ALTA	Abierto	CANTV
13	Incapacidad de bloqueo automatizado de usuarios	1	1	3	1	3	4	1	5	2	3	3	MODERADA	MODERADA	Abierto	CANTV
14	Comunicación insegura entre elementos de la capa de control	1	1	2	1	2	1	1	2	1	2	2	BAJA	BAJA	Abierto	CANTV
15	Falta de autenticación entre UA y Softswitch	1	3	5	1	5	1	2	3	3	5	5	EXTREMA	EXTREMA	Abierto	CANTV
16	Falta de una base de datos centralizada	1	1	5	1	4	3	1	3	2	5	5	ALTA	ALTA	Abierto	CANTV
17	Ausencia de un sistema automatizado de generación de claves de seguridad integrado a la base de datos	1	1	5	1	4	1	1	3	2	5	5	ALTA	ALTA	Abierto	CANTV
18	Falta de autenticación de usuarios multimedia	1	3	5	1	5	1	1	3	3	5	5	EXTREMA	EXTREMA	Abierto	CANTV
19	Ausencia de mecanismo de protección para el reinicio automático de tarjetas del Softswitch	1	1	2	3	2	4	1	2	2	2	2	BAJA	BAJA	Abierto	CANTV
										2		3	MODERADA	MODERADA		

MATRIZ DE RIESGOS CONTROLADOS
Modelo de Seguridad IMS para el Aseguramiento de Plataforma y Servicios - Fase Conceptual



#	IDENTIFICACIÓN DEL RIESGO	CONSECUENCIA	PROBABILIDAD	SEVERIDAD
1	Seguridad comprometida por carencia de autenticación de los elementos que conforman la red NGN	2	3	MODERADA
2	Falta de manejo de algunos códec por parte del Softswitch	1	3	BAJA
3	Seguridad comprometida por conexión directa de los nodos NGN contra el Softswitch	3	3	ALTA
4	Seguridad comprometida debido a que el Softswitch da respuesta a todos los mensajes que recibe	2	3	MODERADA
5	Ausencia de cifrado de la información por parte de los equipos ua5000,	1	3	BAJA
6	Falta de manejo de protocolos de seguridad por parte del Softswitch	2	3	MODERADA
7	Entrega de dirección IP por parte del Softswitch	3	3	ALTA
8	Ausencia de validación de numero infinito	2	2	BAJA
9	Falta de capacidad de procesamiento del Softswitch	3	2	MODERADA
10	Ausencia de sistema de notificación de alarmas alterno	2	2	BAJA
11	Incapacidad de integración de elementos no Huawei para la gestión de seguridad de la red	2	2	BAJA
12	Seguridad comprometida por falta de segmentación de la red	3	4	ALTA
13	Incapacidad de bloqueo automatizado de usuarios	2	3	MODERADA
14	Comunicación insegura entre elementos de la capa de control	1	2	BAJA
15	Falta de autenticación entre UA y Softswitch	3	5	EXTREMA
16	Falta de una base de datos centralizada	2	5	ALTA
17	Ausencia de un sistema automatizado de generación de claves de seguridad integrado a la base de datos	2	5	ALTA
18	Falta de autenticación de usuarios multimedia	3	5	EXTREMA
19	Ausencia de mecanismo de protección para el reinicio automático de tarjetas del Softswitch	2	2	BAJA

Gerencia General de Seguridad Integral
Gerencia de Seguridad de la Operación y Servicios
Coordinación de Riesgos de Servicios y Antifraude

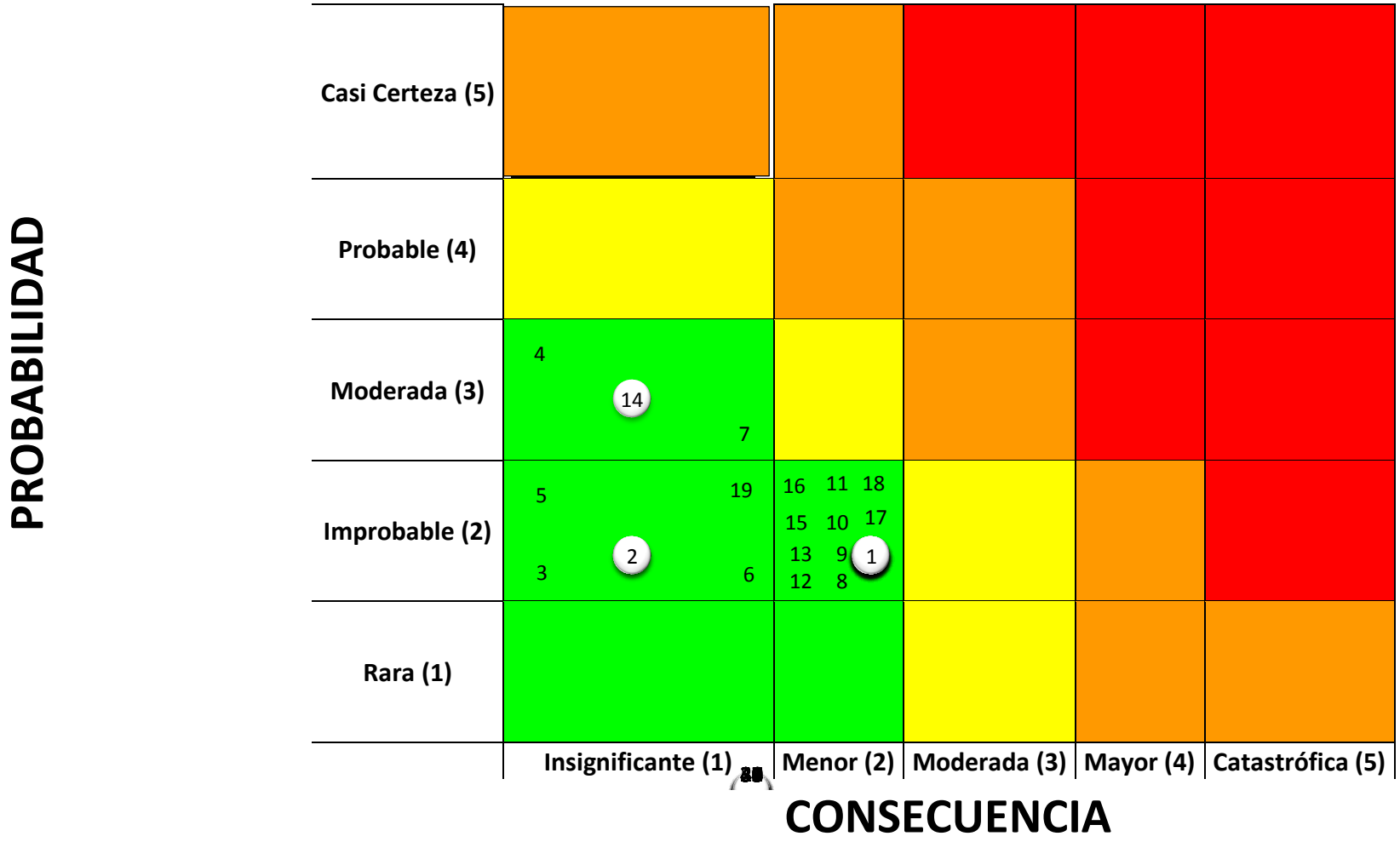
Modelo de Seguridad IMS para el Aseguramiento de Plataforma y Servicios - Fase Conceptual

Fecha: 30/01/2012

Pruebas SOS. Plataforma de Próxima Generación NGN

		CONSECUENCIA									PROBABILIDAD		30/11/2011	10/01/2012			
N°	IDENTIFICACIÓN DEL RIESGO	CLIENTES	FINANCIERO	DURACIÓN (ACCIÓN REQUERIDA)	CALIDAD DEL SERVICIO	IMPORTANCIA ESTRATEGICA	ELEMENTOS DE RED	IMAGEN CORPORATIVA	COMPLEJIDAD	TOTAL	Posibilidad	TOTAL	SEVERIDAD DE RIESGO (INHERENTE)	SEVERIDAD DE RIESGO (CONTROLADO)	SEVERIDAD DE RIESGO (TRATADO)	ESTATUS	RESPONSABLE
1	Seguridad comprometida por carencia de autenticación de los elementos que conforman la red NGN	1	1	5	1	5	1	1	3	2	2	2	MODERADA	MODERADA	BAJA	Abierto	CANTV
2	Falta de manejo de algunos códec por parte del Softswitch	1	1	2	1	1	1	1	2	1	2	2	BAJA	BAJA	BAJA	Abierto	CANTV
3	Seguridad comprometida por conexión directa de los nodos NGN contra el Softswitch	1	1	5	1	3	1	1	3	2	2	2	ALTA	ALTA	BAJA	Abierto	CANTV
4	Seguridad comprometida debido a que el Softswitch da respuesta a todos los mensajes que recibe	1	1	5	1	2	1	1	2	2	2	2	MODERADA	MODERADA	BAJA	Abierto	CANTV
5	Ausencia de cifrado de la información por parte de los equipos ua5000,	1	1	2	1	2	1	1	2	1	2	2	BAJA	BAJA	BAJA	Abierto	CANTV
6	Falta de manejo de protocolos de seguridad por parte del Softswitch	1	1	2	1	3	1	1	4	2	2	2	MODERADA	MODERADA	BAJA	Abierto	CANTV
7	Entrega de dirección IP por parte del Softswitch	1	1	5	1	3	1	1	5	2	2	2	ALTA	ALTA	BAJA	Abierto	CANTV
8	Ausencia de validación de numero infinito	1	1	3	1	2	1	1	2	2	2	2	BAJA	BAJA	BAJA	Abierto	CANTV
9	Falta de capacidad de procesamiento del Softswitch	1	1	3	1	2	1	1	5	2	2	2	MODERADA	MODERADA	BAJA	Abierto	CANTV
10	Ausencia de sistema de notificación de alarmas alterno	1	1	2	1	3	1	1	3	2	2	2	BAJA	BAJA	BAJA	Abierto	CANTV
11	Incapacidad de integración de elementos no Huawei para la gestión de seguridad de la red	1	1	2	1	3	1	1	3	2	2	2	BAJA	BAJA	BAJA	Abierto	CANTV
12	Seguridad comprometida por falta de segmentación de la red	1	1	5	1	4	1	1	5	2	2	2	ALTA	ALTA	BAJA	Abierto	CANTV
13	Incapacidad de bloqueo automatizado de usuarios	1	1	3	1	3	1	1	5	2	2	2	MODERADA	MODERADA	BAJA	Abierto	CANTV
14	Comunicación insegura entre elementos de la capa de control	1	1	2	1	2	1	1	2	1	3	3	BAJA	BAJA	BAJA	Abierto	CANTV
15	Falta de autenticación entre UA y Softswitch	1	1	5	1	5	1	1	3	2	2	2	EXTREMA	EXTREMA	BAJA	Abierto	CANTV
16	Falta de una base de datos centralizada	1	1	5	1	4	1	1	3	2	2	2	ALTA	ALTA	BAJA	Abierto	CANTV
17	Ausencia de un sistema automatizado de generación de claves de seguridad integrado a la base de datos	1	1	5	1	4	1	1	3	2	2	2	ALTA	ALTA	BAJA	Abierto	CANTV
18	Falta de autenticación de usuarios multimedia	1	1	5	1	5	1	1	3	2	2	2	EXTREMA	EXTREMA	BAJA	Abierto	CANTV
19	Ausencia de mecanismo de protección para el reinicio automático de tarjetas del Softswitch	1	1	2	1	2	1	1	2	1	2	2	BAJA	BAJA	BAJA	Abierto	CANTV
										2		2	MODERADA	MODERADA	BAJA		

MATRIZ DE RIESGOS TRATADOS
Modelo de Seguridad IMS para el Aseguramiento de Plataforma y Servicios - Fase Conceptual



#	IDENTIFICACIÓN DEL RIESGO	CONSECUENCIA	PROBABILIDAD	SEVERIDAD
1	Seguridad comprometida por carencia de autenticación de los elementos que conforman la red NGN	2	2	BAJA
2	Falta de manejo de algunos códec por parte del Softswitch	1	2	BAJA
3	Seguridad comprometida por conexión directa de los nodos NGN contra el Softswitch	2	2	BAJA
4	Seguridad comprometida debido a que el Softswitch da respuesta a todos los mensajes que recibe	2	2	BAJA
5	Ausencia de cifrado de la información por parte de los equipos ua5000,	1	2	BAJA
6	Falta de manejo de protocolos de seguridad por parte del Softswitch	2	2	BAJA
7	Entrega de dirección IP por parte del Softswitch	2	2	BAJA
8	Ausencia de validación de numero infinito	2	2	BAJA
9	Falta de capacidad de procesamiento del Softswitch	2	2	BAJA
10	Ausencia de sistema de notificación de alarmas alterno	2	2	BAJA
11	Incapacidad de integración de elementos no Huawei para la gestión de seguridad de la red	2	2	BAJA
12	Seguridad comprometida por falta de segmentación de la red	2	2	BAJA
13	Incapacidad de bloqueo automatizado de usuarios	2	2	BAJA
14	Comunicación insegura entre elementos de la capa de control	1	3	BAJA
15	Falta de autenticación entre UA y Softswitch	2	2	BAJA
16	Falta de una base de datos centralizada	2	2	BAJA
17	Ausencia de un sistema automatizado de generación de claves de seguridad integrado a la base de datos	2	2	BAJA
18	Falta de autenticación de usuarios multimedia	2	2	BAJA
19	Ausencia de mecanismo de protección para el reinicio automático de tarjetas del Softswitch	1	2	BAJA

Gerencia General de Seguridad Integral
Gerencia de Seguridad de la Operación y Servicios
Coordinación de Riesgos de Servicios y Antifraude

Modelo de Seguridad IMS para el Aseguramiento de Plataforma y Servicios - Fase Conceptual

		PUNTOS DE ATENCIÓN Y SEGUIMIENTO				
N°	**IDENTIFICACIÓN DEL RIESGO**	**Descripción**	**Acciones a ejecutar / Seguimiento**	**ESTATUS**	**RESPONSABLE**	**ORIGEN**
1	Seguridad comprometida por carencia de autenticación de los elementos que conforman la red NGN	Este riesgo se refiere a la Seguridad comprometida por carencia de autenticación de los elementos que conforman la red NGN por no manejar protocolos de validación AAA como el Softswitch, UA5000, UMG 8900, SG7000, entre otros. Podría realizarse manipulación no autorizada o fraude interno.	La medida de mitigación para este riesgo seria la Incorporación de protocolos seguros en estos elementos. Por ej. SSH, SFTP, así como AAA.	Abierto	CANTV	TEÓRICO
2	Falta de manejo de algunos códec por parte del Softswitch	Este riesgo va referido a la seguridad comprometida por incorrecto funcionamiento de equipos ya que al recibir una llamada con un códec no manejado por el Softswitch , este consumirá recursos intentando decodificar el paquete	La medida de mitigacion seria la correcta configuracion del Softswitch para que se descarten los paquetes que contengan codecs no autorizados.	Abierto	CANTV	TEÓRICO
3	Seguridad comprometida por conexión directa de los nodos NGN contra el Softswitch	Este riesgo va referido a que los nodos estan directamente conectados al Softswitch para acceder a la informacion de los abonados que se encuentra en la base de datos del Softswitch, como datos de enrutamiento, login/password, facturacion, etc.	La medida de mitigacion de este riesgo es la implementacion de una base de datos centralizada que contenga la informacion de todos los abonados como enrutamiento, login/password, etc, Para con esto eximir al Softswitch de estas funcionalidades	Abierto	CANTV	TEÓRICO
4	Seguridad comprometida debido a que el Softswitch da respuesta a todos los mensajes que recibe	Este riesgo va referido a que el Softswitch da respuesta a todos los mensajes que recibe consumiendo recursos, ya sean usuarios autorizados o no, siendo asi vulnerable a ataques de negación o degradación de servicios	La medida de mitigacion seria la correcta configuracion del Softswitch para que se descarten los paquetes no autorizados y no de respuesta a todos los mensajes.	Abierto	CANTV	TEÓRICO
5	Ausencia de cifrado de la información por parte de los equipos ua5000,	Este riesgo de refiere a la Ausencia de cifrado de la información por parte de los equipos ua5000, debido a que estos equipos solo maneja el protocolo telnet, pudiendo ser usurpada información importante de los usuarios	La medida de mitigación para este riesgo seria la Incorporación de protocolos seguros en estos elementos. Por ej. SSH, SFTP, así como AAA.	Abierto	CANTV	PRUEBAS
6	Falta de manejo de protocolos de seguridad por parte del Softswitch	Este riesgo se refiere a la Falta de manejo de protocolos de seguridad por parte del Softswitch , este únicamente maneja IPsec y no otros como TLS	Las acciones a ejecutar para la mitigacion de este riesgo son la incorporacion de protocolos de seguridad para cifrar y garantizar la integridad de la información, TLS, IPSEC, y tademas la inclusión de equipos SBC para el control del tráfico.	Abierto	CANTV	PRUEBAS
7	Entrega de dirección IP por parte del Softswitch	Este riesgo va referido a que como mecanismo de seguridad el equipo no se identifica como Softswitch pero si da a conocer su dirección IP pudiendo así ser victima de ataques.	La accion a tomar para la mitigacion de este riesgo es la implementacion de una arquitectura de borde para la proteccion de todos los elementos de la capa de control de la red (SBC)	Abierto	CANTV	PRUEBAS
8	Ausencia de validación de numero infinito	Este riesgo va referido a que al discar un numero infinito el Softswitch procesa todos los números para tratar de establecer la llamada consumiendo así recursos en lugar de rechazar la llamada.	La medida de mitigacion seria la correcta configuracion del Softswitch para que se descarten los paquetes que contengan numeros no validos. Uso de DIGIMAP	Abierto	CANTV	PRUEBAS
9	Falta de capacidad de procesamiento del Softswitch	Este riesgo va referido a que al sobrepasar las 400 llamadas por segundo el equipo colapsa, siendo así vulnerable a ataques de degradación o negación de servicios	La accion a ejecutarse seria la implementacion de equipos con una mayor capacidad de procesamiento.	Abierto	CANTV	PRUEBAS

10	Ausencia de sistema de notificación de alarmas alterno	Este riesgo se refiere a que en caso de haber un colapso en la red de transporte se detectara en el gestor que hay desconexión mas no se notificara la falla existente.	La medida de mitigacion de este riesgo seria la implementacion del algun software o sistema de alarmas alterno al del gestor.	Abierto	CANTV	PRUEBAS
11	Incapacidad de integración de elementos no Huawei para la gestión de seguridad de la red	Este riesgo va referido a que es permitida la integración de elementos no Huawei en la capa de control mas no en la gestión de seguridad, lo que genera limitaciones en cuanto a sistemas de seguridad aplicables a la red.	La acción a ejecutar para la mitigación de este riesgo es el desarrollo de una capa de gestión que integre diferentes vendors, o solicitud al proveedor HUAWEI, para incluir elementos de otros vendors en su gestor.	Abierto	CANTV	PRUEBAS
12	Seguridad comprometida por falta de segmentación de la red	Este riesgo va referido a que las capas de seguridad, control y servicios se encuentran en el mismo nivel lógico, en caso de existir una intrusión estarían comprometidas todas las capas.	La accion a ejecutar para la mitigacion de este riesgo es la correcta segmentacion de la red, asignando elementos de seguridad a cada una de las capas.	Abierto	CANTV	PRUEBAS
13	Incapacidad de bloqueo automatizado de usuarios	Este riesgo va referido a la incapacidad de bloqueo automatizado de usuarios fraudulentos o con comportamiento irregular por parte del Softswitch, lo que genera consumo de recursos al procesar las solicitudes de todos los usuarios.	La accion a tomar para la mitigacion de este riesgo es la implementacion de una arquitectura de borde para la proteccion de todos los elementos de la capa de control de la red (SBC)	Abierto	CANTV	PRUEBAS
14	Comunicación insegura entre elementos de la capa de control	Este riesgo va referido a que elementos de la capa de control trabajan con el protocolo H.248 y utilizan udp que no es seguro por ser un protocolo no orientado a conexión y no encriptar la información enviada	La medida de mitigación de este riesgo sería habilitar las características de Seguridad del protocolo H248, implementar IPSEC.	Abierto	CANTV	PRUEBAS
15	Falta de autenticación entre UA y Softswitch	Este riesgo va referido a que entre los UA y el Softswitch no hay una correcta autenticacion, permitiendo suplantacion de identidad y posible fraude.	La medida de mitigacion de este riesgo es la implementacion de una base de datos centralizada que contenga la informacion de todos los abonados como enrutamiento, login/password, etc, Para con esto eximir al Softswitch de estas funcionalidades	Abierto	CANTV	PRUEBAS
16	Falta de una base de datos centralizada	Este riesgo va referido a que no existe una base de datos que contenga la información de todos los usuarios y los servicios que poseen cada uno de ellos, mediante la cual se realice la autentificación de los usuarios, actualmente estos datos se encuentran en el Softswitch generando así consumo de recursos del Softswitch y conexion innecesaria al Softswitch por parte de los usuarios.	La medida de mitigacion de este riesgo es la implementacion de una base de datos centralizada que contenga la informacion de todos los abonados como enrutamiento, login/password, etc, Para con esto eximir al Softswitch de estas funcionalidades	Abierto	CANTV	TEÓRICO
17	Ausencia de un sistema automatizado de generación de claves de seguridad integrado a la base de datos	Este riesgo va referido a la falta de un sistema de generación de claves automatizado y secreto, lo que puede permitir fraudes de suplantación de identidad debido a que las claves son conocidas tanto por el usuario como por el personal de la empresa	La accion a realizar para la mitigacion de este riesgo es la implementacion de un sistema de generacion de claves automatizado para asi evitar este tipo de fraudes	Abierto	CANTV	TEÓRICO
18	Falta de autenticación de usuarios multimedia	Este riesgo va referido a la ausencia de autentificacion de los usuarios multimedia, pudiendo generarse suplantacion de identidad por parte de usuarios fraudulentos	La accion a realizar para la mitigacion de este riesgo es la implementacion de un sistema de generacion de claves automatizado para asi evitar este tipo de fraudes	Abierto	CANTV	TEÓRICO
19	Ausencia de mecanismo de protección para el reinicio automático de tarjetas del Softswitch	Este riesgo va referido a la ausencia de mecanismo de protección para el reinicio automático de alguna tarjeta del Softswitch que presente fallas y poder tomar reestablecer servicio con la brevedad posible	La medida de mitigacion de este riesgo seria la implementacion del algun software o sistema que permita el reinicio automatico de tarjetas que presenten fallas.	Abierto	CANTV	PRUEBAS

Apéndice D

Matrices de Severidad de Evaluación Plataforma IMS

Gerencia General de Seguridad Integral
Gerencia de Seguridad de la Operación y Servicios
Coordinación de Riesgos de Servicios y Antifraude

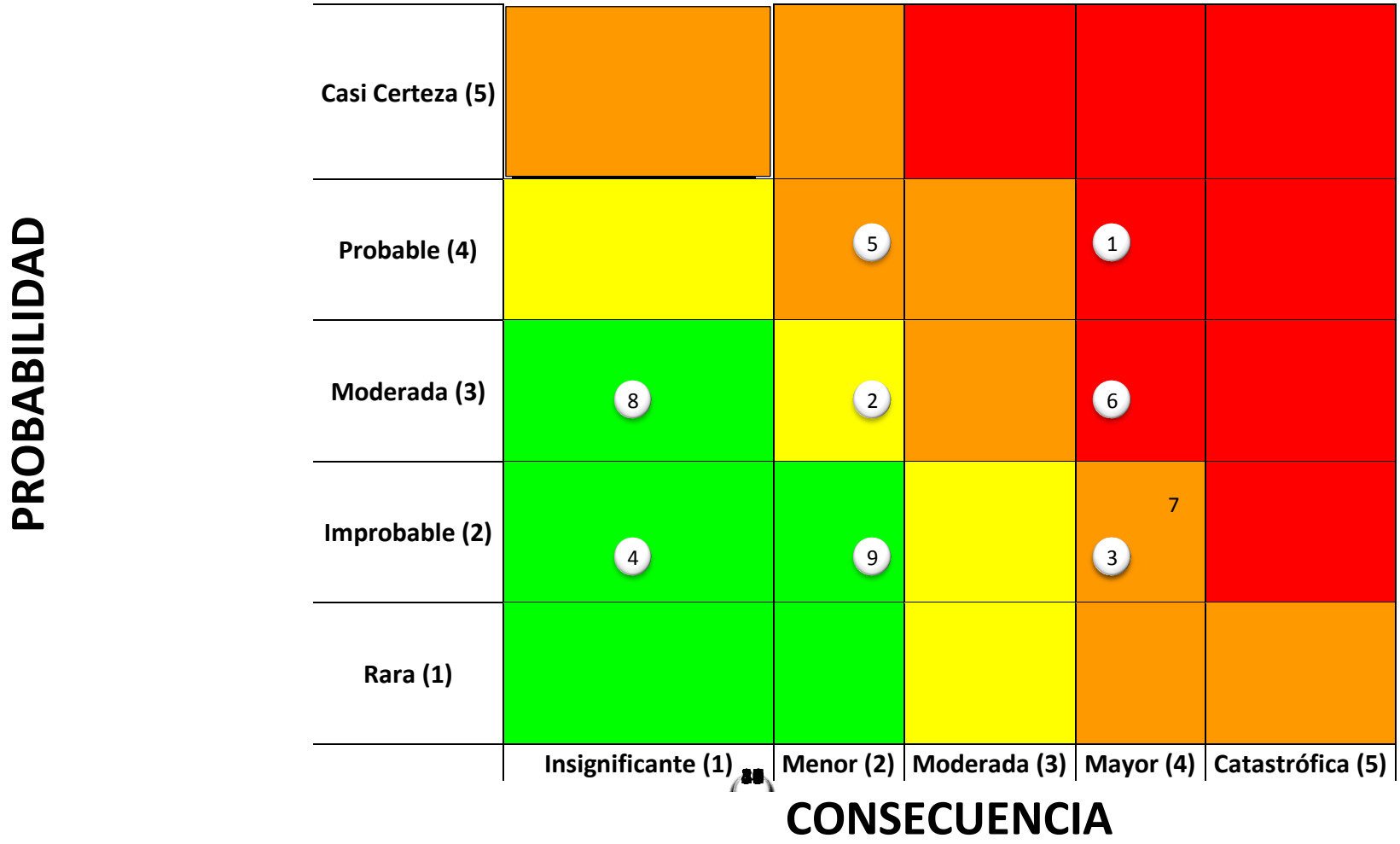
Modelo de Seguridad IMS para el Aseguramiento de Plataforma y Servicios - Fase Conceptual

26/12/2011

Pruebas SOS. Plataforma de Próxima Generación IMS

		CONSECUENCIA									PROBABILIDAD				
N°	IDENTIFICACIÓN DEL RIESGO	CLIENTES	FINANCIERO	DURACIÓN (ACCIÓN REQUERIDA)	CALIDAD DEL SERVICIO	IMPORTANCIA ESTRATEGICA	ELEMENTOS DE RED	IMAGEN CORPORATIVA	COMPLEJIDAD	TOTAL	Posibilidad	TOTAL	SEVERIDAD DE RIESGO (INHERENTE)	ESTATUS	RESPONSABLE
1	Ausencia de autenticacion de los UA	1	2	4	2	4	2	2	3	**3**	4	**4**	ALTA	Abierto	CANTV
2	Ausencia de mecanismo de descarte de mensajes invalidos	2	1	3	3	3	2	1	2	**2**	3	**3**	MODERADA	Abierto	CANTV
3	Prestacion de servicios comprometida por falta de autenticacion de los usuarios	3	3	4	4	4	1	3	3	**3**	2	**2**	MODERADA	Abierto	CANTV
4	Seguridad de informacion comprometida por posibilidad de captura de paquetes en una llamada cualquiera	1	2	2	1	1	1	1	2	**1**	2	**2**	BAJA	Abierto	CANTV
5	Seguridad comprometida debido a que los elementos de la plataforma IMS no manejan protocolos AAA	1	1	3	2	4	2	1	2	**2**	4	**4**	ALTA	Abierto	CANTV
6	Seguridad comprometida debido a que CSCF proporciona su direccion IP	2	3	4	3	4	2	2	5	**3**	3	**3**	ALTA	Abierto	CANTV
7	Prestacion de servicios comprometida por colapso del CSCF al recibir un alto numero de llamadas por segundo	3	3	4	3	3	2	3	5	**3**	2	**2**	MODERADA	Abierto	CANTV
8	Falta de manejo de algunos codec por parte del CSCF	1	1	2	2	1	1	1	2	**1**	3	**3**	BAJA	Abierto	CANTV
9	Incapacidad de integración de elementos no Huawei para la gestión de seguridad de la red	1	1	2	1	3	1	1	3	**2**	2	**2**	BAJA	Abierto	CANTV
										2		**3**	MODERADA		

MATRIZ DE RIESGOS INHERENTES
Modelo de Seguridad IMS para el Aseguramiento de Plataforma y Servicios - Fase Conceptual



#	IDENTIFICACIÓN DEL RIESGO	CONSECUENCIA	PROBABILIDAD	SEVERIDAD
1	Ausencia de autenticacion de los UA	3	4	ALTA
2	Ausencia de mecanismo de descarte de mensajes invalidos	2	3	MODERADA
3	Prestacion de servicios comprometida por falta de autenticacion de los usuarios	3	2	MODERADA
4	Seguridad de informacion comprometida por posibilidad de captura de paquetes en una llamada cualquiera	1	2	BAJA
5	Seguridad comprometida debido a que los elementos de la plataforma IMS no manejan protocolos AAA	2	4	ALTA
6	Seguridad comprometida debido a que CSCF proporciona su direccion IP	3	3	ALTA
7	Prestacion de servicios comprometida por colapso del CSCF al recibir un alto numero de llamadas por segundo	3	2	MODERADA
8	Falta de manejo de algunos codec por parte del CSCF	1	3	BAJA
9	Incapacidad de integración de elementos no Huawei para la gestión de seguridad de la red	2	2	BAJA

Gerencia General de Seguridad Integral
Gerencia de Seguridad de la Operación y Servicios
Coordinación de Riesgos de Servicios y Antifraude

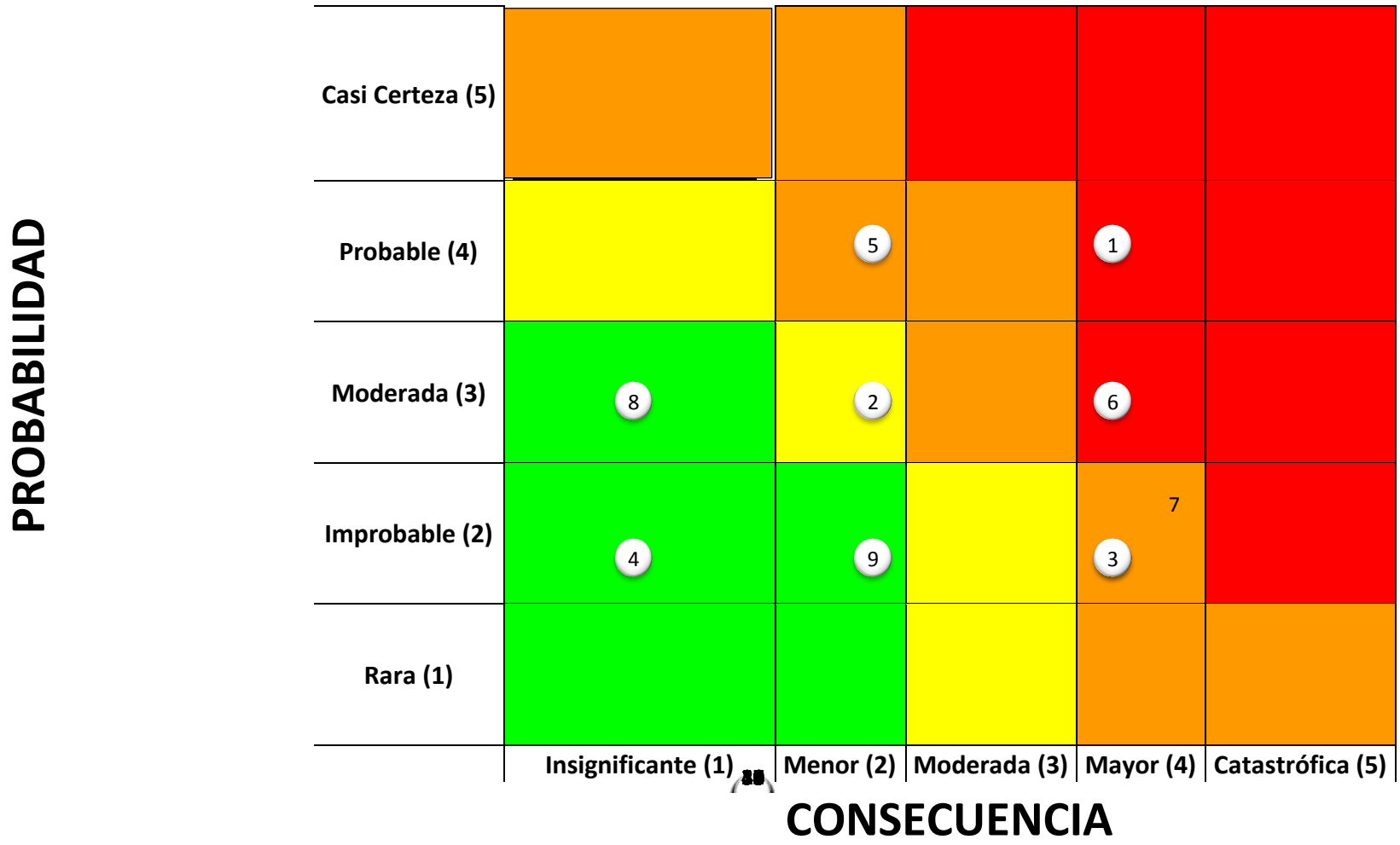
Modelo de Seguridad IMS para el Aseguramiento de Plataforma y Servicios - Fase Conceptual **27/12/2011**

Pruebas SOS. Plataforma de Próxima Generación IMS

26/12/2011

		CONSECUENCIA									PROBABILIDAD					
N°	IDENTIFICACIÓN DEL RIESGO	CLIENTES	FINANCIERO	DURACIÓN (ACCIÓN REQUERIDA)	CALIDAD DEL SERVICIO	IMPORTANCIA ESTRATEGICA	ELEMENTOS DE RED	IMAGEN CORPORATIVA	COMPLEJIDAD	TOTAL	Posibilidad	TOTAL	SEVERIDAD DE RIESGO (INHERENTE)	SEVERIDAD DE RIESGO (CONTROLADO)	ESTATUS	RESPONSABLE
1	Ausencia de autenticacion de los UA	1	2	4	2	4	2	2	3	3	4	4	ALTA	ALTA	Abierto	CANTV
2	Ausencia de mecanismo de descarte de mensajes invalidos	2	1	3	3	3	2	1	2	2	3	3	MODERADA	MODERADA	Abierto	CANTV
3	Prestacion de servicios comprometida por falta de autenticacion de los usuarios	3	3	4	4	4	1	3	3	3	2	2	MODERADA	MODERADA	Abierto	CANTV
4	Seguridad de informacion comprometida por posibilidad de captura de paquetes en una llamada cualquiera	1	2	2	1	1	1	1	2	1	2	2	BAJA	BAJA	Abierto	CANTV
5	Seguridad comprometida debido a que los elementos de la plataforma IMS no manejan protocolos AAA	1	1	3	2	4	2	1	2	2	4	4	ALTA	ALTA	Abierto	CANTV
6	Seguridad comprometida debido a que CSCF proporciona su direccion IP	2	3	4	3	4	2	2	5	3	3	3	ALTA	ALTA	Abierto	CANTV
7	Prestacion de servicios comprometida por colapso del CSCF al recibir un alto numero de llamadas por segundo	3	3	4	3	3	2	3	5	3	2	2	MODERADA	MODERADA	Abierto	CANTV
8	Falta de manejo de algunos codec por parte del CSCF	1	1	2	2	1	1	1	2	1	3	3	BAJA	BAJA	Abierto	CANTV
9	Incapacidad de integración de elementos no Huawei para la gestión de seguridad de la red	1	1	2	1	3	1	1	3	2	2	2	BAJA	BAJA	Abierto	CANTV
										2		3	MODERADA	MODERADA		

MATRIZ DE RIESGOS CONTROLADOS
Modelo de Seguridad IMS para el Aseguramiento de Plataforma y Servicios - Fase Conceptual



#	IDENTIFICACIÓN DEL RIESGO	CONSECUENCIA	PROBABILIDAD	SEVERIDAD
1	Ausencia de autenticacion de los UA	3	4	ALTA
2	Ausencia de mecanismo de descarte de mensajes invalidos	2	3	MODERADA
3	Prestacion de servicios comprometida por falta de autenticacion de los usuarios	3	2	MODERADA
4	Seguridad de informacion comprometida por posibilidad de captura de paquetes en una llamada cualquiera	1	2	BAJA
5	Seguridad comprometida debido a que los elementos de la plataforma IMS no manejan protocolos AAA	2	4	ALTA
6	Seguridad comprometida debido a que CSCF proporciona su direccion IP	3	3	ALTA
7	Prestacion de servicios comprometida por colapso del CSCF al recibir un alto numero de llamadas por segundo	3	2	MODERADA
8	Falta de manejo de algunos codec por parte del CSCF	1	3	BAJA
9	Incapacidad de integración de elementos no Huawei para la gestión de seguridad de la red	2	2	BAJA

Gerencia General de Seguridad Integral
Gerencia de Seguridad de la Operación y Servicios
Coordinación de Riesgos de Servicios y Antifraude

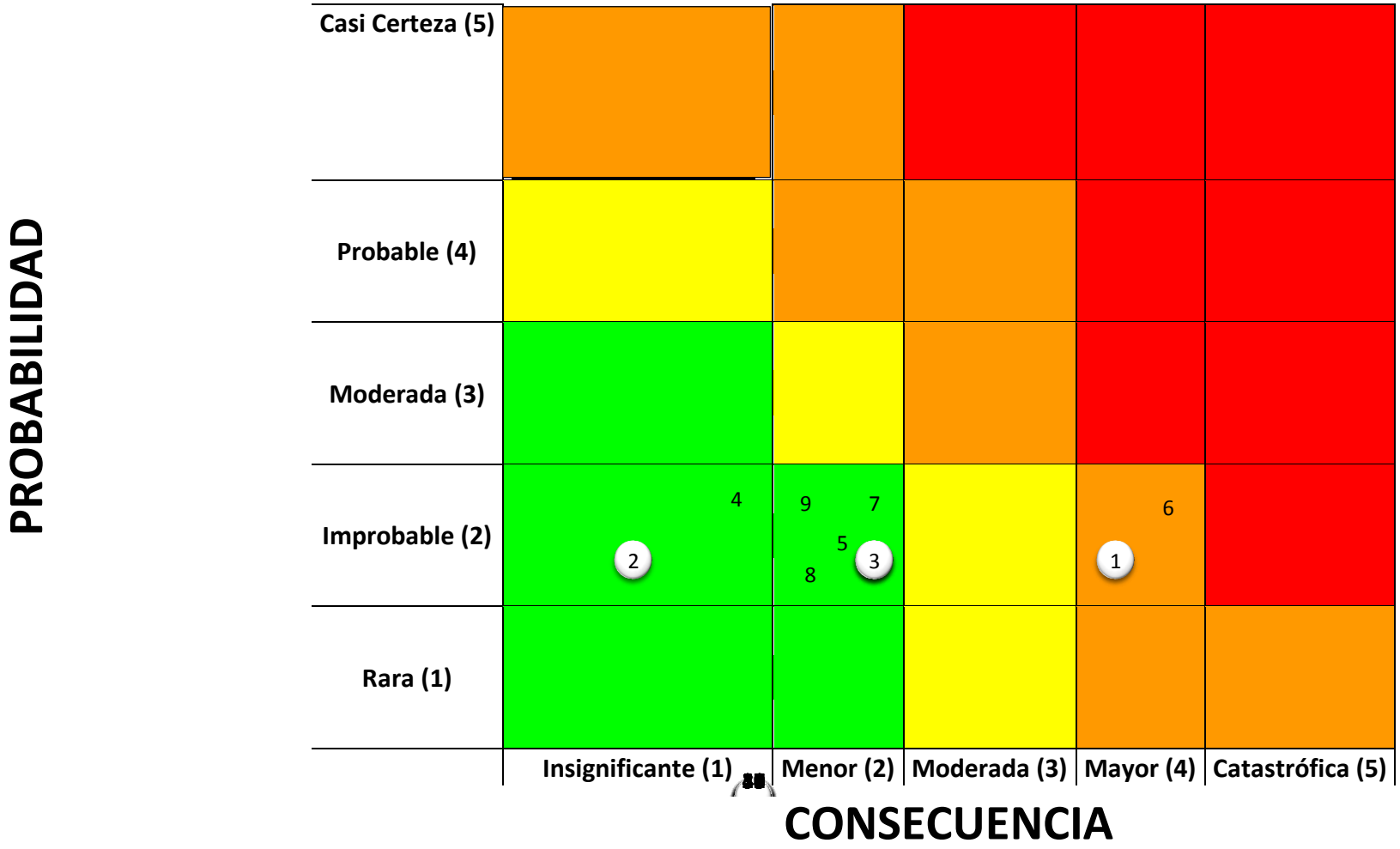
Modelo de Seguridad IMS para el Aseguramiento de Plataforma y Servicios - Fase Conceptual

Fecha: 05/01/2012

Pruebas SOS. Plataforma de Próxima Generación IMS

		CONSECUENCIA									PROBABILIDAD		26/12/2011	27/12/2011			
N°	IDENTIFICACIÓN DEL RIESGO	CLIENTES	FINANCIERO	DURACIÓN (ACCIÓN REQUERIDA)	CALIDAD DEL SERVICIO	IMPORTANCIA ESTRATEGICA	ELEMENTOS DE RED	IMAGEN CORPORATIVA	COMPLEJIDAD	TOTAL	Posibilidad	TOTAL	SEVERIDAD DE RIESGO (INHERENTE)	SEVERIDAD DE RIESGO (CONTROLADO)	SEVERIDAD DE RIESGO (TRATADO)	ESTATUS	RESPONSABLE
1	Ausencia de autenticacion de los UA	1	2	5	2	4	2	2	3	3	2	2	ALTA	ALTA	MODERADA	Abierto	CANTV
2	Ausencia de mecanismo de descarte de mensajes invalidos	1	1	2	2	1	1	1	2	1	2	2	MODERADA	MODERADA	BAJA	Abierto	CANTV
3	Prestacion de servicios comprometida por falta de autenticacion de los usuarios	1	1	4	2	4	1	2	3	2	2	2	MODERADA	MODERADA	BAJA	Abierto	CANTV
4	Seguridad de informacion comprometida por posibilidad de captura de paquetes en una llamada cualquiera	1	1	1	1	1	2	1	2	1	2	2	BAJA	BAJA	BAJA	Abierto	CANTV
5	Seguridad comprometida debido a que los elementos de la plataforma IMS no manejan protocolos AAA	1	1	4	1	4	3	1	2	2	2	2	ALTA	ALTA	BAJA	Abierto	CANTV
6	Seguridad comprometida debido a que CSCF proporciona su direccion IP	1	1	4	2	4	2	2	5	3	2	2	ALTA	ALTA	MODERADA	Abierto	CANTV
7	Prestacion de servicios comprometida por colapso del CSCF al recibir un alto numero de llamadas por segundo	2	1	2	2	3	2	2	5	2	2	2	MODERADA	MODERADA	BAJA	Abierto	CANTV
8	Falta de manejo de algunos codec por parte del CSCF	1	1	2	2	1	1	2	2	2	2	2	BAJA	BAJA	BAJA	Abierto	CANTV
9	Incapacidad de integración de elementos no Huawei para la gestión de seguridad de la red	1	1	2	1	3	1	1	3	2	2	2	BAJA	BAJA	BAJA	Abierto	CANTV
										2		2	MODERADA	MODERADA	BAJA		

MATRIZ DE RIESGOS TRATADOS
Modelo de Seguridad IMS para el Aseguramiento de Plataforma y Servicios - Fase Conceptual



#	IDENTIFICACIÓN DEL RIESGO	CONSECUENCIA	PROBABILIDAD	SEVERIDAD
1	Ausencia de autenticacion de los UA	3	2	MODERADA
2	Ausencia de mecanismo de descarte de mensajes invalidos	1	2	BAJA
3	Prestacion de servicios comprometida por falta de autenticacion de los usuarios	2	2	BAJA
4	Seguridad de informacion comprometida por posibilidad de captura de paquetes en una llamada cualquiera	1	2	BAJA
5	Seguridad comprometida debido a que los elementos de la plataforma IMS no manejan protocolos AAA	2	2	BAJA
6	Seguridad comprometida debido a que CSCF proporciona su direccion IP	3	2	MODERADA
7	Prestacion de servicios comprometida por colapso del CSCF al recibir un alto numero de llamadas por segundo	2	2	BAJA
8	Falta de manejo de algunos codec por parte del CSCF	2	2	BAJA
9	Incapacidad de integración de elementos no Huawei para la gestión de seguridad de la red	2	2	BAJA

Gerencia General de Seguridad Integral
Gerencia de Seguridad de la Operación y Servicios
Coordinación de Riesgos de Servicios y Antifraude

Modelo de Seguridad IMS para el Aseguramiento de Plataforma y Servicios - Fase Conceptual

		PUNTOS DE ATENCIÓN Y SEGUIMIENTO				
N°	**IDENTIFICACIÓN DEL RIESGO**	**Descripción**	**Acciones a ejecutar / Seguimiento**	**ESTATUS**	**RESPONSABLE**	**ORIGEN**
1	Ausencia de autenticacion de los UA	Este riesgo va referido a la suplantacion de identidad debido a la falta de autenticacion de los UA	La accion a ejecutar para la mitigacion de este riesgo es la implementacion de un sistema de autenticacion por IP, MAC address y login/password	Abierto	CANTV	PRUEBAS
2	Ausencia de mecanismo de descarte de mensajes invalidos	Este riesgo va referido a la ausencia de un mecanismo de descarte de mensajes invalidos por parte del CSCF, ya que este responde a todos los mensajes validos o no, generando consumo de recursos innecesario	La medida de mitigacion para este riesgo es la correcta configuracion del CSCF para que sean descartados los mensajes invalidos y no envia mensajes de respuesta a todos los mensajes recibidos	Abierto	CANTV	PRUEBAS
3	Prestacion de servicios comprometida por falta de autenticacion de los usuarios	Este riesgo va referido a la prestacion de los servicios comprometida debido a que dos usuarios con una misma cuenta de pueden registrar en el CSCF, deshabilitando al usuario legitimo	La accion a ejecutar para la mitigacion de este riesgo es la implementacion de un sistema de autenticacion por IP, MAC address y login/password	Abierto	CANTV	PRUEBAS
4	Seguridad de informacion comprometida por posibilidad de captura de paquetes en una llamada cualquiera	Este riesgo se refiere a la posibilidad de capturar los paquetes enviados durante una llamada cualquiera pudiendo asi acceder a la informacion contenida en ellos	La medida de mitigacion para este riesgo es la correcta configuracion del CSCF para que sean encriptados los mensajes y asi sea mas dificil obtener la informacion contenida en ellos.	Abierto	CANTV	PRUEBAS
5	Seguridad comprometida por carencia de autenticacion de los elementos que conforman la plataforma IMS	Este riesgo se refiere a la Seguridad comprometida por carencia de autenticación de los elementos que conforman la plataforma IMS por no manejar protocolos de validación AAA. Podría realizarse manipulación no autorizada o fraude interno.	La medida de mitigación de este riesgo es habilitar los protocolos AAA para la gestión remotas de equipos de la plataforma.	Abierto	CANTV	PRUEBAS
6	Seguridad comprometida debido a que CSCF proporciona su direccion IP	Este riesgo va referido a que como mecanismo de seguridad el equipo no se identifica como CSCF pero si da a conocer su dirección IP pudiendo así ser victima de ataques.	La accion a tomar para la mitigacion de este riesgo es la implementacion de una arquitectura de borde para la proteccion de todos los elementos de la capa de control de la red (SBC)	Abierto	CANTV	PRUEBAS
7	Prestacion de servicios comprometida por colapso del CSCF al recibir un alto numero de llamadas por segundo	Este riesgo va referido a que al sobrepasar las 2500 llamadas por segundo el equipo colapsa, siendo así vulnerable a ataques de degradación o negación de servicios	La accion a ejecutarse seria la implementacion de equipos con una mayor capacidad de procesamiento.	Abierto	CANTV	PRUEBAS
8	Falta de manejo de algunos codec por parte del CSCF	Este riesgo va referido a la seguridad comprometida por incorrecto funcionamiento de equipos ya que al recibir una llamada con un códec no manejado por el CSCF , este consumirá recursos intentando decodificar el paquete	La medida de mitigacion seria la correcta configuracion del CSCF para que se descarten los paquetes que contengan codecs no autorizados.	Abierto	CANTV	PRUEBAS
9	Incapacidad de integración de elementos no Huawei para la gestión de seguridad de la red	Este riesgo va referido a que es permitida la integración de elementos no Huawei en la capa de control mas no en la gestión de seguridad, lo que genera limitaciones en cuanto a sistemas de seguridad aplicables a la red.	La acción a ejecutar para la mitigación de este riesgo es el desarrollo de una capa de gestión que integre diferentes vendors, o solicitud al proveedor HUAWEI, para incluir elementos de otros vendors en su gestor.	Abierto	CANTV	PRUEBAS