NUEVAS TENDENCIAS DE SEGURIDAD INFORMÁTICA EN LAS REDES DE DATOS MÓVILES EN COLOMBIA

Ing. WILMAR LIBERTO COPETE MARIN
Cc 18.605.200

Asesor
Ing. HAROLD EMILIO CABREZA MEZA, MsC.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PEREIRA, RISARALDA
2015

Nota de aceptación:

Firma presidente del jurado

Firma del jurado

Firma del jurado

Pereira Septiembre de 2015

CONTENIDO

Pág

INTRODUCCIÓN 15

2. ASPECTOS GENERALES 17

2.1. TITULO DEL PROYECTO 17

2.2. PLANTEAMIENTO DEL PROBLEMA 17

2.2.1. Descripción del Problema. 17

2.2.2. Pregunta de Investigación. 18

2.3. JUSTIFICACIÓN. 19

2.4. OBJETIVOS. 20

2.4.1. Objetivo General. 20

2.4.2. Objetivos Específicos. 20

3. MARCO DE REFERENCIA. 21

3.1. MARCO LEGAL. 21

3.2. MARCO CONCEPTUAL. 22

3.3. MARCO TEÓRICO. 34

3.3.1. Redes Móviles. 34

3.3.2. Redes Móviles Gsm, de segunda generación. 38

3.3.3. Transmisión de Datos Gprs. 50

3.3.4. Universal Mobile Telecommunication System - UMTS, tercera generación. 58

3.3.5. Red Móvil Long Term Evolution LTE- A, 4G, cuarta generación. 66

4. DISEÑO METODOLÓGICO 72

4.1. TIPO DE INVESTIGACIÓN: 72

4.1.1. Metodología de Investigación. 72

4.1.2. Fuentes para la Recolección de Datos. 74

4.1.3. Diseño de la Investigación. 74

5. NORMAS DE SEGURIDAD INFORMÁTICA APLICADAS EN REDES MÓVILES 75

5.1. NORMAS APLICADAS. 75

5.1.2. Entidades Normalizadoras. 76

6. TENDENCIAS EN SEGURIDAD INFORMÁTICA PARA REDES MÓVILES EN EL CONTEXTO INTERNACIONAL Y NACIONAL. 114

6.1. ESTADO REDES MÓVILES. 114

6.1.1. Estado de las Redes Móviles en América Latina. 114

6.1.2. Nuevas Normas y Estándares de Seguridad Informática para Redes Móviles en el Contexto Internacional. 117

7. ANALISIS DE RESULTADOS 128

8. DEFINICIÓN DE LOS SISTEMAS DE SEGURIDAD INFORMÁTICA PARA REDES MÓVILES. 142

8.1. NORMAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA APLICABLES A LAS REDES MÓVILES. 142

8.1.1. Tipología de Red Móvil para Colombia. 142

8.1.2. Normas Legales Aplicables a la Seguridad Informática en las Redes Móviles para Colombia. 144

8.1.3. Guía para la Protección de Datos en Redes Móviles de Datos. 146

9. CONCLUSIONES 149

10. RECOMENDACIONES 151

11. BIBLIOGRAFIA 152

12. ANEXOS 159

LISTA DE TABLAS

Pág

Tabla 1. Información tercer trimestre 2014, abonados de telefonía móvil, por proveedor. 22
Tabla 2. Información tercer trimestre 2014, abonados y tráfico internet móvil. 24
Tabla 3. Información tercer trimestre 2014, penetración de abonados de internet móvil. 24
Tabla 4. Información tercer trimestre 2014, cantidad de mensajes de texto, por proveedor. 25
Tabla 5. Información tercer trimestre 2014, suscriptores personas a internet móvil, por tecnología, ingresos y tráfico. 29
Tabla 6. Información tercer trimestre 2014, suscriptores personas a internet móvil, por tecnología, ingresos y tráfico. 31
Tabla 7. Consolidado 2010- 2014, suscriptores a internet móvil, por tecnología.33
Tabla 8.Consolidado 2010- 2014 tráfico en Kb internet móvil. 33
Tabla 9. Relación entre interfaces y protocolos GSM 43
Tabla 10. Características capa física en GSM. 45
Tabla 11. Bandas mejor identificadas para el despliegue de LTE. 70
Tabla 12. Capacidad de red, procedimientos de seguridad para red IMT-2000.78
Tabla 13. Especificaciones técnicas 3GPP relativas a la seguridad. 82
Tabla 14. Ejemplo de activos, recursos e información UNI. 86
Tabla 15. Ejemplo de activos, recursos e información UNI. 87
Tabla 16. Ejemplo de activos, recursos, información de interfaces del estrato de transporte. 87
Tabla 17. Ejemplo de activos, recursos, información e interfaces del estrato de servicio. 88
Tabla 18. Ejemplo de activos, recursos, información e interfaces del estrato de servicio. 89
Tabla 19. Ejemplo de activos, recursos, información e interfaces de gestión. . 89
Tabla 20. Ejemplo de activos, recursos, información e interfaces de gestión. . 90
Tabla 21. Algunos campos básicos de un certificado de clave pública X.509.. 90
Tabla 22. Las dimensiones de seguridad que corresponden a las amenazas.95

Tabla 23. Aplicación de las dimensiones de seguridad a la capa de infraestructura en el plano de gestión. 97
Tabla 24. Aplicación de las dimensiones de seguridad a la capa de infraestructura en el plano de control. 98
Tabla 25. Aplicación de las dimensiones de seguridad a la capa de infraestructura en el plano de usuario de extremo. 99
Tabla 26. Aplicación de las dimensiones de seguridad a la capa de servicios en el plano de gestión. 99
Tabla 27. Aplicación de las dimensiones de seguridad a la capa de servicios en el plano de control. 101
Tabla 28. Aplicación de las dimensiones de seguridad a la capa de servicios en el plano de usuario de extremo. 102
Tabla 29. Aplicación de las dimensiones de seguridad a la capa de aplicaciones en el plano de gestión. 103
Tabla 30. Aplicación de las dimensiones de seguridad a la capa de aplicaciones en el plano de control. 104
Tabla 31. Aplicación de las dimensiones de seguridad a la capa de aplicaciones en el plano de usuario de extremo. 105
Tabla 32. Relación entre amenazas generales contra la seguridad y modelos.106
Tabla 33. Relación entre amenazas de seguridad en sistemas móviles y modelos. 107
Tabla 34. Relación entre los requisitos de seguridad y las amenazas generales contra la seguridad. 108
Tabla 35. Relación entre los requisitos de seguridad y las amenazas contra la seguridad en sistemas móviles. 109
Tabla 36. Ilustración de la relación entre los requisitos de seguridad y las funciones. 110
Tabla 37. Relación entre tecnologías de seguridad en comunicaciones móviles y modelo. 111
Tabla 38. Consolidado respuestas y aportes Fiscalía General de la Nación. 128
Tabla 39. Consolidado respuestas y aportes MINTIC. 129
Tabla 40. Consolidado respuestas y aportes SIC. 130
Tabla 41. Consolidado respuestas y aportes CRC. 131

Tabla 42. Consolidado respuestas y aportes AVANTEL. 132
Tabla 43. Consolidado respuestas y aportes UNE. 133
Tabla 44. Consolidado respuestas y aportes VIRGIN MOBILE..... 134
Tabla 45. Consolidado respuestas y aportes CLARO. 135
Tabla 46. Consolidado respuestas y aportes TIGO..... 136
Tabla 47. Consolidado respuestas y aportes MOVISTAR..... 137
Tabla 48. Consolidado respuestas y aportes GIDAM..... 138
Tabla 49. Consolidado respuestas y aportes GECTI. 139
Tabla 50. Consolidado respuestas y aportes GIIT. 140
Tabla 51. Consolidado respuestas y aportes 4G AMÉRICAS..... 141

LISTA DE FIGURAS

Pág

Figura 1. Cobertura de macrocelda. 35
Figura 2. Sectorización clúster de celdas. 36
Figura 3. Métodos de acceso múltiple. 37
Figura 4. Traspaso MS a BTS 38
Figura 5. Dispositivos descriptivos red GSM. 39
Figura 6. Arquitectura red móvil GSM. 40
Figura 7. Esquema de interfaces en el estándar GSM. 42
Figura 8. Protocolos asociados a cada interfaz. 42
Figura 9. Pila de protocolo en la estación base y el subsistema de radio. 44
Figura 10. Arquitectura GSM, con sus elementos de operación. 47
Figura 11. Arquitectura red móvil 2.5G 49
Figura 12. Transmisión de datos GPRS. 51
Figura 13. Pila de protocolos en el plano de transmisión GPRS. 52
Figura 14. Pila de protocolos en el plano de señalización GPRS 53
Figura 15. Dispositivos descriptivos red GPRS. 54
Figura 16. Interfaces en la red GPRS. 55
Figura 17. Transmisión de datos EDGE 56
Figura 18. Pila de protocolos, comparativa GPRS/ EDGE. 57
Figura 19. Cambios en los dispositivos descriptivos de la red GPRS a EDGE. 58
Figura 20. Arquitectura red móvil UMTS. 60
Figura 21. Protocolos de la red de transporte para la interfaz Iub. 62
Figura 22. Protocolos de la red de transporte para la interfaz Iur 62
Figura 23. Protocolos de la red de transporte para la interfaz Iu- CS 63
Figura 24. Protocolos de la red de transporte para la interfaz Iu- PS. 63
Figura 25. Dispositivos descriptivos red UMTS. 64
Figura 26. Arquitectura de red LTE. 66
Figura 27. Pila de protocoles interfaz de radio E-UTRAN. 67
Figura 28. Pila de protocolos del plano de usuario en E-UTRAN. 68
Figura 29. Pila de protocolos del plano de control en E-UTRAN. 69
Figura 30. Comparativa de dispositivos descriptivos de red LTE con red UMTS. 69

Figura 31. Interfaces físicas para un miembro de la familia IMT 2000. 79
Figura 32. Servicio de gestión de la seguridad IMT-2000. 84
Figura 33. Arquitectura de seguridad de ITU-T X.805. 85
Figura 34. Marco genérico de claves para la seguridad de la movilidad en las NGN. 93
Figura 35. Procedimiento genérico de autenticación. 94
Figura 36. Arquitectura de seguridad representada en un cuadro de combinación, capa y plano. 96
Figura 37. Modelo de pasarela de comunicación móvil de extremo a extremo entre un usuario móvil y el ASP. 106
Figura 38. Modelo de pasarela de sistemas móviles seguros basados en PKI.113
Figura 39. Predicción del Cisco VNI América Latina para 2019. 115
Figura 40. Conexiones totales por generación de tecnología. 117
Figura 41. Modelo de confianza de 3 lados o esquinas. 119
Figura 42. Modelo de confianza de 4 lados o esquinas. 119
Figura 43. Receptores mejorados para rendimiento LTE-A, cancelación interferencia. 123
Figura 44. Nuevas propuestas de LTE-A. 124
Figura 45. LTE en América Latina y el Caribe. 125
Figura 46. Conexiones de banda ancha móvil y fija en mercados seleccionados.126
Figura 47. Tasas de adopción de smartphone. 127
Figura 48. Prototipo de redes 2G y 3G utilizadas en Colombia. 143
Figura 49. Prototipo de redes 4G utilizadas en Colombia. 144
Figura 50. Tendencias sobre seguridad informática en las redes móviles para Colombia durante los años 2015 – 2016. 145

LISTA DE ANEXOS

Pág

Anexo 1. Cuadro SPOA, consolidado delitos informáticos ley 1273 de 2009, desde el año 2010-2014 en redes de telecomunicaciones, Fiscalía General de la Nación. 159
Anexo 2. Legislación Informática de República de Colombia..... 160
Anexo 3. Respuesta Fiscalia General de la Nación 161
Anexo 4. Respuesta Ministerio de Tecnologías de la Información y Comunicación de Colombia- MinTic..... 164
Anexo 5. Respuesta Superintendencia de Industria Comercio. 166
Anexo 6.Respuesta Comisión de Regulación Comunicaciones- CRC. 167
Anexo 7. Respuesta AVANTEL..... 168
Anexo 8. Respuesta UNE 169
Anexo 9. Respuesta VIRGIN MOBILE. 170
Anexo 10. Respuesta CLARO. 173
Anexo 11. Respuesta Grupo De Investigación en Desarrollo Aplicaciones Móviles de la Universidad de Magdalena. 174
Anexo 12. Respuesta Grupo de Investigación en Comercio Electrónico, Telecomunicaciones E Informática- Gecti. Universidad de Los Andes 176
Anexo 13. Respuesta Grupo de Investigación de Informática y Telecomunicaciones- Universidad Ecesi. 177
Anexo 14. Respuesta 4G Américas. 178

RESUMEN

La presente investigación se presenta con un contenido de doce capítulos, que exploran las tendencias, nuevas tecnologías, estándares en seguridad informática aplicadas en las redes móviles para Colombia. Para llevar a cabo la misma, hace una revisión de los estándares implementados en las redes móviles, pasado por el contexto internacional, especialmente en Latinoamérica; ubicándose luego en Colombia.

De manera específica, en el capítulo 1 se hace la introducción a la investigación, en el capítulo 2 se evalúan los aspectos generales de la investigación, su objetivo general, basado en sus objetivos específicos, que avala el capítulo 3, que presenta el marco de referencia, donde se encuentra los conceptos teóricos de la seguridad informática aplicada en las redes móviles, referidas en las diferentes generaciones de telefonía móvil a nivel internacional y nacional, teniendo en cuenta a las Entidades encargadas de la estructuración de las normas técnicas y estándares. A continuación se desarrolla el marco contextual, en base a cifras y reportes del Ministerio de Tecnologías de la Información y las Comunicaciones para Colombia, durante la última vigencia de 2014, relacionado con la cantidad de abonados de los servicios móviles en el país, incluidos los de voz y datos, y la relación con las normatividad aplicada en el país, en su marco legal.

En el capítulo 4, se presenta el diseño metodológico de la investigación, teniendo en cuenta los pasos que se desarrollaron, se recolectan los datos, desde diferentes actores del medio, como las entidades de control y vigilancia, los operadores móviles y los consultores y expertos en el área.

Para el capítulo 5, se abordan las normas de seguridad informática en el contexto nacional e internacional, de allí se desprende el capítulo 6, acerca de las tendencias en seguridad informática en el contexto nacional e internacional. En el capítulo 7, aplicado el diseño metodológico, se presenta el respectivo análisis de resultados de la información recolectada tanto a las Entidades del Estado Colombiano, como a los operadores del servicio móvil y expertos del tema.

En el capítulo 8, se definen las normas en seguridad informática que se avecinan para el país, teniendo en cuenta, la agenda regulatoria en comunicaciones, y los estudios de las redes móviles actuales del país

En el capítulo 9, se entregan las conclusiones de la investigación, seguidamente del capítulo 10, que contiene las recomendaciones finales.
Seguido del capítulo 11, con la bibliografía consultada y finalmente el capítulo 12, con los anexos de la investigación.

ABSTRACT

This research is presented containing twelve chapters that explore the trends, new technologies, computer security standards applied in mobile networks for Colombia. To perform it, it makes UAN review of the standards implemented in mobile networks, passed by the international context, especially in Latin America; then being located in Colombia.

So specifies, in chapter 1 introduction to research done in chapter 2 general aspects of research, overall objective, based on their specific objectives, which guarantees Chapter 3, which presents the framework of evaluating reference, where the theoretical concepts of information security applied in mobile networks, based on the different generations of mobile telephony at international and national level is, considering the Entities structuring of technical rules and standards. Then the contextual framework is developed, based on figures and reports the Ministry of Information Technology and Communications to Colombia, during the last term of 2014, related to the number of subscribers of mobile services in the country, including voice and data, and the relationship with the regulations applied in the country in its legal framework.

In Chapter 4, the methodological design of the research is presented, taking into account the phases were developed, data are collected from different actors in the environment, such as control and monitoring bodies, mobile operators and consultants and experts in the area.

For Chapter 5, information security standards at the national and international context, there Chapter 6, about trends in computer security at the national and international context follows addresses. In Chapter 7, applied study design, conduct an analysis of results is presented.

In Chapter 8, computer security standards ahead for the country, taking into account the regulatory agenda in communications, and studies of existing mobile networks in the country are defined.

In Chapter 9, the conclusions of the investigation are given, then the chapter 10, which contains the final recommendations.

Chapter 11 followed with the literature and finally chapter 12, with the accompanying research.

INTRODUCCIÓN

La seguridad informática, ha cobrado relevancia en el mundo tecnológico, legal, empresarial y de entretenimiento actual, toda vez que su estudio e implementación favorece el uso general de estos por parte de los usuarios, buscando minimizar los riesgos de afectación a la información contenida en los diferentes medios físicos y electrónicos en los que la humanidad ha almacenado sus datos. Este paradigma de proteger y desproteger datos nació con el hombre mismo, en el afán de tener información secreta, privilegiada, confidencial, que sirviera de tener ventaja en la guerra, en los negocios, en la industrialización de los campos y las ciudades.

Primero fueron los documentos físicos que viajaban de un lado a otro, transportados por un emisario, quien llevada los mensajes, guardado en cilindros metálicos, que solo se podían abrir si se conocía la clave dada por el emisor del mensaje, y si no era la llave la correcta, activándose un mecanismo que liberaba líquidos, dañando el manuscrito impreso en los documentos. Ahora los mensajes de voz, texto e imagen, que viajan por dispositivos electrónicos, como computadores, tabletas, teléfonos móviles, utilizando antenas de transmisión, switches, routers, modems, usando un canal de transmisión, internet, como medio de interconexión global, pero que, aunque los mecanismos de llevar el mensaje de un lado a otro han evolucionado, de igual manera lo han hecho los intentos por violentar las claves y la codificación para conocer el contenido de estos datos y hacerlos públicos o pedir recompensas a cambio de no divulgar la misma.

Ahora bien, con el auge de la miniaturización de los dispositivos electrónicos de comunicación, como los teléfonos móviles inteligentes “Smartphone”, tabletas, que integran el servicio de llamadas, con el video, imagen, conexión permanente a internet, consulta del correo electrónico, servicios bancarios, de

salud, con prestaciones suficientes de conexión, se ha desplegado otro universo de explotación de datos tanto para los usuarios como para los atacantes que quieren saber la información que transmiten sus víctimas y poder usarla a favor propio.

El desarrollo de esta investigación pretende obtener información oportuna acerca de la apropiación de la seguridad informática aplicada en las redes de datos móviles usadas en Colombia, donde se evidencia el manejo dado por las Entidades que norman el proceso, las que lo vigilan; de igual manera, las Empresas que explotan estos servicios de telecomunicaciones, con el fin de dar a conocer a los usuarios del servicio, las condiciones evolutivas y próximas en implementarse en el país.

2. ASPECTOS GENERALES

2.1. TITULO DEL PROYECTO

Nuevas tendencias de seguridad informática en las redes de datos móviles en Colombia.

2.2. PLANTEAMIENTO DEL PROBLEMA

2.2.1. Descripción del Problema.

La forma de comunicación de los seres humanos ha evolucionado, desde los mensajes de persona a persona, en inscripciones en madera, en piedra, en papel, digital, enviados de un lugar a otro, usando medios físicos como las mismas personas, animal, fluvial, por aire, por tierra, hasta llegar a lo que conocemos en la actualidad, que es la red de conexión universal, llamada internet. Para lograr dicha comunicación, se han desarrollado dispositivos desde el criptograma hasta los computadores, haciendo subdivisión en la computación móvil, donde aparecen los teléfonos móviles, tabletas, computadores portátiles que a su vez han repercutido en la evolución de las redes donde estos elementos se pueden comunicar, logrando el salto de las redes fijas cableadas a redes móviles.

Sin embargo, faltaba el elemento que permite confirmar y asegurar esa transmisión de información de una sitio a otro, de una persona a otra, de un mensaje a otro, y ese es el elemento de la seguridad informática, como eje fundamental de la confidencialidad, integridad y disponibilidad de los datos.

Este elemento integrador ha sido de conocimiento de los gobiernos de los países, las empresas de telecomunicaciones, organizaciones internacionales, universidades y la academia, de donde han informado a la comunidad en general acerca de las precauciones en el tratamiento de la información, y que

se debe tener en cuenta para evitar que la delincuencia digital, haga uso indebido de la información en las redes de computadores fijas.

Ahora bien, ante el desarrollo en las comunicaciones móviles y en consecuencia de las redes móviles, los ciudadanos han utilizado dichos elementos para el desarrollo de su empresa, vida familiar y personal, pero los conocimientos acerca de cómo funcionan dichas redes, quien protege su información, bajo qué características técnicas y como ellos mismos pueden protegerse, no se encuentran divulgados ampliamente.

A la par del desarrollo de las redes móviles, ha evolucionado la delincuencia digital, para contrarrestar los efectos en los datos de los usuarios, se han creado leyes y normas que buscan castigar a la mencionada delincuencia, sin embargo, dichas normas no son divulgadas de manera amplia y los ciudadanos no conocen como proteger sus datos y tampoco como los protege la legislación ante una posible vulneración de sus derechos digitales.

2.2.2. Pregunta de Investigación.

¿Cómo mejorar la seguridad informática en las redes móviles en Colombia?

2.3. JUSTIFICACIÓN.

Las comunicaciones digitales han tomado el control de la vida social, personal, académica y empresarial de las personas, en donde comparten gran cantidad de datos, tipificados en imágenes, archivos de texto, mensajes, audio y video.

En el afán por poder interactuar con todos estos aspectos de la vida que influyen en el desarrollo de la misma, los usuarios se han visto en la necesidad de usar diversos dispositivos electrónicos, donde primero fue el computador personal, luego el computador portátil, más recientemente a las tabletas, y a la par con ello los teléfonos inteligentes o Smartphone, en donde se pueden concentrar las conexiones a correos personales, empresariales, redes sociales de amigos y de profesionales, almacenamiento de archivos de audio, video e imagen, mediante las redes de datos móviles que prestan el servicio en el país.

Lo anterior quiere decir, que la carga de prestaciones y de gestión de usuario, datos y seguridad informática recae en estas redes móviles y en los dispositivos usados, pero lo critico de la anterior afirmación, radica en que los usuarios típicos no saben cómo protegerse y como enfrentar posibles amenazas que están vigentes en las redes de datos como la ingeniería social, suplantación de identidad, robo de datos. Es allí donde esta investigación ofrecerá herramientas de análisis, de mejores prácticas y de condiciones básicas para las transacciones de información a cualquier nivel.

Por esto se hace necesario el estudio mediante la investigación de las nuevas tendencias en cuanto a la seguridad informática en las redes móviles en el país, y que sean de conocimiento tanto por los usuarios cotidianos de los servicios telemáticos, como para las empresas del sector industrial y del comercio, protegiendo el activo más valioso, que es la información contenida en datos.

2.4. OBJETIVOS.

2.4.1. Objetivo General.

Identificar las nuevas tendencias, normas, protocolos, estándares de seguridad informática aplicados a las redes de datos móviles en Colombia.

2.4.2. Objetivos Específicos.

Ahondar en los protocolos, normas, tendencias y estándares de seguridad informática usados para la transmisión de datos en las redes móviles en Colombia.

Indagar en las compañías operadoras de telecomunicaciones la aplicación de protocolos y normas de seguridad en las redes móviles de acuerdo al número de incidentes de seguridad informática reportados a las autoridades administrativas y judiciales.

Presentar las tendencias de seguridad informática aplicadas a las redes móviles de acuerdo a la tecnología actual de los operadores de redes móviles en Colombia.

3. MARCO DE REFERENCIA.

3.1. MARCO LEGAL.

Para el caso de Colombia, se aprobó la Ley 37 de 1994, encargada de distribuir el país en zonas para la operación de los primeros operadores de telefonía móvil.

Para ese mismo año, la Ley 170 de 1994, donde se busca que se eliminen los obstáculos comerciales y de competencia en la implementación de redes y servicios basados en telecomunicaciones, como es el caso de las redes móviles de datos.

De igual manera, entro en vigencia la Ley 1341 de 2009, allí se hace evidente que para relacionar y consolidar las relaciones de los ciudadanos y las Instituciones, es necesario el acceso y uso eficientes de las Tecnologías de la Información y Comunicación (TIC), además de desarrollar la infraestructura física existente en el país, desarrollo de contenidos multimediales y aplicaciones, la protección de los datos del usuario, buscando así mejorar la competitividad de Colombia.

Por el lado la seguridad informática, está la Ley 1273 de 2009, como el primer intento por castigar los abusos y delitos informáticos en el país, buscando los tres pilares básicos de la información, que sea confidencial, que sea integral y que esté disponible, la ley 1273 quedó como un artículo que se incluyó en el Código Penal Colombiano (Art. 269).

Sin dejar de lado la protección de los datos, la Ley 1581 de 2012, busca ir más allá de solo castigar a los infractores de la Ley 1273, la cual está más enfocada en proteger los datos personales de los usuarios de la manipulación ilegal de

datos como correo electrónico, identificación, dirección, nombre y demás información que puede ser usado con fines diferentes, especialmente de los delincuentes informáticos[1]. En el año 2013, se reglamenta parte de la ley, con el Decreto 1377, el cual adiciona al tema de la manipulación de los datos y que la misma debe estar autorizada por el titular de la información, la obligación de establecer cláusulas para la transmisiones y transferencias de datos, que el usuario conozca quien está interesado en su información personal y que se defina el tratamiento y finalidad de los mismos, estableciendo formatos de autorización para ello[2].

3.2. MARCO CONCEPTUAL.

El dato inicial es sorprendente: El número de líneas activas es de 53.583.664, según informe del tercer trimestre de 2014 del Ministerio TIC, lo que significa que esta cantidad, puede ser potencialmente usada no solo como línea para voz, sino para uso de datos[3]. Eso de vital importancia mencionar que para el periodo 2010-2014, se han presentado 104 delitos informáticos relacionados con redes de telecomunicaciones, según lo ha informado la Fiscalía General de la Nación, según anexo 1.

Tabla 1.Información tercer trimestre 2014, abonados de telefonía móvil, por proveedor.

INFORMACIÓN 3 TRIMESTRE 2014 ABONADOS DE TELEFONÍA MÓVIL					
PROVEEDOR	ABONADOS EN SERVICIO	ABONADOS EN PREPAGO	ABONADOS EN POSPAGO	LÍNEAS ACTIVADAS	LÍNEAS RETIRADAS

[1]Tomado de: http://colombiadigital.net/publicaciones_ccd/anexos/certicamara_proteccion_datos_ago28.pdf

[2]Tomado de: http://www.redipd.org/noticias_todas/2013/novedades/common/DECRETO1377_27062013.pdf

[3]Tomado de http://colombiatic.mintic.gov.co/602/articles-3853_archivo_pdf.pdf

ALMACENES EXITO INVERSIONES S.A.S.	273.818	225.573	-	50.237	8.510
AVANTEL S.A.S.	245.229	39.057	173.410	50.025	13.570
COLOMBIA MOVIL S.A. E.S.P. *	8.692.171	6.944.223	1.413.261	1.824.486	1.452.400
COLOMBIA TELECOMUNICACIONES S.A. ESP *	12.581.553	8.982.442	3.268.298	1.431.754	1.450.387
COMUNICACION CELULAR S A COMCEL S.A *	29.290.815	23.276.224	5.815.472	3.518.175	3.336.383
EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. ESP.	-	34.684	-	-	-
UFF MOVIL SAS	415.300	416.309	-	68.092	69.101
UNE EPM TELECOMUNICACIONES S.A. E.S.P. - UNE EPM TELCO S.A.	380.015	104.444	271.111	35.738	19.955
VIRGIN MOBILE COLOMBIA S.A.S.	1.704.763	1.235.298	-	486.214	71.082
TOTAL NACIONAL	**53.583.664**	**41.258.254**	**10.941.552**	**7.464.721**	**6.421.388**

Fuente: http://colombiatic.mintic.gov.co/602/w3-article-8127.html

Un dato importante, el operador UNE ha iniciado en junio 2012 su oferta de servicios de datos soportados en la tecnología LTE[4].

Es decir, que en Colombia, el consumo de datos por parte de los usuarios va en crecimiento toda vez, que las compañías ofrecen diversos servicios y planes cada vez más ajustados a las necesidades de usuarios de todos los estratos

[4]Tomado de http://www.evaluamos.com/2006/PDF/borrador2resolucion4G.pdf

sociales y que la cantidad de abonados, hipotéticamente, ofrecería capacidad de servicios de datos.

En el marco de la investigación, se han adelantado indagaciones de la información acerca del estado de nuestro país frente al uso de los estándares de conectividad a redes móviles, y se han encontrado los siguientes datos:

Tabla 2. Información tercer trimestre 2014, abonados y tráfico internet móvil.

INFORMACIÓN 3 TRIMESTRE 2014 ABONADOS Y TRÁFICO DE INTERNET MÓVIL - DEMANDA		
TECNOLOGÍA	**TOTAL ABONADOS**	**TRÁFICO (KB)**
2G	540.352	20.196.080.028.145
3G	3.814.806	
4G	808.762	
TOTAL NACIONAL	**5.163.920**	**20.196.080.028.145**

Fuente: http://colombiatic.mintic.gov.co/602/w3-article-8127.html

En lo que concierne al último año, y el despliegue de la redes 4G, se detecta pocos abonados comparado con las redes 3G, pero el uso de datos considerablemente amplio, estos identificados en el consumo en Kb. En este punto se debe tener en cuenta, el tipo de dispositivos que no son homologables con este tipo de red, obliga a un cambio tecnológico por parte del usuario:

Tabla 3. Información tercer trimestre 2014, penetración de abonados de internet móvil.

INFORMACIÓN 3 TRIMESTRE 2014 PENETRACIÓN ABONADOS DE INTERNET MÓVIL - SUSCRIPCIÓN, POR PROVEEDOR	
PROVEEDORES	**No. SUSCRIPTORES**
AVANTEL S.A.S.	859
COLOMBIA MOVIL S.A. E.S.P.	897.149
COLOMBIA TELECOMUNICACIONES S.A. ESP	1.831.646
COMUNICACION CELULAR S A COMCEL S A	2.146.298
EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. ESP.	16.857

UNE EPM TELECOMUNICACIONES S.A. E.S.P. - UNE EPM TELCO S.A.	271.111
TOTAL NACIONAL	**5.163.920**

Fuente: http://colombiatic.mintic.gov.co/602/w3-article-8127.html

Para el caso de los nuevos abonados en uso de internet móvil, teniendo en cuenta los proveedores, se nota la marcada ventaja de uno de ellos, pero no se logra identificar con cual red móvil se abonan o hacen uso los usuarios:

Tabla 4. Información tercer trimestre 2014, cantidad de mensajes de texto, por proveedor.

INFORMACIÓN 3 TRIMESTRE 2014 - CANTIDAD DE MENSAJES DE TELEFONÍA MÓVIL, POR PROVEEDOR			
PROVEEDORES	**TIPO DE MENSAJE**	**RED DESTINO**	**CANTIDAD DE MENSAJES**
ALMACENES EXITO INVERSIONES S.A.S.	SMS	COLOMBIA MOVIL S.A. E.S.P.	82.123
ALMACENES EXITO INVERSIONES S.A.S.	SMS	VIRGIN MOBILE COLOMBIA S.A.S.	7.128
ALMACENES EXITO INVERSIONES S.A.S.	SMS	TPBC	9.830
ALMACENES EXITO INVERSIONES S.A.S.	SMS	UNE EPM TELECOMUNICACIONES S.A. E.S.P.	447
ALMACENES EXITO INVERSIONES S.A.S.	SMS	EMPRESA DE TELECOMUNICACIONES DE BOGOTA S.A. ESP.	1.662
ALMACENES EXITO INVERSIONES S.A.S.	SMS	UFF MOVIL S.A.S.	2.267
ALMACENES EXITO INVERSIONES S.A.S.	SMS	COMUNICACION CELULAR S A COMCEL S A	226.941
ALMACENES EXITO INVERSIONES S.A.S.	SMS	AVANTEL S.A.S.	643
ALMACENES EXITO INVERSIONES S.A.S.	SMS	COLOMBIA TELECOMUNICACIONES S.A. ESP	59.237
ALMACENES EXITO	SMS	ALMACENES EXITO	95.772

INVERSIONES S.A.S.		INVERSIONES S.A.S.	
AVANTEL S.A.S.	SMS	ALMACENES EXITO INVERSIONES S.A.S.	262
AVANTEL S.A.S.	SMS	VIRGIN MOBILE COLOMBIA S.A.S.	5.878
AVANTEL S.A.S.	SMS	COLOMBIA MOVIL S.A. E.S.P.	105.058
AVANTEL S.A.S.	SMS	EMPRESA DE TELECOMUNICACIONES DE BOGOTA S.A. ESP.	3.908
AVANTEL S.A.S.	SMS	COMUNICACION CELULAR S A COMCEL S A	564.527
AVANTEL S.A.S.	SMS	COLOMBIA TELECOMUNICACIONES S.A. ESP	245.103
AVANTEL S.A.S.	SMS	AVANTEL S.A.S.	109.090
AVANTEL S.A.S.	SMS	UNE EPM TELECOMUNICACIONES S.A. E.S.P.	114
AVANTEL S.A.S.	SMS	UFF MOVIL S.A.S.	2.262
COLOMBIA MOVIL S.A. E.S.P.	MMS	COLOMBIA MOVIL S.A. E.S.P.	270.503
COLOMBIA MOVIL S.A. E.S.P.	SMS	UFF MOVIL S.A.S.	8.665
COLOMBIA MOVIL S.A. E.S.P.	SMS	UNE EPM TELECOMUNICACIONES S.A. E.S.P.	104
COLOMBIA MOVIL S.A. E.S.P.	SMS	EMPRESA DE TELECOMUNICACIONES DE BOGOTA S.A. ESP.	9.681
COLOMBIA MOVIL S.A. E.S.P.	SMS	COMUNICACION CELULAR S A COMCEL S A	16.377.805
COLOMBIA MOVIL S.A. E.S.P.	SMS	COLOMBIA MOVIL S.A. E.S.P.	505.063.969
COLOMBIA MOVIL S.A. E.S.P.	SMS	TPBC	94.568
COLOMBIA MOVIL S.A. E.S.P.	SMS	AVANTEL S.A.S.	153.223
COLOMBIA MOVIL S.A. E.S.P.	SMS	ALMACENES EXITO INVERSIONES S.A.S.	8.209
COLOMBIA MOVIL S.A. E.S.P.	SMS	COLOMBIA TELECOMUNICACIONES S.A. ESP	5.681.097
COLOMBIA TELECOMUNICACIONES S.A. ESP	SMS	COLOMBIA TELECOMUNICACIONES S.A. ESP	325.781.745
COLOMBIA TELECOMUNICACIONES S.A. ESP	SMS	AVANTEL S.A.S.	97.107

COLOMBIA TELECOMUNICACIONES S.A. ESP	MMS	COLOMBIA TELECOMUNICACIONES S.A. ESP	582.601
COLOMBIA TELECOMUNICACIONES S.A. ESP	SMS	COMUNICACION CELULAR S A COMCEL S A	35.794.886
COLOMBIA TELECOMUNICACIONES S.A. ESP	SMS	COLOMBIA MOVIL S.A. E.S.P.	6.717.622
COLOMBIA TELECOMUNICACIONES S.A. ESP	SMS	UFF MOVIL S.A.S.	758.733
COMUNICACION CELULAR S A COMCEL S A	SMS	COLOMBIA TELECOMUNICACIONES S.A. ESP	28.667.810
COMUNICACION CELULAR S A COMCEL S A	SMS	TPBC	155.592
COMUNICACION CELULAR S A COMCEL S A	SMS	UFF MOVIL S.A.S.	501.641
COMUNICACION CELULAR S A COMCEL S A	SMS	AVANTEL S.A.S.	254.397
COMUNICACION CELULAR S A COMCEL S A	SMS	COLOMBIA MOVIL S.A. E.S.P.	19.665.722
COMUNICACION CELULAR S A COMCEL S A	SMS	COMUNICACION CELULAR S A COMCEL S A	675.868.180
COMUNICACION CELULAR S A COMCEL S A	MMS	COMUNICACION CELULAR S A COMCEL S A	1.989.436
COMUNICACION CELULAR S A COMCEL S A	SMS	UNE EPM TELECOMUNICACIONES S.A. E.S.P.	33.659
EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. ESP.	SMS	AVANTEL S.A.S.	-
EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. ESP.	SMS	COMUNICACION CELULAR S A COMCEL S A	-
EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. ESP.	SMS	COLOMBIA MOVIL S.A. E.S.P.	-
EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. ESP.	SMS	VIRGIN MOBILE COLOMBIA S.A.S.	-
EMPRESA DE	SMS	EMPRESA DE	-

TELECOMUNICACIONES DE BOGOTÁ S.A. ESP.		TELECOMUNICACIONES DE BOGOTA S.A. ESP.	
EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. ESP.	SMS	COLOMBIA TELECOMUNICACIONES S.A. ESP	-
EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. ESP.	SMS	ALMACENES EXITO INVERSIONES S.A.S.	-
EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. ESP.	SMS	UNE EPM TELECOMUNICACIONES S.A. E.S.P.	-
EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. ESP.	SMS	UFF MOVIL S.A.S.	-
UFF MOVIL SAS	SMS	AVANTEL S.A.S.	951
UFF MOVIL SAS	SMS	COMUNICACION CELULAR S A COMCEL S A	531.424
UFF MOVIL SAS	SMS	COLOMBIA MOVIL S.A. E.S.P.	180.292
UFF MOVIL SAS	SMS	UFF MOVIL S.A.S.	94.256
UFF MOVIL SAS	SMS	COLOMBIA TELECOMUNICACIONES S.A. ESP	177.076
UNE EPM TELECOMUNICACIONES S.A. E.S.P. - UNE EPM TELCO S.A.	SMS	EMPRESA DE TELECOMUNICACIONES DE BOGOTA S.A. ESP.	1
UNE EPM TELECOMUNICACIONES S.A. E.S.P. - UNE EPM TELCO S.A.	SMS	UNE EPM TELECOMUNICACIONES S.A. E.S.P.	88.831
UNE EPM TELECOMUNICACIONES S.A. E.S.P. - UNE EPM TELCO S.A.	SMS	TPBC	21.421
UNE EPM TELECOMUNICACIONES S.A. E.S.P. - UNE EPM TELCO S.A.	SMS	COLOMBIA MOVIL S.A. E.S.P.	16.219
UNE EPM TELECOMUNICACIONES S.A. E.S.P. - UNE EPM TELCO S.A.	SMS	COLOMBIA TELECOMUNICACIONES S.A. ESP	8.274
UNE EPM TELECOMUNICACIONES S.A. E.S.P. - UNE EPM TELCO S.A.	SMS	ALMACENES EXITO INVERSIONES S.A.S.	229
UNE EPM TELECOMUNICACIONES S.A. E.S.P. - UNE EPM TELCO S.A.	SMS	AVANTEL S.A.S.	40

UNE EPM TELECOMUNICACIONES S.A. E.S.P. - UNE EPM TELCO S.A.	SMS	COMUNICACION CELULAR S A COMCEL S A	26.179
UNE EPM TELECOMUNICACIONES S.A. E.S.P. - UNE EPM TELCO S.A.	SMS	UFF MOVIL S.A.S.	431
UNE EPM TELECOMUNICACIONES S.A. E.S.P. - UNE EPM TELCO S.A.	SMS	VIRGIN MOBILE COLOMBIA S.A.S.	1.099
VIRGIN MOBILE COLOMBIA S.A.S.	SMS	COLOMBIA TELECOMUNICACIONES S.A. ESP	20.461.987
VIRGIN MOBILE COLOMBIA S.A.S.	SMS	COMUNICACION CELULAR S A COMCEL S A	5.945
VIRGIN MOBILE COLOMBIA S.A.S.	SMS	COLOMBIA MOVIL S.A. E.S.P.	6.210
TOTAL NACIONAL			**1.647.680.072**

Fuente: http://colombiatic.mintic.gov.co/602/w3-article-8127.html

La cifra de casi dos millones de mensajes de texto de la tabla 4, genera una pregunta acerca del contenido de los mismos, y la sensibilidad de los mismos, donde se envían números de cédula, números de cuentas de correo con clave incluida, datos personales, número de cuentas bancarias, y demás datos que son vitales para los usuarios, pero que en este cuadro no queda evidencia acerca de la forma de proteger el contenido de los mismos:

Tabla 5. Información tercer trimestre 2014, suscriptores personas a internet móvil, por tecnología, ingresos y tráfico.

INFORMACIÓN 3 TRIMESTRE 2014 SUSCRIPTORES PERSONAS A INTERNET MOVIL, POR TECNOLOGIA, INGRESOS Y TRÁFICO						
PROVEEDORES	**TIPO DE PLAN**	**TERMINAL**	**TECNOLOGÍA**	**No. SUSCRIPTORES**	**INGRESOS (pesos Colombianos)**	**TRÁFICO (KB)**
AVANTEL S.A.S.	EMPRESAS	TELÉFONO MÓVIL	2G	859	$ 27.799.136	43.270.683

COLOMBIA MOVIL S.A. E.S.P.	PERSONAS	DATA CARD	2G	-	$ 7.074.870.710	3.579.883.014.719
COLOMBIA MOVIL S.A. E.S.P.	PERSONAS	DATA CARD	3G	123.901		
COLOMBIA MOVIL S.A. E.S.P.	PERSONAS	DATA CARD	4G	2.673		
COLOMBIA MOVIL S.A. E.S.P.	PERSONAS	TELÉFONO MÓVIL	2G	18.867	$ 82.512.834.922	
COLOMBIA MOVIL S.A. E.S.P.	PERSONAS	TELÉFONO MÓVIL	3G	590.090		
COLOMBIA MOVIL S.A. E.S.P.	PERSONAS	TELÉFONO MÓVIL	4G	123.803		
COLOMBIA TELECOMUNICACIONES S.A. ESP	PERSONAS	DATA CARD	2G	7.882	$ 6.696.245.298	4.836.973.901.008
COLOMBIA TELECOMUNICACIONES S.A. ESP	PERSONAS	DATA CARD	3G	131.091		
COLOMBIA TELECOMUNICACIONES S.A. ESP	PERSONAS	DATA CARD	4G	12.823		
COLOMBIA TELECOMUNICACIONES S.A. ESP	PERSONAS	TELÉFONO MÓVIL	2G	64.810	$ 81.309.476.335	
COLOMBIA TELECOMUNICACIONES S.A. ESP	PERSONAS	TELÉFONO MÓVIL	3G	719.367		
COLOMBIA TELECOMUNICACIONES S.A. ESP	PERSONAS	TELÉFONO MÓVIL	4G	152.903		
COMUNICACION CELULAR S A COMCEL S A	PERSONAS	DATA CARD	2G	27.718	$ 111.509.044.498	8.471.328.451.777
COMUNICACION CELULAR S A COMCEL S A	PERSONAS	DATA CARD	3G	775.395		
COMUNICACION CELULAR S A COMCEL S A	PERSONAS	DATA CARD	4G	78.873		
COMUNICACION	PERSON	TELÉFO	2G	27.315	$	

CELULAR S A COMCEL S A	AS	NO MÓVIL			83.095.338.338	
COMUNICACION CELULAR S A COMCEL S A	PERSONAS	TELÉFONO MÓVIL	3G	681.287		
COMUNICACION CELULAR S A COMCEL S A	PERSONAS	TELÉFONO MÓVIL	4G	144.615		
EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. ESP.	PERSONAS	DATA CARD	3G	13.382	$ 912.439.376	26.225.089
UNE EPM TELECOMUNICACIONES S.A. E.S.P. - UNE EPM TELCO S.A.	PERSONAS	DATA CARD	3G	93.128	$ 16.625.304.498	3.307.825.164.869
UNE EPM TELECOMUNICACIONES S.A. E.S.P. - UNE EPM TELCO S.A.	PERSONAS	DATA CARD	4G	136.061		
TOTAL NACIONAL				**3.926.843**	**389.763.353.110**	**20.196.080.028.145**

Fuente: http://colombiatic.mintic.gov.co/602/w3-article-8127.html

Tabla 6. Información tercer trimestre 2014, suscriptores personas a internet móvil, por tecnología, ingresos y tráfico.

INFORMACIÓN 3 *TRIMESTRE 2014 ABONADOS DE TELEFONÍA MÓVIL*					
PROVEEDOR	**ABONADOS EN SERVICIO**	**ABONADOS EN PREPAGO**	**ABONADOS EN POSPAGO**	**LÍNEAS ACTIVADAS**	**LÍNEAS RETIRADAS**
ALMACENES EXITO INVERSIONES S.A.S.	273.818	225.573	-	50.237	8.510
AVANTEL S.A.S.	245.229	39.057	173.410	50.025	13.570

COLOMBIA MOVIL S.A. E.S.P. *	8.692.171	6.944.223	1.413.261	1.824.486	1.452.400
COLOMBIA TELECOMUNICACIONES S.A. ESP *	12.581.553	8.982.442	3.268.298	1.431.754	1.450.387
COMUNICACION CELULAR S A COMCEL S.A *	29.290.815	23.276.224	5.815.472	3.518.175	3.336.383
EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. ESP.	-	34.684	-	-	-
UFF MOVIL SAS	415.300	416.309	-	68.092	69.101
UNE EPM TELECOMUNICACIONES S.A. E.S.P. - UNE EPM TELCO S.A.	380.015	104.444	271.111	35.738	19.955
VIRGIN MOBILE COLOMBIA S.A.S.	1.704.763	1.235.298	-	486.214	71.082
TOTAL NACIONAL	**53.583.664**	**41.258.254**	**10.941.552**	**7.464.721**	**6.421.388**

Fuente: http://colombiatic.mintic.gov.co/602/w3-article-8127.html

En la tabla 6 se hace evidente que las personas representan el 76,04% de las suscripciones de internet móvil en el país y 18.809,065 Tb de tráfico. Son datos nada despreciables para los operadores de las redes móviles en cuanto a los ingresos, teniendo en cuenta que los usuarios hacen uso de sus teléfonos móviles como de data card, representadas estas en modem usb, tablet.

Los datos obtenidos del informe del MinTic, solo son una muestra del desarrollo de las telecomunicaciones en Colombia, y del avance de los usuarios de los servicios de redes móviles en adoptar estas tecnologías, para

su beneficio personal, académico y profesional siendo de gran utilidad y cerrando la brecha de conectividad a internet. Para demostrar lo anterior, se muestra el siguiente cuadro consolidado:

Tabla 7. Consolidado 2010- 2014, suscriptores a internet móvil, por tecnología.

INFORMACIÓN 2010-2014 SUSCRIPTORES A INTERNET MOVIL, POR TECNOLOGIA			
AÑO	SUSCRIPTORES		
	2G	3G	4G
2010	1.110.382	598.251	NA
2011	1.060.792	1.727.941	NA
2012	856.746	2.315.975	36.338
2013	759.598	3.645.928	158.118
2014(4to trimestre)	540.352	3.814.806	808.762

Fuente: http://colombiatic.mintic.gov.co/602/w3-propertyvalue-715.html

Es necesario dilucidar lo proyectado en la tabla 7, en el entendido que se pueden extraer varias situaciones. La primera de ellas, que la suscripción a internet en el estándar 2G bajo un 51,34%, de 2010 a 2014; mientras que el estándar 4G, aumento un 2.225,66% en el periodo 2012- 2014, esto debido al aumento en la cantidad de proveedores que ofrecen el servicio 4G.

Consecuencia de la implementación de nuevos estándares de redes móviles y del aumento de los suscriptores de los servicios ofrecidos en bases a los estándares, ha crecido el tráfico en Kb.

Tabla 8.Consolidado 2010- 2014 tráfico en Kb internet móvil.

CONSOLIDADO 2010-2014 TRÁFICO Kb INTERNET MOVIL

AÑO	TRÁFICO KB
2010	6.883.958.805.906
2011	9.024.660.283.923
2012	11.850.580.877.347
2013	19.072.053.445.265
2014(3er trimestre)	20.196.080.028.145

Fuente: http://colombiatic.mintic.gov.co/602/w3-propertyvalue-715.html

Los datos que se desprenden de los tablas 6, 7 y 8 son el resultado de la consolidación de las informes de la industria TIC de nuestro país para los años 2010 a 2014 (tercer trimestre), y muestra un claro aumento en la cantidad de suscriptores como el consumo de Kb. Lo que infiere que los colombianos hacen uso de estas redes para el envío constante de información propia. Sin embargo es importante mencionar que se han presentado incidentes de seguridad informática, haciendo uso de estas redes, como se ha mencionado al inicio de este marco de referencia.

3.3. MARCO TEÓRICO.

3.3.1. Redes Móviles. Las redes móviles ofrecen transmisión de datos mediante conexiones inalámbricas. La conexión se realiza mediante radio, lo cual es logrado por la infraestructura fija desplegada para que los usuarios obtengan conectividad a los servicios ofrecidos, como voz y datos.

La infraestructura final contiene: Estación base (BS Base Station) y terminales (MS Mobile Station). Para obtener la cobertura esperada se hace necesario dividir el territorio en fragmentos más pequeños, llamados celdas y las mismas son atendidas por la BS.

Los tamaños de las celdas se pueden clasificar de la siguiente manera:

- Femtoceldas: Utilizado para cubrir áreas que reciben un señal de baja calidad de otras celdas. La cobertura de estas puede ser de varios metros.

- Picocelda: Para este caso, la cobertura aumenta pero no de manera sustancial.

- Microceldas: La cobertura se amplía a varios cientos de metros, dándole acceso a usuarios de zonas urbanas.

- Macroceldas: Estas celdas buscan dar cobertura sobre áreas de terreno y son de varios kilómetros de radio.

- Celda satelital: Este tipo de celdas, busca da cobertura donde las otras celdas no pueden hacerlo. La intensidad de la señal depende dela ubicación de satélite y de los dispositivos de recepción y trasmisión, permite la conexión en lugares inaccesibles para los tipos de células anteriores.

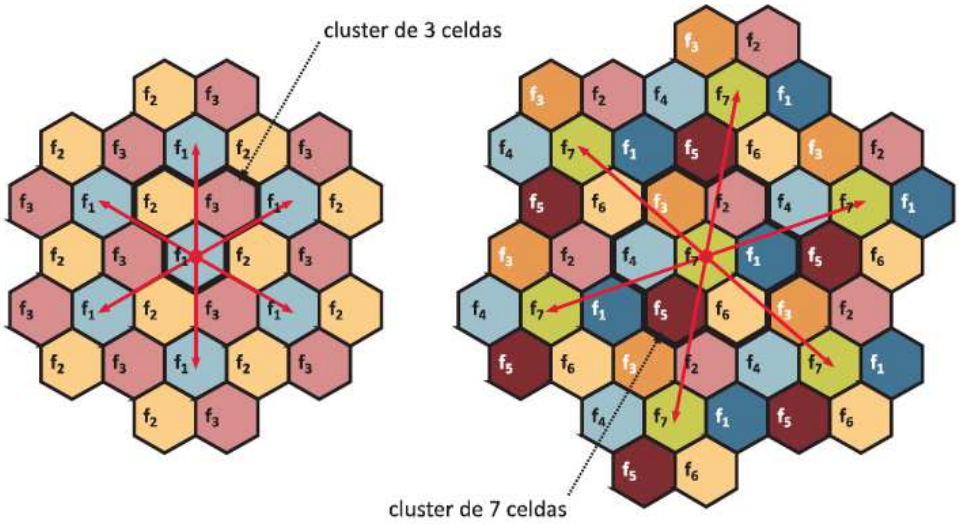

Figura 1. Cobertura de macrocelda.

Fuente: Redes móviles, Zdenek Becvar, Pavel Mach, Ivan Pravda, Pág 16.

Es necesario mencionar que las frecuencias (f1 a f7), deben ser planificadas con el objetivo de dar cobertura en el territorio y su diámetro máximo son pocos kilómetros. En este modelo se basa la red GSM, usando macroceldas.

3.3.1.1. Sectorización. Este principio en la implementación de redes móviles se basa en la administración de varias celdas por una sola estación base (BS), donde la intersección de tres celdas, constituye un sector para que la BS administre. Lo cual facilita la cobertura de grandes áreas geográficas de territorio.

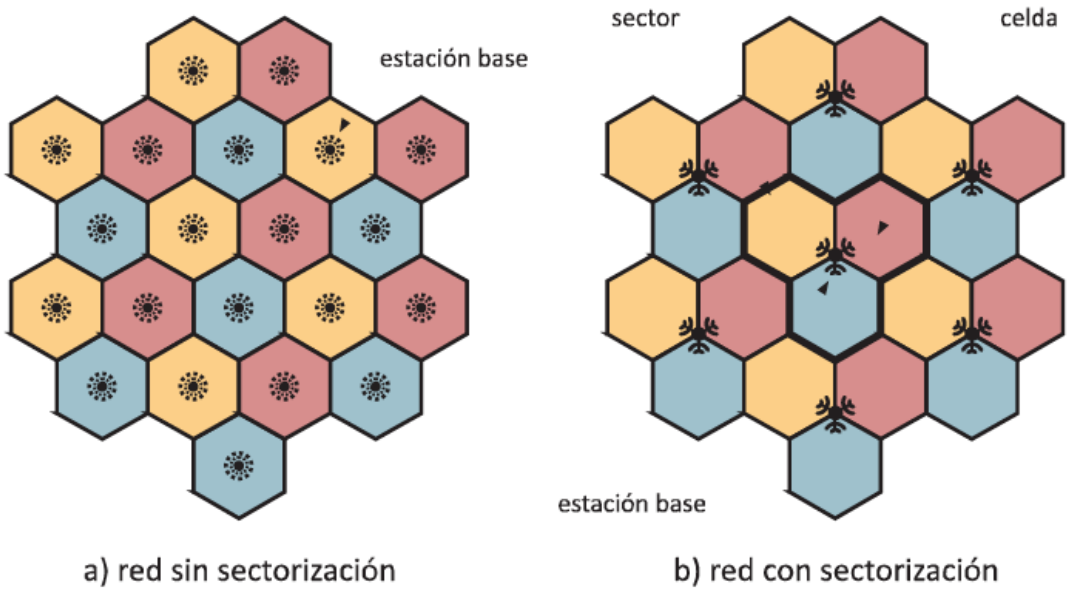

Figura 2. Sectorización clúster de celdas.

Fuente: Redes móviles, Zdenek Becvar, Pavel Mach, Ivan Pravda, Pág 17.

3.3.1.2. Métodos de Acceso.

Los usuarios del servicio móvil buscan tener conexión permanente con la BS, lo anterior no se lograría si no existieran los métodos de acceso múltiple como los siguientes:

FDM: Divide las frecuencias en subcanales y asigna uno de estos subcanales de frecuencia el enlace de comunicación.

TDMA: Divide un subcanal de frecuencia en diferentes segmentos temporales y a su vez cada segmento se subdivide en una secuencia de ranuras temporales.

CDM: Las señales de cada canal se pueden transmitir usando la misma banda de frecuencia y en simultánea. Los canales habilitados se diferencian unos de otros en la recepción a partir del esquema de codificación única utilizado para la codificación en el transmisor al momento de procesar los datos en cada extremo del canal.

OFDMA: Se obtiene en una combinación de acceso múltiple por división en tiempo y frecuencia En consecuencia a los usuarios individuales se les atribuye no sólo una o varias subportadoras sino también un lapso de tiempo para la comunicación sea efectuada y pueda transmitir.

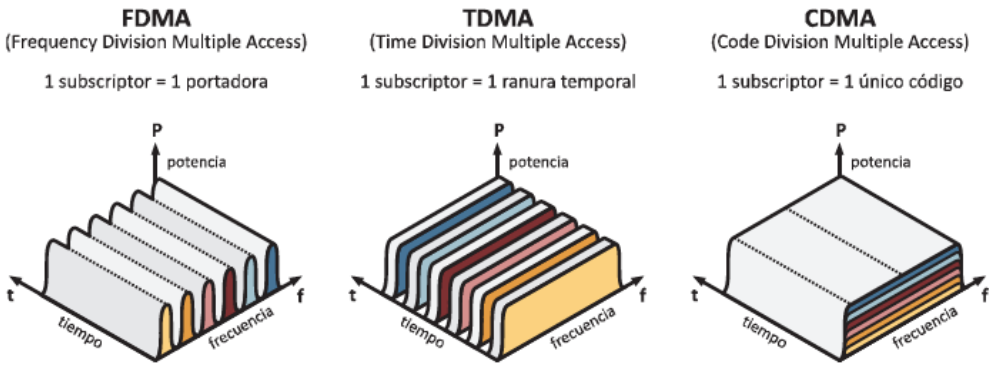

Figura 3. Métodos de acceso múltiple.

Fuente: Redes móviles, Zdenek Becvar, Pavel Mach, Ivan Pravda, Pág 19.

3.3.1.3. Reconexión Automática.

La movilidad del dispositivo o estación móvil (MS), es posible a que la BS ofrece la disponibilidad de celdas más cercanas, ofreciendo potencia en la señal hacia el usuario. Para ello es necesario gestionar la conexión nuevamente con la célula vecina, pero de manera automática para el usuario, este fenómeno es llamado handrover o traspaso. Es necesario para ofrecer la

mejor calidad de servicio al usuario o mejorar la distribución de carga en la red; para lograrlo la red almacena un registro de ubicación de la MS para enrutar la red hacia este.

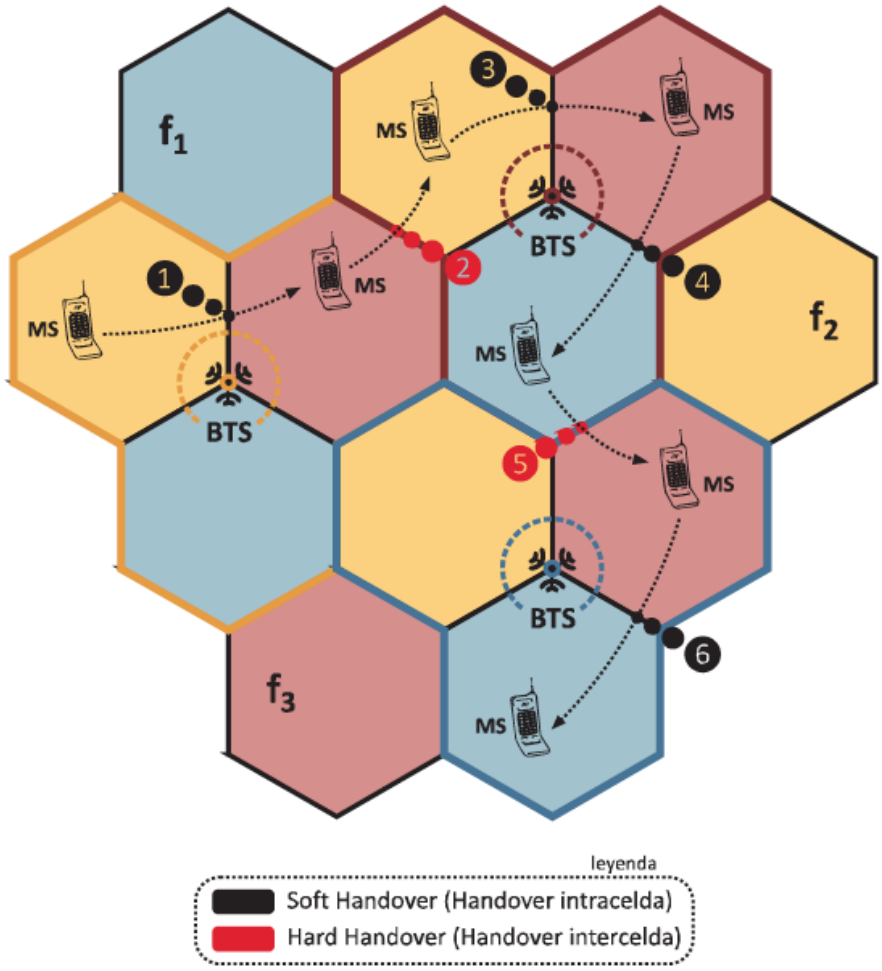

Figura 4. Traspaso MS a BTS

Fuente: Redes móviles, Zdenek Becvar, Pavel Mach, Ivan Pravda, Pág 22.

3.3.2. Redes Móviles Gsm, de segunda generación.

Las redes móviles han generado la necesidad de comunicación constante, permanente y de calidad con entidades y otro usuario de la red. Para ello se hace necesario conocer que para identificarse en la misma, utiliza la SIM (Suscriber Identity Module), que contiene los datos básicos de identificación del usuario, claves de autenticación , información de servicios adicionales y las llamadas de emergencia.

El proceso de comunicación se ejecuta de la siguiente manera: el MS envía su número de identificación IMSI (International Mobile Subscriber Identity) a través de la BS y del controlador de la estación base (BSC, Base Station Controller) al centro de conmutación móvil MSC (Mobile Switching Centre). El bloque AuC (Authentication Centre) envía a través del MS un número aleatorio que es convertido de acuerdo a los algoritmos y datos almacenados en la tarjeta SIM a otro número diferente que se envía como respuesta al número original para autenticar al usuario. Luego, los datos individuales se comparan con los datos que se encuentra en una base de datos ubicada en el bloque VLR. Si los datos son coherentes, se permite que el MS pueda acceder a la red móvil.

Es necesario identificar los dispositivos necesarios para realizar la comunicación móvil, para lo cual se ejemplifica en la siguiente figura.

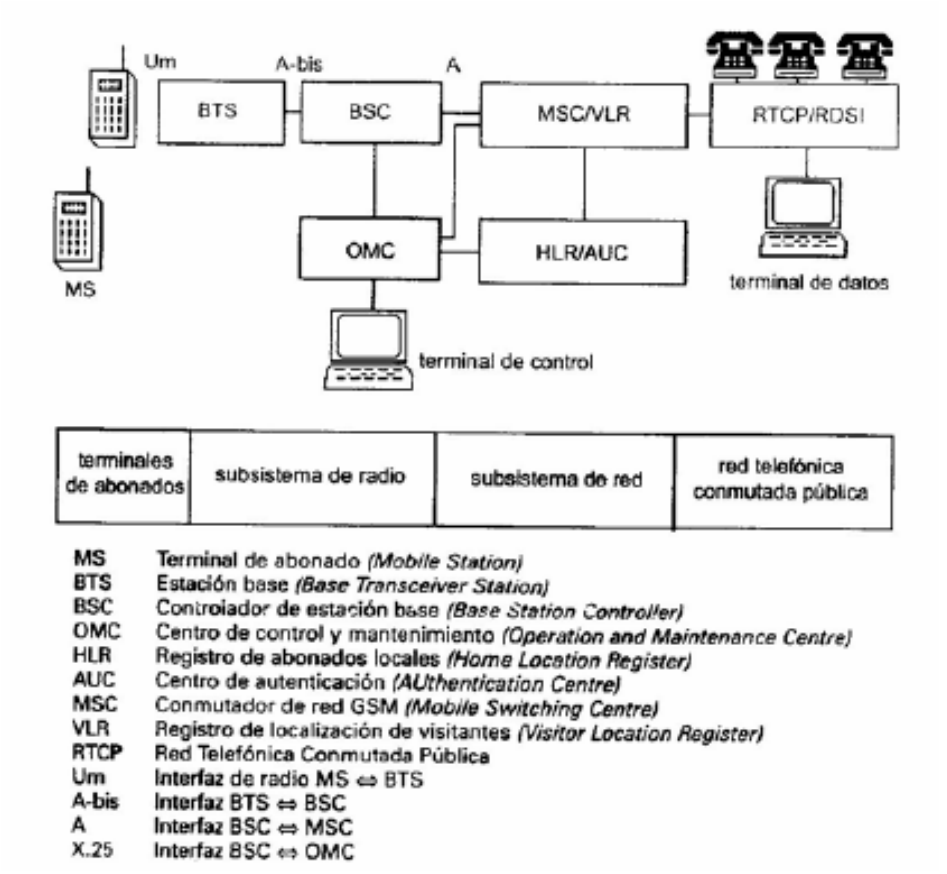

Figura 5. Dispositivos descriptivos red GSM.

Fuente: Red Gsm. Infraestructura de una red Gsm. Rev 20 de febrero de 2015. [Citado en 20 de febrero de 2015].Disponible en internet: <http://www.geocities.ws/rosa_virgen_sm/Comunicaciones/Tel_celular/INFRA_RED_GSM.pdf>

Detallados los dispositivos requeridos, ahora se evidencia con la siguiente figura, la arquitectura de la red GSM.

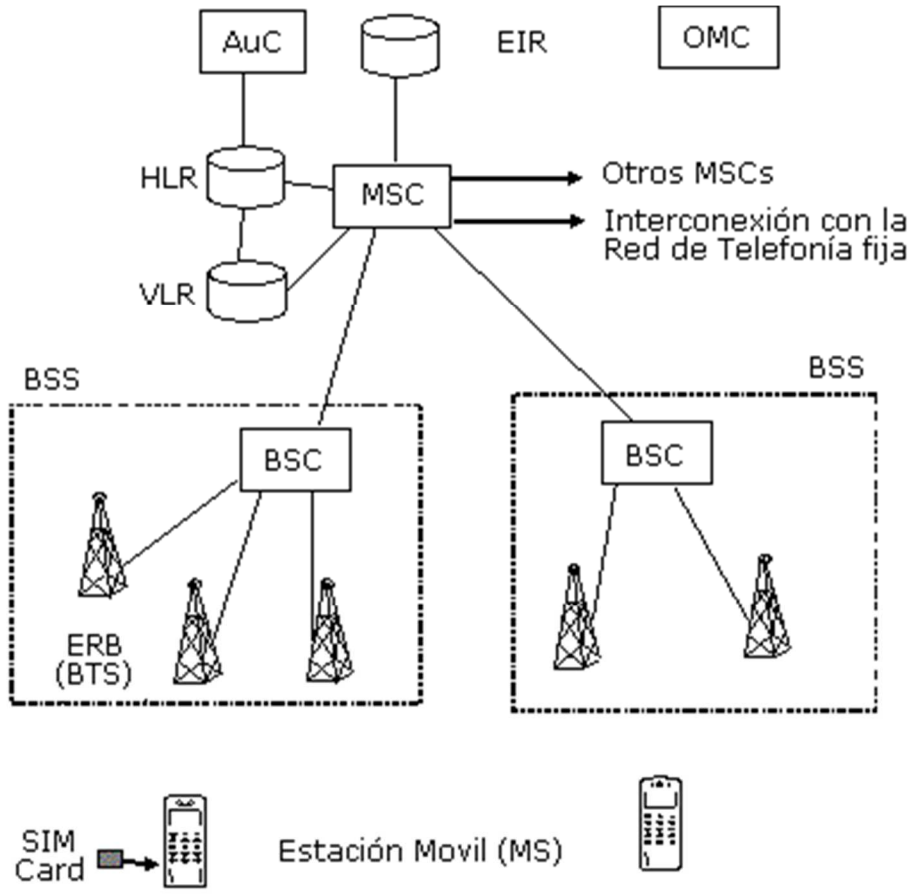

Figura 6. Arquitectura red móvil GSM.

Fuente: TELECO, Inteligencia en Telecomunicaciones (Brasil). Rev 21 de febrero de 2015. [Citado en 21 de febrero de 2015].Disponible en internet:<http://www.teleco.com.br/imagens/es_imagens/figura1_tutorialgsm.gif >

3.3.2.1. Estándares Utilizados.

Se presenta la red Gsm como la oportunidad para aprovechar la banda de frecuencia ante el aumento significativo del tráfico de los datos. Existen tres a mencionar:

• GSM 900 – banda de frecuencias de 900 MHz, capacidad máxima de 2 × 124 canales, ancho de banda de 2 × 25 MHz

• GSM 1800 – banda de frecuencia de 1800 MHz, capacidad máxima de 2 × 374 canales, ancho de banda de 2 × 75 MHz

• GSM 1900 – banda de frecuencias de 1900 MHz, capacidad máxima de 2 × 298 canales, ancho de banda de 2 × 75 MHz.

3.3.2.2. Protocolos de Transmisión y Recepción.

Los principales protocolos de esta interfaz son DTAP (Direct Transfer Application Part) y BSSAP (Base Station Subsystem Application Part). Ahora se procede a su explicación.

DTAP es un protocolo de aplicación para transferir información de señalización entre la MS y la MSC en redes GSM.

BSSAP es un protocolo para transportar información de control de la BSC entre la MSC y la BSS, por ejemplo, para la asignación de canales de tráfico entre la MSC y la BSS[5].

[5]Diseño, integracion y optimización de estaciones bases de segunda generacion. GSM. España. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet: <http://bibing.us.es/proyectos/abreproy/11980/fichero/CAP%CDTULO+3+-+FUNDAMENTOS+GSM+Y+UMTS%252F3.3+GSM.pdf>

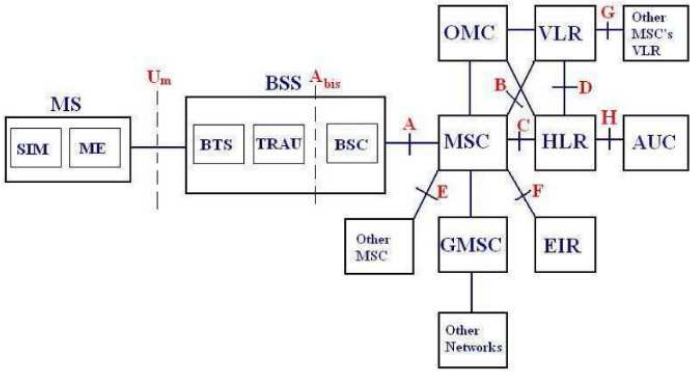

Figura 7. Esquema de interfaces en el estándar GSM.

Fuente: Diseño, Integración y Optimización de Estaciones Base de Segunda Generación. Disponible en internet: <http://bibing.us.es/proyectos/abreproy/11980/fichero/CAP%CDTULO+3+-+FUNDAMENTOS+GSM+Y+UMTS%252F3.3+GSM.pdf>

3.3.2.3. Interfaces y Relación con Protocolos.

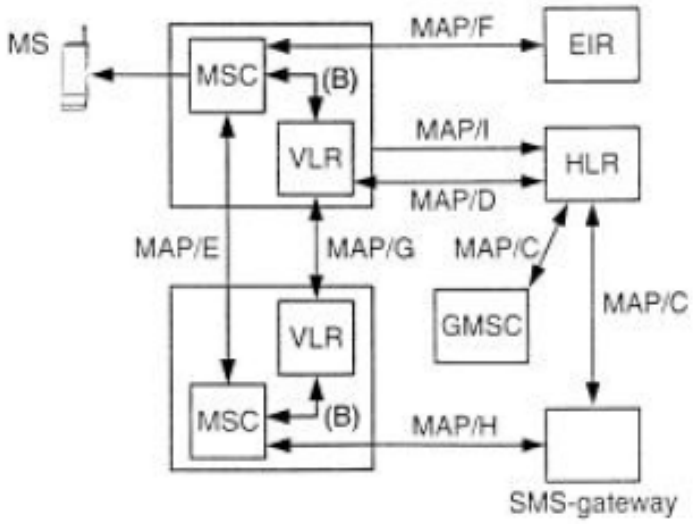

Figura 8. Protocolos asociados a cada interfaz.

Fuente: Diseño, Integración y Optimización de Estaciones Base de Segunda Generación. Disponible en internet: <http://bibing.us.es/proyectos/abreproy/11980/fichero/CAP%CDTULO+3+-+FUNDAMENTOS+GSM+Y+UMTS%252F3.3+GSM.pdf>

A continuación se presenta una tabla con la información de cada interfaz, la información que administra y el protocolo con el cual tiene relación.

Tabla 9. Relación entre interfaces y protocolos GSM [6]

Interfaz	Situada entre	Descripción	Intercambio de información de	
			usuario	Señalización
A	MSC-BSC	Permite el intercambio de información sobre la gestión del subsistema BSS, de las llamadas y de la movilidad. A través de ella, se negocian los circuitos que serán utilizados entre el BSS y el MSC.	SI	SS7
Abis	BSC-BTS	Permite el control del equipo de radio.	SI	LAPD
B	VLR-MSC asociados	VLR es la base de datos que contiene toda la información que permite ofrecer el servicio a los clientes que se encuentran en el área de influencia de sus MSC asociados. Por lo tanto, cuando un MSC necesite proporcionar información sobre un móvil acudirá a su VLR. Esta interfaz NO debe ser externa NO(por desempeño, por el volumen de información intercambiado).	NO	MAP/B
C	HLR-GMSC	Es la interfaz utilizada por los gateways GMSC para enrutar la llamada hacia el MSC destino. La GMSC no necesita contar con un VLR, se trata de un nodo que sólo transmite llamadas.	NO	MAP/C
D	HLR-HLR	Permite intercambiar información entre ambas bases de datos, esta información se encuentra relacionada con la posición del móvil y la gestión del servicio contratado por el usuario.	NO	MAP/D

[6]Diseño, integracion y optimización de estaciones bases de segunda generacion. GSM. España. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet: <http://bibing.us.es/proyectos/abreproy/11980/fichero/CAP%CDTULO+3+-+FUNDAMENTOS+GSM+Y+UMTS%252F3.3+GSM.pdf>

E	MSC-MSC	Permite intercambiar la información necesaria para iniciar y realizar un intercambio Inter-MSC cuando el móvil cambia de área de influencia de un MSC a otro.	SI	MAP/E, RDSI e ISUP
F	MSC-EIR	Utilizada cuando el MSC desea comprobar el IMEI de un equipo.	NO	
G	VLR-VLR	Utilizada para permitir la interconexión entre dos VLRs de diferentes MSCs.	NO	MAP/G
H	HLR-AuC		SI	MAP/H
I	MSC-MS	Permite el intercambio transparente de datos entre el MSC y el MS a través del BSS.		
Um	BSS-MS	Es la interfaz de radio, se encuentra entre la estación móvil y el BSS.	SI	LAPDm

Es de anotar, los protocolos que intervienen en la transmisión y recepción de datos, de manera gráfica.

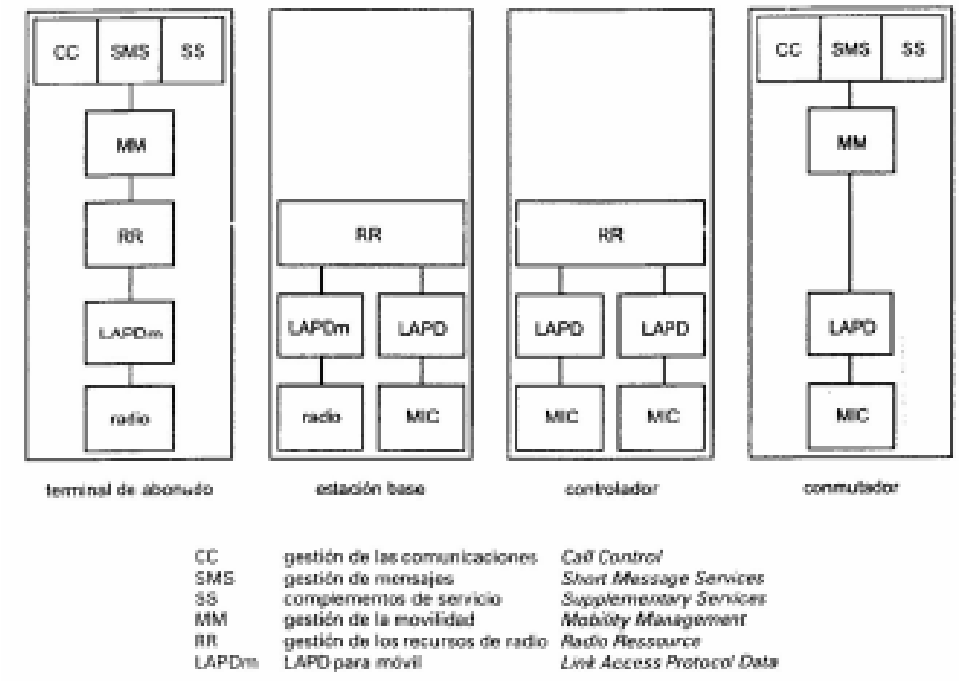

Figura 9. Pila de protocolo en la estación base y el subsistema de radio.

Fuente: Red Gsm, McGraw Hill, Página 7.

3.3.2.4. Bandas de Transmisión y Recepción

Se dispone de la siguiente tabla, donde se evidencia las frecuencias en Mhz, y demás características de la capa física:

Tabla 10. Características capa física en GSM.

Parámetro	**GSM**
Frecuencia de Transmisión (MHz) Base a Móvil Móvila Base	 935-960 1805-1880 890-915 1710-1785
Tipo de accesomúltiple	TDMA
Método de Duplexado	FDD
Ancho de banda por radiocanal	200 KHz
Nº canales de tráfico por radiocanal Nº total de canales de tráfico	8 1000
Canal vocal: Tipo de Modulación Velocidad Txon/Desviación Frec. Tipo de VOCODER y velocidad	 GSMK 270,8 Kbps 13 Kbps
Canal de Servicio Tipo de modulación	 GMSK

Fuente: Diseño, integración y optimización de estaciones bases de segunda generación. GSM. España. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet: <http://bibing.us.es/proyectos/abreproy/11980/fichero/CAP%CDTULO+3+-+FUNDAMENTOS+GSM+Y+UMTS%252F3.3+GSM.pdf>

3.3.2.5. Servicios Ofrecidos.

En cuanto a los servicios que ofrece la red Gsm, se mencionan los siguientes:

- Telefonía (incluyendo llamadas de emergencia, llamadas mediante itinerancia y también en todas las otras redes).
- Servicios de mensajes, tales como SMS (Short Message Services).
- Correo de voz.
- E-mail.
- Servicios bancarios.
- Servicios de entretenimiento.

3.3.2.6. Arquitectura Red Gsm.

Para mayor claridad acerca del desarrollo de la red y su funcionalidad, se ilustra de la siguiente manera:

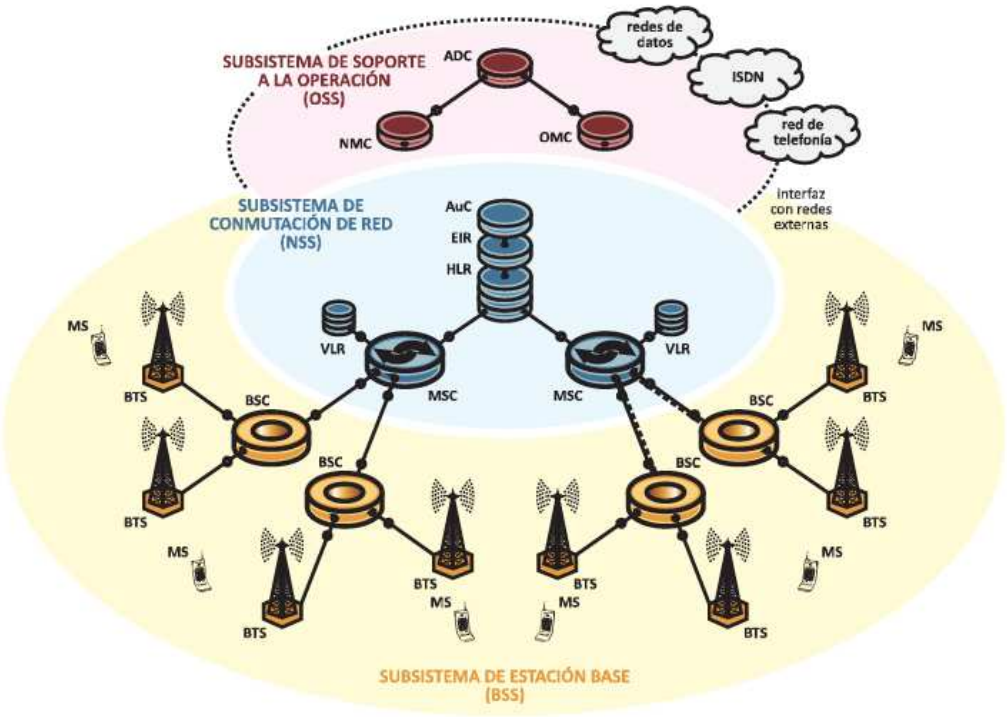

Figura 10. Arquitectura GSM, con sus elementos de operación.

Fuente: Redes móviles, Zdenek Becvar, Pavel Mach, Ivan Pravda, Pág 28.

La red GSM cuenta con tres partes fundamentales, subsistema de estación base, subsistema de conmutación de red y subsistema de soporte de operación.

Subsistema de estación base (BSS): La tarea es la asignación y liberación de canales radio para la comunicación con los MS, garantizando el proceso de traspaso o handover.

La central de conmutación móvil (MSC), se encarga de iniciar, terminar y canalizar las llamadas de los BSC y BS el MS llamado.

Subsistema de Conmutación de red: Este componente permite portar y administrar las comunicaciones de los MS a la red conmutada telefónica. Además posee otras funciones como son:

• HLR (Home Location Register): Proporciona un registro de todos los participantes en el área. La AuC proporciona la autenticación.

• VLR (Visitor Location Register): Almacena temporalmente la información más reciente sobre la situación de un terminal móvil en el rango de su MSC. El VLR solicita y obtiene datos del HLR y si el MS abandona la zona visitada sus datos se eliminan del VLR.

• EIR (Equipment Identity Register): Contiene información acerca de MS.

Subsistema de soporte a la operación: Posee tres componentes, de supervisión (ADC), gestión global de flujo de información (NMC), y de operación y mantenimiento (OMC).

3.3.2.7. Transmisión de Datos en Red Gsm.

El uso de la red GSM para voz, tiene una velocidad de transferencia de 13,2 Kbps en ambos sentidos. Ahora bien, el canal es usado para la transmisión de datos que se basa en la conmutación de circuitos CSD, con una tasa de transferencia de 9,6 Kbps, luego paso a 14,4Kbps.

Existen dos clases de transmisiones:

Basada en conmutación de paquetes: Comúnmente conocida como GPRS a una velocidad de 171 Kbps.

Basada en conmutación de circuitos: Conocida como HSCSD, a una tasa de 115 Kbps.

Los anteriores conceptos hacen parte de las redes 2.5G.

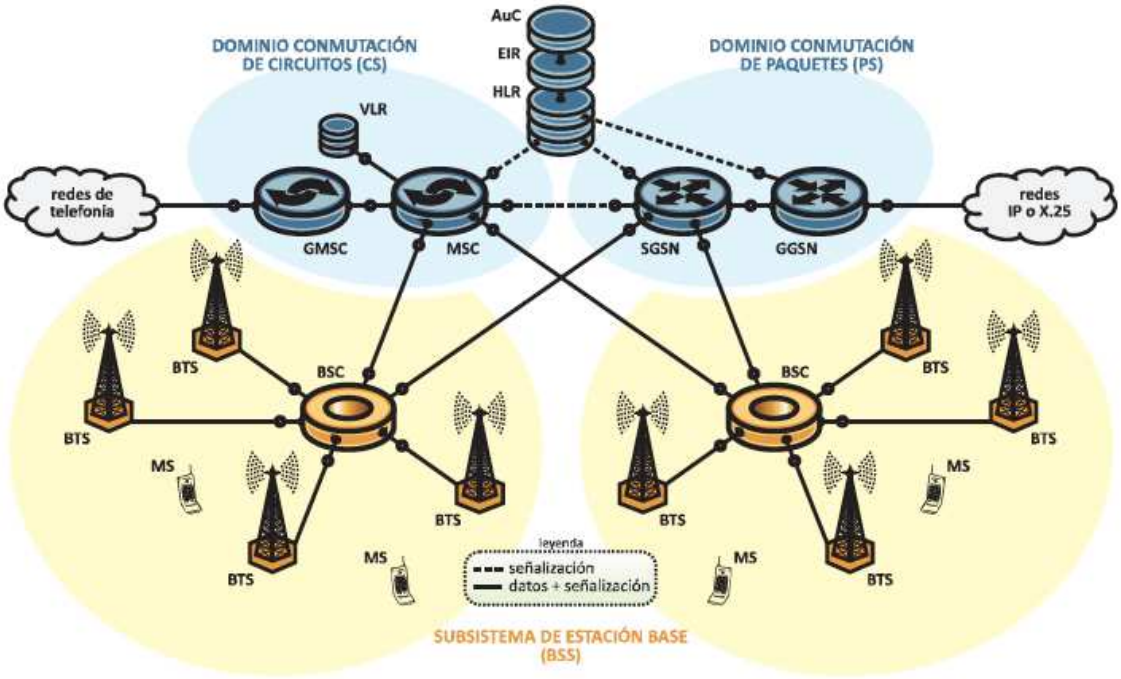

Figura 11. Arquitectura red móvil 2.5G

Fuente: Redes móviles, Zdenek Becvar, Pavel Mach, Ivan Pravda, Pág 33

3.3.2.8. Ataques Red Gsm.

- Interceptación de la comunicación: La interceptación de la comunicación, se basa en capturar la señal en la red Gsm, ha sido considerada la debilidad manifiesta de dicha red, porque permite capturar la señal, romper el cifrado del algoritmo A5/* y decodificar los resultados mediante una herramienta llamada Airprobe (Open Source Project).

- Man in themiddle: La red Gsm no cuenta con protección alguna contra este ataque, que se basa en ubicar antenas falsas (BTS), toda vez que no se autentica la conexión entre la antena y el suscriptor.

- Vector de autenticación: Para el caso de la red Gsm, es vulnerable. Toda vez que no autentica la conexión.

- Suplantación de identidad: Es vulnerable.

- Autenticación: Es vulnerable.

- Señalización: Es vulnerable.

- RF- DoS: No tiene protección.

3.3.3. Transmisión de Datos Gprs.

En la evolución de las redes móviles, ya no solo era necesaria la transmisión de la voz, sino de datos. Es por ello que con el objetivo de aumentar la velocidad de transmisión, tuvo que cambiar el modo de transferencia de circuitos a paquetes. A continuación con la figura 12, se muestra el cambio.

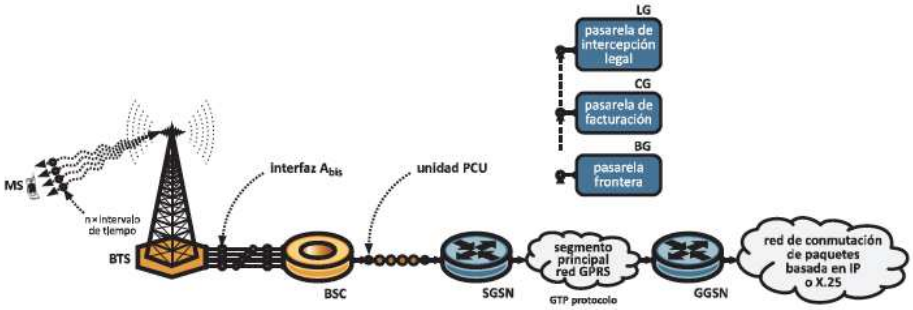

Figura 12. Transmisión de datos GPRS.

Fuente: Redes móviles, Zdenek Becvar, Pavel Mach, Ivan Pravda, Pág 37.

Para la conexión a internet es posible por medio del protocolo WAP, que permite que un MS pueda acceder al contenido de sitios web utilizando canales de baja capacidad y pantallas con resolución limitada. La aplicación de comunicación de datos y WAP permite la utilización de GPRS y la mejora de tasas de transferencia hasta 192 Kbps. Aunque el valor de la infraestructura de red GSM y los MS aumentan significativamente. La ventaja en la red GSM que utilizan HSCS los enlaces de transferencia no está permanentemente bloqueada. Y la desventaja es el retraso hasta de segundos cuando los paquetes son de un 1Kb.

- Protocolos de transmisión.

Gtp: GPRS Tunneling Protocol. Es el encargado de transportar los paquetes del usuario y sus señales relacionadas entre los nodos de soporte de GPRS (GSN)[7]. Los paquetes GTP contienen los paquetes IP o X.25 del usuario. Por debajo de él, los protocolos estándares TCP o UDP se encargan de transportar los paquetes por la red. Resumiendo, en el Backbone del GPRS tenemos una arquitectura de transporte IP/X.25-sobre-GTP-sobre-UDP/TCP-sobre IP.

[7] Universitat de Valencia. GPRS. España. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet: <http://www.uv.es/~montanan/redes/trabajos/GPRS.doc>

Sndcp: Subnetwork Dependent Convergence Protocol. Es el encargado de transferir los paquetes de datos entre los SGSN (nodo responsable de la entrega de paquetes al terminal móvil) y la estación móvil. Las funciones que desempeña:

Multiplexación de diversas conexiones de la capa de red en una conexión lógica virtual de la capa LLC.

Compresión y descompresión de los datos e información redundante de cabecera.

Air interface: Concierne a las comunicaciones entre la estación móvil y la BSS en los protocolos de las capas física, MAC, y RLC.

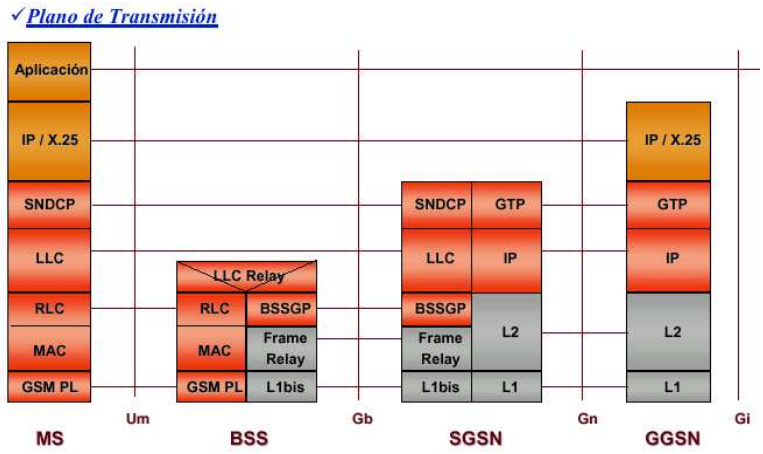

Figura 13. Pila de protocolos en el plano de transmisión GPRS.

Fuente: Universitat de Valencia. GPRS. España. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet: <http://www.uv.es/~montanan/redes/trabajos/GPRS.doc>

- Protocolos de señalización.

Gmm/sm: Gprs mobility management/session management. Es el protocolo que se encarga de la movilidad y la gestión de la sesión[8] en momentos de la ejecución de funciones de seguridad, actualizaciones de rutas, etc.

La señalización entre SGSN y los registros HLR, VLR, y EIR utilizan los mismos protocolos que GSM con ciertas funciones ampliadas para el funcionamiento con el GPRS.

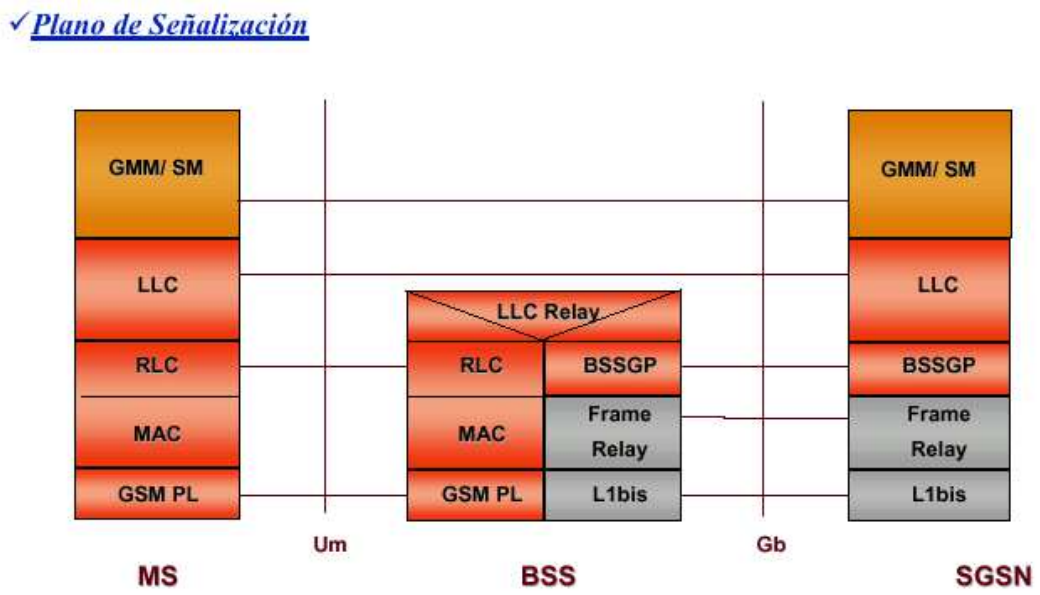

Figura 14. Pila de protocolos en el plano de señalización GPRS.

Fuente: Universitat De Valencia. GPRS. España. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet: <http://www.uv.es/~montanan/redes/trabajos/GPRS.doc>

- Dispositivos red gprs.

[8] Universitat de Valencia. GPRS. España. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet: <http://www.uv.es/~montanan/redes/trabajos/GPRS.doc>

Para interpretar la relación que existe entre los nuevos elementos adicionados a la red GSM, adicionando una red de transporte ip (IP Backbone), se presenta la siguiente figura.

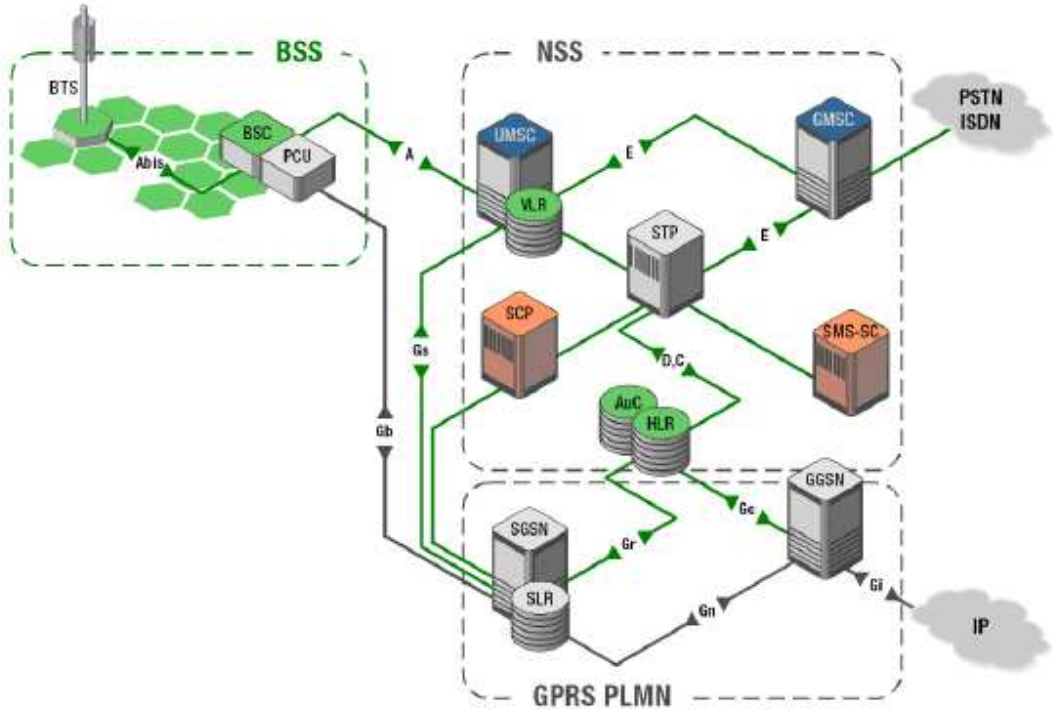

Figura 15. Dispositivos descriptivos red GPRS.[9]

- Interfaces red gprs

Gb: Usa Frame Relay y transporta el tráfico y señalización entre la red de Radio GSM y el backbone GPRS[10].

Gn: Comunica a los GSN's (GGSN y SGSN). Utiliza TCP/IP.

[9]Seminario de Redes SS7/GSM/(E)GPRS. (Argentina). Memorias. Tektronix. 52 p. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<http://www.ladeprofesional.com.ar/seminariok15-gsm-gprs.pdf>

[10] Universidad Simon Bolivar. Redes De Computadores II. (Venezuela). Memorias. GPRS-Global Packet Radio Services. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<http://ldc.usb.ve/~poc/RedesII/Grupos/G2/>

Gr: Busca en la base de datos los APN (nombre de punto de acceso, es un nombre simbólico para una interfaz de red en el GGSN que lleva a una red externa), IMSI y los datos del subscriptor.

Ga: Comunica a los GSN's con el CG para compilar los CDR's (Charging Data Record: información de cobro). Utiliza TCP/IP.

Gi: Comunica al GGSN con las redes externas. Utiliza TCP/IP.

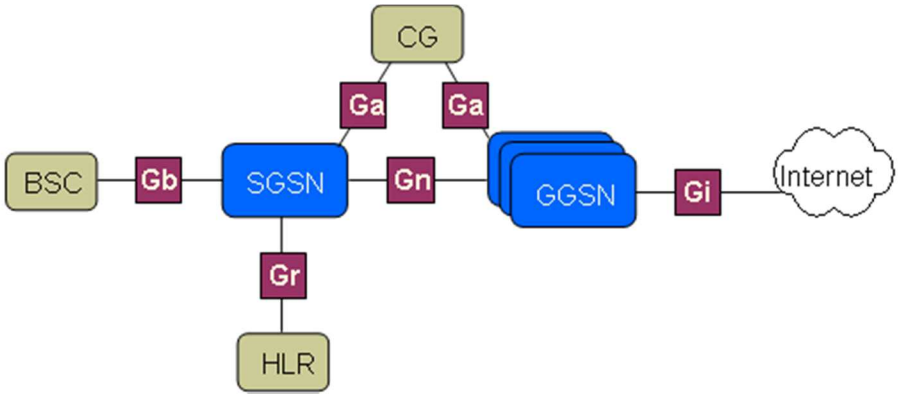

Figura 16. Interfaces en la red GPRS.

Fuente: http://ldc.usb.ve/~poc/RedesII/Grupos/G2/

- Bandas de transmisión y recepción.

Las redes GPRS, comparten las mismas frecuencias de las redes GSM, utilizando la transmisión de datos por medio de "paquetes". Lo que mejora la velocidad de transmisión hasta 144Kbps.

- Transmisión de datos edge.

Este tipo de transmisión pertenece a las redes 2.75G, y busca el aumento del rendimiento mediante una modulación más eficiente. La modulación original

GMSK (Gaussian Minimum Shift Keying), EDGE utiliza la modulación en fase 8-PSK (Phase Shift Keying).

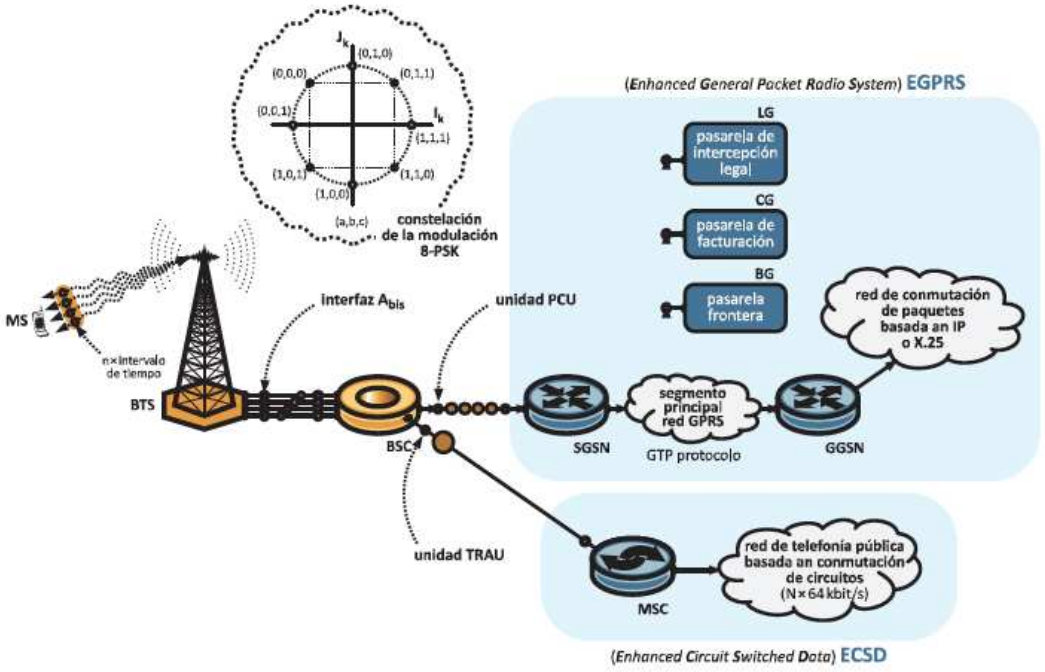

Figura 17. Transmisión de datos EDGE

Fuente: Redes móviles, Zdenek Becvar, Pavel Mach, Ivan Pravda, Pág 39.

Los esquemas de modulación de ocho niveles logran que la tasa de bits sea tres veces más rápida que la modulación original. La máxima tasa de transmisión posible es de 473.6 Kbps (59.2 Kbps por intervalo de tiempo).

- Protocolos de transmisión.

La mejora que busca la transmisión de datos en EDGE, significa mayor tasa de transferencia y mayor eficiencia del espectro. En este aspecto se han introducido cambios sustanciales en los protocolos de modulación y codificación del canal, que puede usarse para transmitir servicios de voz y datos por conmutación de circuitos o de paquetes. En atención a los cambios, los protocolos se han modificado en comparativa con GPRS, lo anterior se evidencia en la siguiente figura.

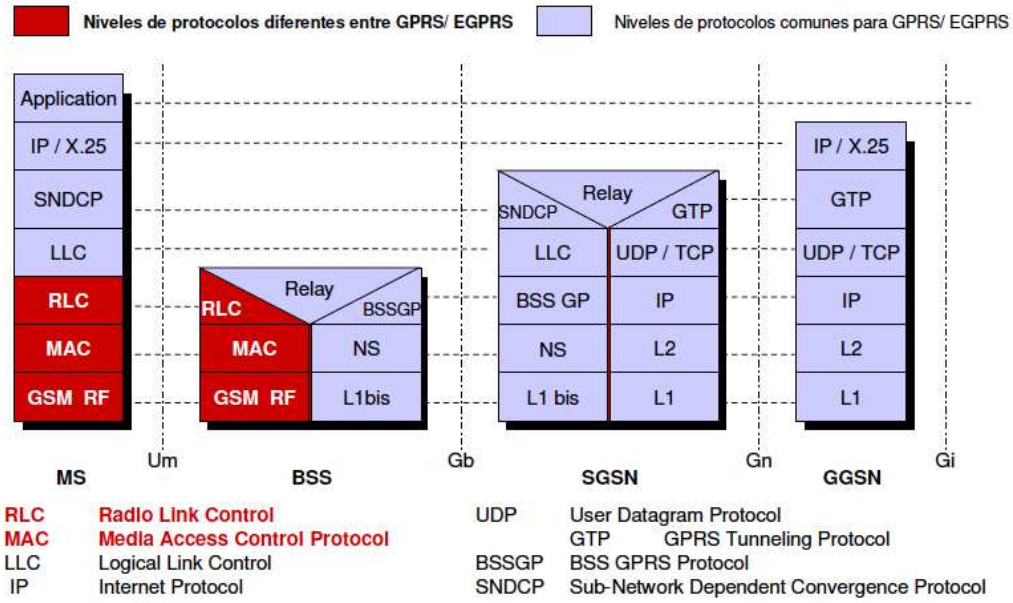

Figura 18. Pila de protocolos, comparativa GPRS/ EDGE.[11]

En conclusión, la parte física que debe ser actualizada en la red GPRS, para soportar EDGE, es la radio base, cambiando el transceptor que soporte EDGE, y se debe actualizar el software a los elementos de la BSS.

- Dispositivos de red edge.

Los cambios de la red GPRS a EDGE, se refleja en los dispositivos físicos, como la estación base, lo anterior se ejemplifica en la siguiente figura.

[11]Seminario de redes SS7/GSM/(E)GPRS. (Argentina). Memorias. Tektronix. 52 p. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet:<http://www.ladeprofesional.com.ar/seminariok15-gsm-gprs.pdf>

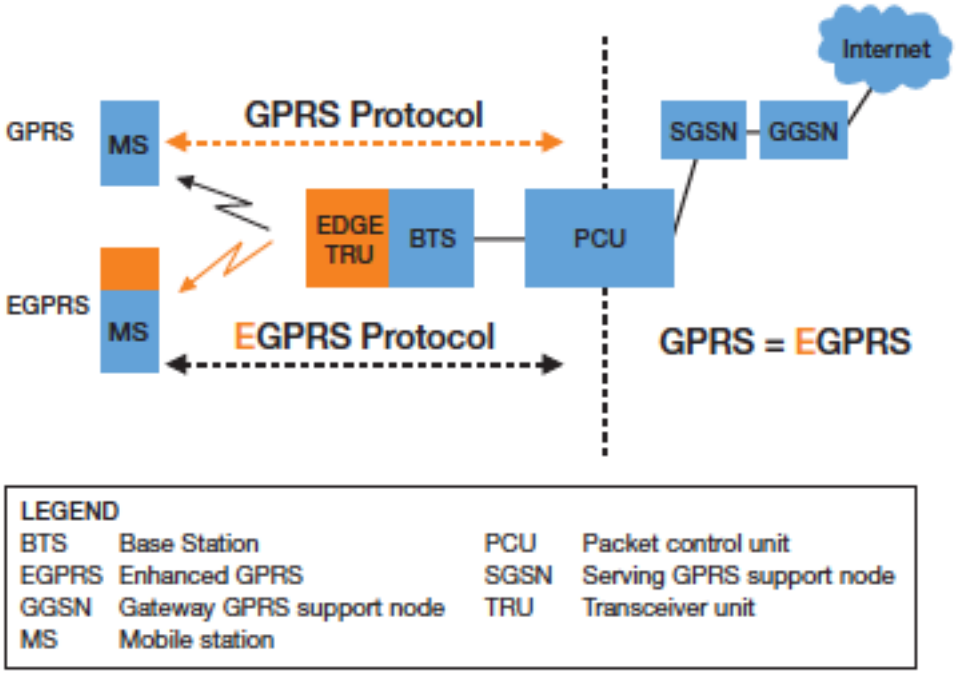

Figura 19. Cambios en los dispositivos descriptivos de la red GPRS a EDGE.

Fuente: Ericcson White Paper, Introduction of high – speed data in GSM/GPRS networks.[12]

- Bandas de transmisión y recepción.

Los cambios suscitados son lo siguiente:

En downliknk (BTS a MS): 1930 a 1990Mhz

En Uplink (MS a BTS: 1850 a 1910Mhz

3.3.4. Universal Mobile Telecommunication System - UMTS, tercera generación.

[12]ERICSSON AB. Introduction of high-speed data in GSM/GPRS networks. Ericsson AB. 2003. AE/LZT 123 7058 R2. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet:<http://www.satnac.org.za/proceedings/2003/plenary/EricssonEDGE.pdf>

La búsqueda constante de mayor cantidad de datos fluyan por la red 2G, hace difícil su administración, a razón de lo anterior, aparece las redes de tercera generación o 3G. Para enfrentar esta situación UMTS adopta el método llamado WCDMA (Wideband Code Division Multiple Access).

3.3.4.1. Wcdma.

En este método los datos representados en bits, tienen mucho más canal de banda ancha, aumentando inmediatamente su capacidad y velocidad de transmisión de los datos. Una característica importante es el uso de la frecuencia, en atención a que todas las celdas utilizan la misma frecuencia, contrario a GSM, que usa frecuencias diferentes por celdas para atenuar la interferencia.

3.3.4.2. Arquitectura De Red.

Para el estudio de la red móvil UMTS, la misma está divida a nivel lógico, en tres partes, UE (equipo usuario), la UTRAN, y la CN (red del núcleo). Estas partes se encuentran separadas por interfaces que ha definido el 3GPP, y el objetivo de las mismas es la comunicación y coordinación de la transmisión. En la figura 20, se muestra la arquitectura de red.

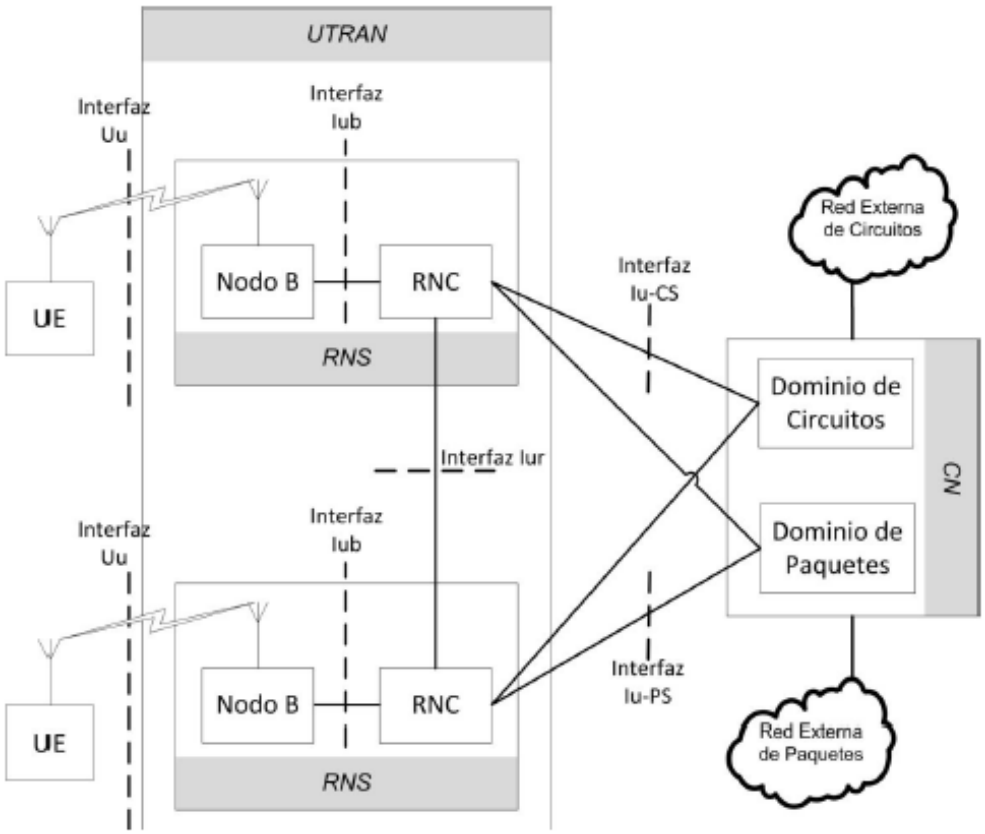

Figura 20. Arquitectura red móvil UMTS.

Fuente Capitulo II: "Aspectos generales del sistema de telefonía móvil UMTS de tercera generación"[13]

En la primera parte, se encuentra el UE (equipo usuario, MT) que consta de terminal móvil (MT) y módulo de identidad del suscriptor UMTS (USIM).

En la segunda parte, se halla la UTRAN, que a su vez está compuesta por la estación base (Nodo B, BTS), controlador de red radio (RNC).

Y la tercera parte, se encuentra la red del núcleo (CN).

[13]Capitulo II. Aspectos Generales Del Sistema de Telefonía Móvil Umts de Tercera Generación. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet: <http://www.tierradelazaro.com/cripto/UMTS.pdf>

3.3.4.3. Evolución Umts.

En el marco del crecimiento y desarrollo de las redes 3G para el año de 1999 aparece la primera versión UMTS, conocida como Release 99. Desde ese momento se han aprobado varias versiones o reléase, que buscan a mejora de la red móvil y brindar mejor acceso a los datos transmitidos.

- Release 99: Esta versión se basa en la red GSM, siendo así UMTS compatible con GSM. La Release 99 aporta un nuevo tipo de red de acceso de radio, conocida como UTRAN (UMTS Universal Radio Access Networks).

- Release 4: Fue aprobada en 2001 e introduce varios cambios sustanciales en la red del núcleo (core).

- Release 5: Introduce la tecnología HSDPA (High Speed Downlink Packet Access). HSDPA aumenta la tasa de bits transferidos en el enlace descendente hasta aproximadamente 14 Mbps.

- Release 6: La versión 6 busca una mejoría importante en la transmisión de datos a partir de la especificación HSUPA (High Speed Uplink Packet Access).

- Release 7: Aparece HSPA +, también llamada como “Evolved High Speed Packet Access”. La mejora consiste en la introducción de una modulación más eficaz (64 QAM) y la técnica MIMO (Multiple Input Multiple Output) en la que tanto el emisor como el receptor pueden emplear más antenas.

3.3.4.4. Protocolos De Transmisión.

Para el uso de la red UMTS, se ha subdivido en tres subredes, la parte inferior, se encuentra la red transporte, en la parte intermedia, está la red de radio y en la parte superior la red del sistema. La red de transporte, provee los servicios generales y la red de radio y de sistema, soportan las funcionalidades de UMTS. Con las siguientes figuras, se muestran en la ubicación según el plano de uso.

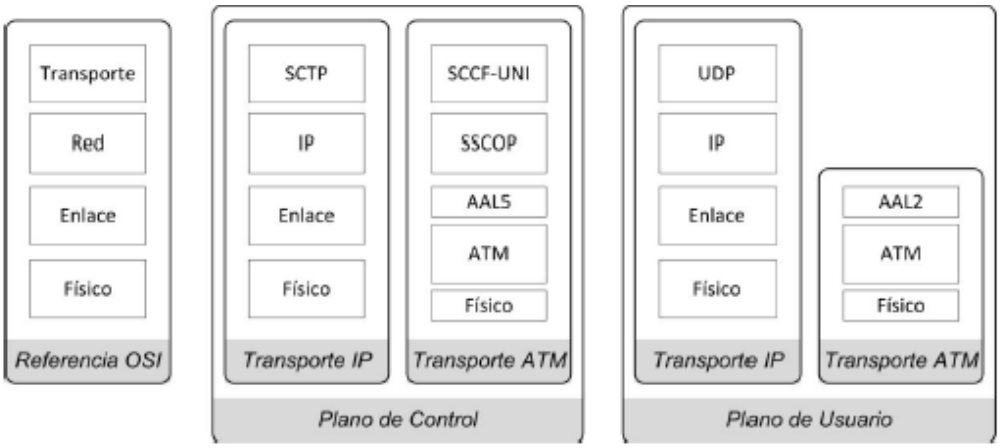

Figura 21. Protocolos de la red de transporte para la interfaz Iub.

Fuente Capítulo II: "Aspectos generales del sistema de telefonía móvil UMTS de tercera generación"[14]

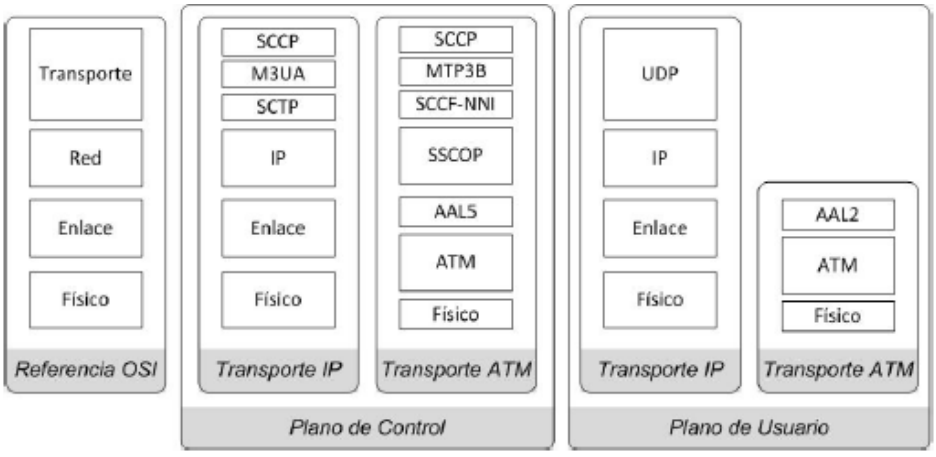

Figura 22. Protocolos de la red de transporte para la interfaz Iur.

[14]Capitulo II. Aspectos generales del sistema de telefonía móvil umts de tercera generación. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet: <http://www.tierradelazaro.com/cripto/UMTS.pdf>

Fuente Capitulo II: “Aspectos generales del sistema de telefonía móvil UMTS de tercera generación”[15]

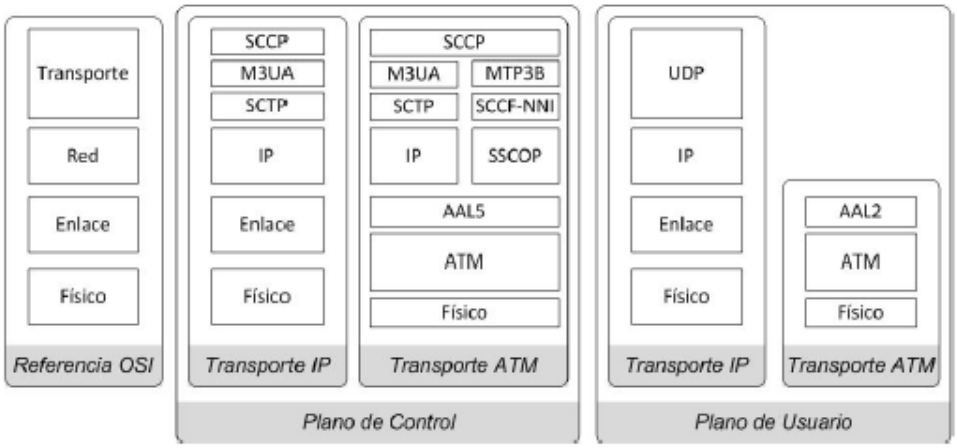

Figura 23. Protocolos de la red de transporte para la interfaz Iu- CS.

Fuente Capitulo II: “Aspectos generales del sistema de telefonía móvil UMTS de tercera generación”[16]

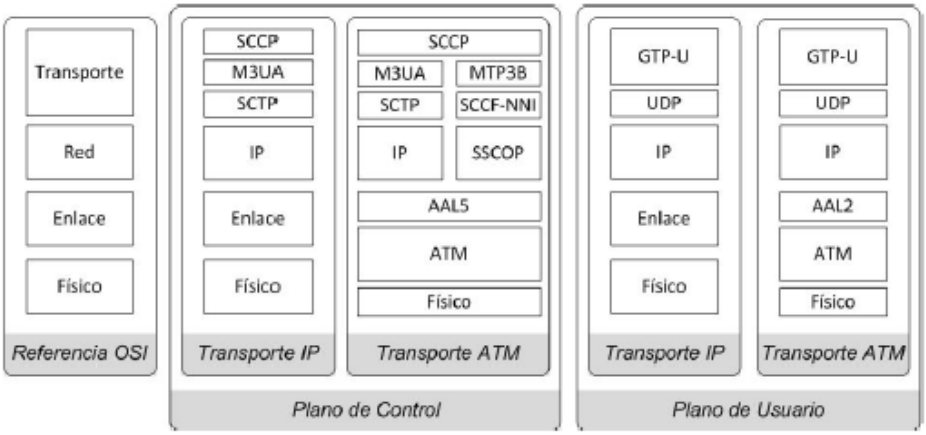

Figura 24. Protocolos de la red de transporte para la interfaz Iu- PS.

Fuente Capitulo II: “Aspectos generales del sistema de telefonía móvil UMTS de tercera generación”[17]

[15]Capitulo II. Aspectos generales del sistema de telefonía móvil umts de tercera generación..Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet: <http://www.tierradelazaro.com/cripto/UMTS.pdf>

[16]Capitulo II. Aspectos generales del sistema de telefonía móvil umts de tercera generación. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet: <http://www.tierradelazaro.com/cripto/UMTS.pdf>

3.3.4.5. Dispositivos De Red Umts.

En este apartado se distinguen 3 dispositivos en la red UMTS:

- Los equipos del usuario (UE o MS).
- La red de acceso UTRAN (UMTS Terrestrial Radio Acces).
- Núcleo de la red, divido en dos partes, Dominio de circuitos (voz) y dominio de paquetes (datos).

La comprensión de la relación de dichos dispositivos, de ejemplifica en la siguiente figura.

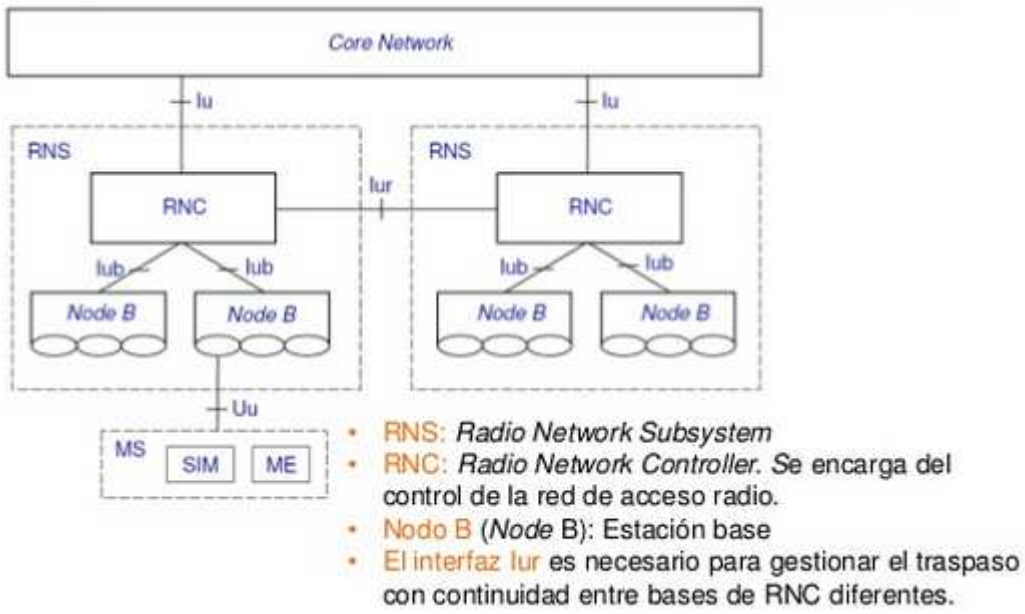

Figura 25. Dispositivos descriptivos red UMTS.

Fuente: http://es.slideshare.net/c09271/uni-fiee-scm-sesion-12-redes-moviles-3-g4g, diapositiva 33.

[17]Capitulo II. Aspectos generales del sistema de telefonía móvil umts de tercera generación. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet: <http://www.tierradelazaro.com/cripto/UMTS.pdf>

3.3.4.6. Bandas de Transmisión y Recepción.

Los cambios suscitados son los siguientes:

En downliknk (BTS a MS) banda 1: 2110 a 2170Mhz

En downliknk (BTS a MS) banda 2: 1930 a 1990Mhz

En downliknk (BTS a MS) banda 3: 1805 a 1880Mhz

En Uplink (MS a BTS) banda 1: 1920 a 1980Mhz

En Uplink (MS a BTS) banda 2: 1850 a 1910Mhz

En Uplink (MS a BTS) banda 3: 1710 a 1785Mhz

3.3.4.7. Ataques Red 3g.

- Man in themiddle: La red 3g cuenta con autenticidad, integridad y control de verificación del mensaje enviado entre la antena y el suscriptor.

- Vector de autenticación: Para el caso de la red 3g, es vulnerable. Allí se configura el ataque MiTM complejo, y se captura los datos de autenticación del usuario.

- Suplantación de identidad: Es vulnerable, aplicando el vector de autenticación y también es vulnerable a la clonación de tarjeta Sim.

- Autenticación: Es obligatorio la utilización y verificación del cifrado.

- Señalización: Para la red 3g existe el control integridad en los mensajes de señalización.

- RF- DoS: No tiene protección. Sin embargo el control de integridad puede ayudar a prevenirlo.

3.3.5. Red Móvil Long Term EvolutionLTE- A, 4G, cuarta generación.

La evolución de las redes continua, así como su modo de conexión, operación, gestión de transmisión de múltiples antenas, manejo de interferencias de las celdas. Es así como arroja medidas de tasas máximas de datos de hasta un 1Gbps. Cabe mencionar que LTE-A fue aprobado en el release 10 de 3GPP, el cual es la primera norma compatible con 4G, donde implementa nuevas manera de agregar portadoras, mejoras en enlace descendente y ascendente de múltiples antenas. A su vez, mejora la coordinación de la interferencia que permite desarrollar e implementar femtoceldas.

3.3.5.1. Arquitectura de Red.

Las arquitecturas de redes móviles han tenido como propósito mejorar los servicios que presta, haciendo uso de las capacidades tanto de los nodos como de los terminales. Siendo necesario mencionar, que la red LTE está diseñada para soportar la conmutación de paquetes más de no circuitos. Los componentes de la arquitectura de red, está representada por la red de acceso, llamada E-UTRAN (Evolved Universal Terrestrial Radio Access Network) y EPC (Evolved Packet Core). La figura 26, indica gráficamente la distribución de la red.

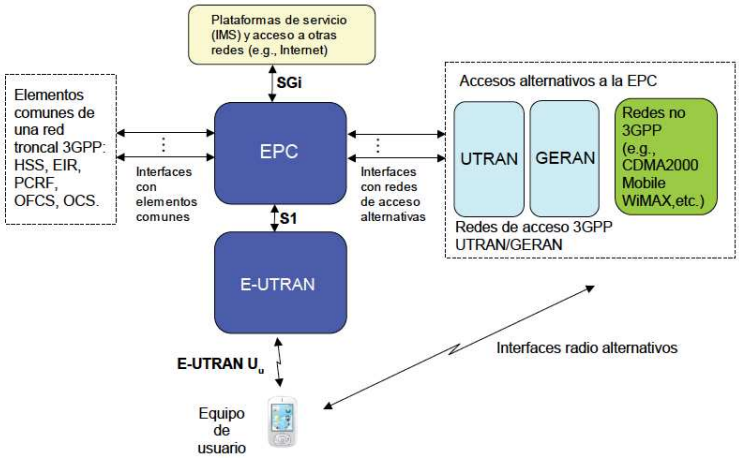

Figura 26. Arquitectura de red LTE.

Fuente LTE: Nuevas tendencias en comunicaciones móviles, pág 60.[18]

El componente de acceso a la red, E-UTRAN, está constituido por las estaciones base llamadas eNodeBs, encargados de la gestión de radio, movilidad, planificación de los enlaces ascendentes y descendentes, cifrado de datos.

3.3.5.2. Protocolos de Transmisión.

En las redes LTE, conocidas como 4G, los protocolos en las tres interfaces E-UTRAN (radio, S1 y X2), se estructuran en torno al plano de usuario y a un plano de control. Para el caso del plano de usuario, contempla los protocolos utilizados para el tráfico de paquetes IP. Para el caso del plano de control, son el soporte de las funciones y procedimientos en las diferentes interfaces.

- Protocolos en la interfaz de radio.

Corresponden a los protocolos que se encargan del envío de un paquete entre el Nodo o BTS y el usuario o MT, conformada por una capa de nivel de enlace (capa 2) y una capa física del modelo OSI. Lo anterior, se demuestra en la siguiente figura.

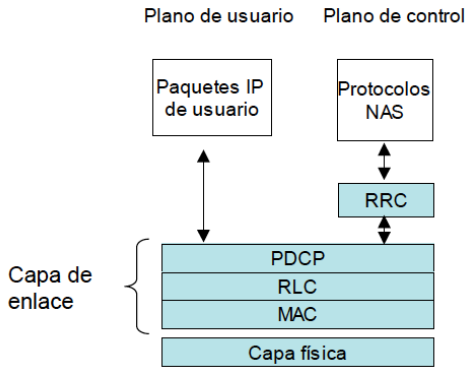

Figura 27. Pila de protocoles interfaz de radio E-UTRAN.[19]

[18]AUGUSTI, Ramon. BERNARDO, Francisco. CASADEVALL, Fernando. FERRÚS, Ramon. PÉREZ-ROMERO, Jordi. SALLENT, Oriol. LTE: Nuevas tendencias en comunicaciones móviles. Fundación Vodafone. España. 2010. ISBN: 84-934740-4-5. 431 p. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<https://proyectolte.files.wordpress.com/2012/09/lte-nuevas-tendencias.pdf>

- Protocolos en el plano de usuario.

Los protocolos en el plano de usuario, indican en el paquete IP enviado, el tipo de servicio que el usuario está usando, la señalización a nivel de aplicación. Se muestra en la siguiente figura, la interacción respectiva.

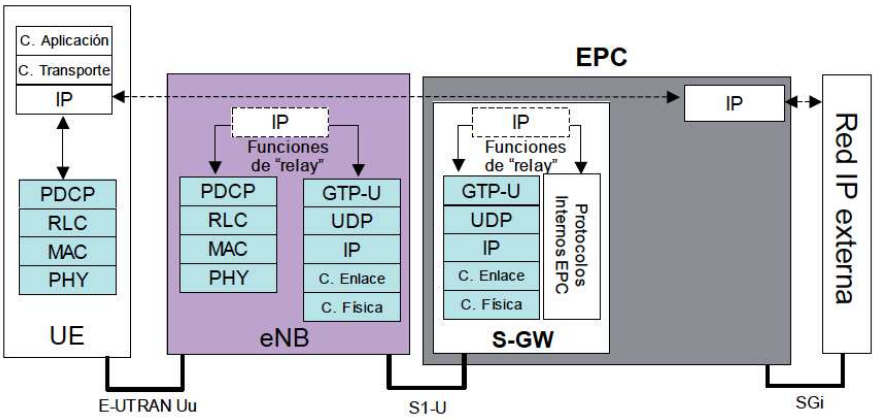

Figura 28. Pila de protocolos del plano de usuario en E-UTRAN.[20]

Fuente: LTE: Nuevas tendencias en comunicaciones móviles, pág 75.

- Protocolos en el plano de control.

Se utilizan para enviar la señalización de los paquetes enviados entre el equipo del usuario y la red troncal.

[19]AUGUSTI, Ramon. BERNARDO, Francisco. CASADEVALL, Fernando. FERRÚS, Ramon. PÉREZ-ROMERO, Jordi. SALLENT, Oriol. LTE: Nuevas tendencias en comunicaciones móviles. Fundación Vodafone. España. 2010. ISBN: 84-934740-4-5. 431 p. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<https://proyectolte.files.wordpress.com/2012/09/lte-nuevas-tendencias.pdf>

[20]AUGUSTI, Ramon. BERNARDO, Francisco. CASADEVALL, Fernando. FERRÚS, Ramon. PÉREZ-ROMERO, Jordi. SALLENT, Oriol. LTE: Nuevas tendencias en comunicaciones móviles. Fundación Vodafone. España. 2010. ISBN: 84-934740-4-5. 431 p. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<https://proyectolte.files.wordpress.com/2012/09/lte-nuevas-tendencias.pdf>

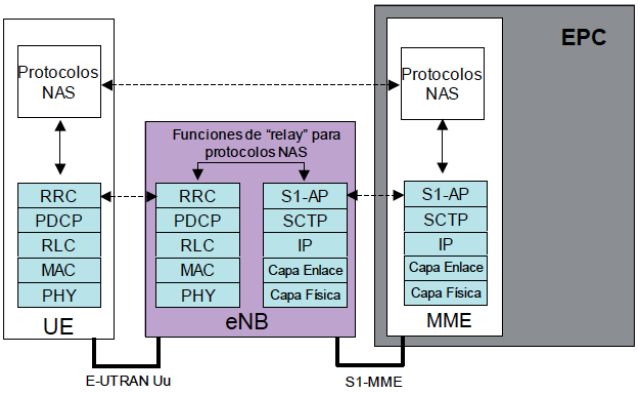

Figura 29. Pila de protocolos del plano de control en E-UTRAN.[21]

Fuente LTE: Nuevas tendencias en comunicaciones móviles, pág 75.

3.3.5.3. Dispositivos de Red 4G- LTE.

Para el caso de las redes 4G, en este apartado se distinguen 3 dispositivos en la red:

- Los equipos de los usuarios (UE o MS).
- La red de acceso mejorada: E- UTRAN.
- La red troncal de saquetes mejorada: EPC

La comprensión de la relación de dichos dispositivos, de ejemplifica en la siguiente figura.

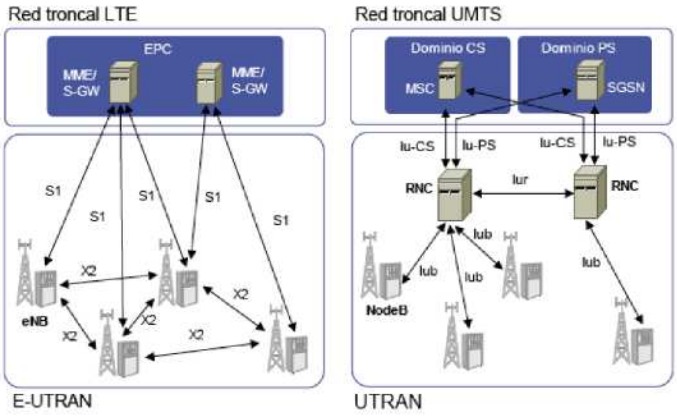

Figura 30. Comparativa de dispositivos descriptivos de red LTE con red UMTS.

[21]AUGUSTI, Ramon. BERNARDO, Francisco. CASADEVALL, Fernando. FERRÚS, Ramon. PÉREZ-ROMERO, Jordi. SALLENT, Oriol. LTE: Nuevas tendencias en comunicaciones móviles. Fundación Vodafone. España. 2010. ISBN: 84-934740-4-5. 431 p. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<https://proyectolte.files.wordpress.com/2012/09/lte-nuevas-tendencias.pdf>

3.3.5.4. Bandas de Transmisión y Recepción.

Para el caso de LTE, pueden existir bandas pareadas (FDD, Duplexado por división en frecuencia) y no pareadas (TDD, Duplexado por División de Tiempo). Se han identificado algunas bandas para el mejor despliegue de LTE, que a continuación de relacionan.

Tabla 11. Bandas mejor identificadas para el despliegue de LTE.[22]

Banda LTE	Banda para UL			Banda para DL			Tipo de Duplexado
1	1920 MHz	–	1980 MHz	2110 MHz	–	2170 MHz	FDD
2	1850 MHz	–	1910 MHz	1930 MHz	–	1990 MHz	FDD
3	1710 MHz	–	1785 MHz	1805 MHz	–	1880 MHz	FDD
4	1710 MHz	–	1755 MHz	2110 MHz	–	2155 MHz	FDD
5	824 MHz	–	849 MHz	869 MHz	–	894MHz	FDD
6	830 MHz	–	840 MHz	875 MHz	–	885 MHz	FDD
7	2500 MHz	–	2570 MHz	2620 MHz	–	2690 MHz	FDD
8	880 MHz	–	915 MHz	925 MHz	–	960 MHz	FDD
9	1749.9 MHz	–	1784.9 MHz	1844.9 MHz	–	1879.9 MHz	FDD
10	1710 MHz	–	1770 MHz	2110 MHz	–	2170 MHz	FDD
11	1427.9 MHz	–	1452.9 MHz	1475.9 MHz	–	1500.9 MHz	FDD
12	698 MHz	–	716 MHz	728 MHz	–	746 MHz	FDD
13	777 MHz	–	787 MHz	746 MHz	–	756 MHz	FDD
14	788 MHz	–	798 MHz	758 MHz	–	768 MHz	FDD
17	704 MHz	–	716 MHz	734 MHz	–	746 MHz	FDD
33	1900 MHz	–	1920 MHz	1900 MHz	–	1920 MHz	TDD
34	2010 MHz	–	2025 MHz	2010 MHz	–	2025 MHz	TDD
35	1850 MHz	–	1910 MHz	1850 MHz	–	1910 MHz	TDD
36	1930 MHz	–	1990 MHz	1930 MHz	–	1990 MHz	TDD
37	1910 MHz	–	1930 MHz	1910 MHz	–	1930 MHz	TDD
38	2570 MHz	–	2620 MHz	2570 MHz	–	2620 MHz	TDD
39	1880 MHz	–	1920 MHz	1880 MHz	–	1920 MHz	TDD
40	2300 MHz	–	2400 MHz	2300 MHz	–	2400 MHz	TDD

Fuente: LTE: Nuevas tendencias en comunicaciones móviles, página 75.

3.3.5.5. Ataques Red 4G.

- Man in themiddle: La red 4g no es vulnerable a este tipo de ataque.

[22]AUGUSTI, Ramon. BERNARDO, Francisco. CASADEVALL, Fernando. FERRÚS, Ramon. PÉREZ-ROMERO, Jordi. SALLENT, Oriol. LTE: Nuevas tendencias en comunicaciones móviles. Fundación Vodafone. España. 2010. ISBN: 84-934740-4-5. 431 p. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<https://proyectolte.files.wordpress.com/2012/09/lte-nuevas-tendencias.pdf>

- Vector de autenticación: Para el caso de la red 4g no es vulnerable.

- Suplantación de identidad: Es vulnerable a la clonación de la tarjeta Sim.

- Autenticación: No es vulnerable.

- Señalización: Para la red 4g el control de integridad esta implementado.

- RF- DoS: No tiene protección. Sin embargo el control de integridad puede ayudar a prevenirlo.

4. DISEÑO METODOLÓGICO

4.1. TIPO DE INVESTIGACIÓN:

Exploratoria.

4.1.1. Metodología de Investigación.

Exploratoria. Se ha utilizado este tipo de investigación en atención a que en la búsqueda de información relacionada con la seguridad informática en las redes móviles en Colombia, no se encontró estudio técnico especializado sobre el asunto. De igual los operadores del servicio de conexión a redes móviles no entregaron información al respecto.

Para abordar la investigación se hace uso del derecho que asiste a los colombianos para solicitar información a entidades estatales, privadas y/o personas, como lo es el derecho de petición consagrado en el Art. 23 de la Constitución Política de Colombia, solicitando a los operadores del servicio, entidades del Gobierno Nacional, entidades de control, de judicialización, de asesoría y consultoría, y organizaciones internacionales, información acerca de los protocolos, estándares y normas de la seguridad informática aplicadas a las redes móviles de datos. De igual manera, la consulta permanente de información disponible en internet, como también en las redes sociales como lo son twitter, facebook.

El formato utilizado fue el siguiente:

Pereira, 24 de marzo de 2014

Señores
xxxxxxx
República de Colombia

Ref: Derecho de petición Solicitud respetuosa de información.

En atención al proyecto de tesis de mi especialización en seguridad informática llamado "NUEVAS TENDENCIAS DE SEGURIDAD INFORMÁTICA EN LAS

REDES DE DATOS MÓVILES EN COLOMBIA.", solicito a ustedes de manera respetuosa la siguiente información.

1. Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.

2. Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.

3. Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.

4. Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.

Favor anexar las respuestas al correo que relaciono en mi firma.

Muchas gracias.

Ing. Wilmar L. Copete Marín
Egresado Especialista en Seguridad Informática
Docente ECBTI
31139394888-3207544436
wilmar.copete@unad.edu.co
CCAV Eje Cafetero- Universidad Nacional Abierta y a Distancia UNAD
Skype: wilmarcopeteinvestigacionunad

Este tipo de investigación, permite consultar de múltiples fuentes, la información que se requiere y descubrir los problemas sociales o de construcción social que han llevado a que el tema de la seguridad informática no se conozca a profundidad por parte de la sociedad colombiana.

Durante el desarrollo de esta investigación, se detectó que no solo los factores enteramente técnicos acerca de la seguridad informática, los que dificultan el

conocimiento de la sociedad de cómo proteger sus datos en las redes móviles, sino otros asuntos como la legislación y control estatal aplicado a los operadores, son determinantes a la hora de comprobar su uso y aplicabilidad.

4.1.2. Fuentes para la Recolección de Datos.

Entidades del Estado Colombiano, relacionados con la vigilancia y control de la operación de las redes móviles, MinTic, Comisión de Regulación de Comunicaciones, Fiscalía General de la Nación, Superintendencia de Industria y Comercio; operadores de telefonía móvil: Avantel, Claro, Tigo, Movistar, Une, Virgin Mobile; expertos sobre seguridad informática y/o grupos de investigación, como GIDAM, de la Universidad del Magdalena, GECTI, de la Universidad de los Andes, GIIT, de la Universidad Icesi; y consultores internacionales sobre seguridad informática, como 4GAméricas y exploración de sitios web, reportes técnicos o "whitepaper" o libros blancos acerca de las normas y estándares en seguridad informática, relacionados con el tema expuesto.

4.1.3. Diseño de la Investigación.

Para la realización de la investigación exploratoria, se hizo necesaria la construcción de una serie de preguntas a realizar a las fuentes de datos relacionados en el ítem anterior. Dichas preguntas se enmarcaron en el Art. 23 de la Constitución Política de Colombia, invocando el derecho de petición, donde todo ciudadano, tiene derecho a conocer la información de su interés, en el marco del respeto de las partes, tanto el solicitante como el solicitado, toda vez que se estructura como un canal oficial para requerir de la información necesaria.

5. NORMAS DE SEGURIDAD INFORMÁTICA APLICADAS ENREDES MÓVILES.

5.1. NORMAS APLICADAS.

En los inicios de la redes móviles, el objetivo primordial era la transmisión de la voz, como una señal análoga, entre un emisor y un receptor, de manera digital, separados geográficamente, haciendo uso de técnicas de enrutamiento, enmarcadas en paquetes de formas y procedimientos, llamadas así mismas, generaciones de la telefonía móvil.

Ese objetivo ha venido cambiando, toda vez que no solo se quiere llevar la voz, sino también, una infraestructura de servicios de telecomunicaciones, representados en datos y servicios multimedia, donde los tres eventos, convergen en la misma red, y son conocidos como las redes de la próxima generación.

5.1.1. Redes de Próxima Generación- NGN.

Las redes de próxima generación, o Next Generation Networks – NGN, por sus siglas en inglés, se han tratado de definir de varias maneras, pero la más acertada, fue dada por la UIT (o ITU en inglés), en su recomendación UIT-T Y.2001:

“Red basada en paquetes que permite prestar servicios de telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha propiciadas por la QoS, y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite a los usuarios el acceso sin trabas a redes y a

proveedores de servicios y/o servicios de su elección. Se soporta movilidad generalizada que permitirá la prestación coherente y ubicua de servicios a los usuarios"[23]

5.1.2. Entidades Normalizadoras.

En este apartado, existen varias entidades normalizadoras encargadas de este proceso, a mencionar:

ITU: Es la Unión Internacional de Telecomunicaciones, organismo especializado, que pertenece a las Naciones Unidas para las tecnologías de las información y comunicación. Son además los encargados de atribuir el espectro radioeléctrico y las órbitas de satélite a nivel mundial, de igual manera, se encargan del desarrollo de normas técnicas para para la interconexión de redes y sus tecnologías, sirviendo como marco de referencia obligatoria de los gobiernos del mundo, en la aplicación de normatividad en las redes móviles.

Tiene 193 estados miembros y alrededor de 700 empresas privadas, que apoyan el desarrollo de las mismas.[24]

ETSI: Es el Instituto Europeo de Normas de Telecomunicaciones, genera normas de aplicación mundial para la información y tecnologías de la

[23]International Telecommunication Union ITU. Serie Y: Infraestructura mundial de la Información, aspectos del protocolo Internet y redes de la próxima generación. Redes de la próxima generación – Marcos y modelos arquitecturales funcionales. Visión general de las redes de próxima generación. RECOMENDACIÓN UIT-T Y.2001. Comisión de Estudio 13 (2005-2008) del UIT-T. Ginebra, Suiza. 2005. 10 p.

[24]International Telecommunication Union ITU. Visión general. Ginebra, Suiza. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet:<http://www.itu.int/es/about/Pages/overview.aspx>

comunicación, incluye telefonía fija, móvil, radio y convergentes. Son reconocidos por la Unión Europea. Tiene alrededor de 700 miembros.

ANSI: Es el Instituto Nacional Americano de Normas, siendo el encargado de evaluar la conformidad de aplicación de las normas en materia de redes móviles, tanto para Estados Unidos, como referencia a nivel internacional.

IETF: Es el grupo de trabajo de ingeniería de internet, el cual ofrece tanto a operadores, investigadores, la oportunidad de aportar para el desarrollo de la arquitectura de internet y su funcionamiento óptimo.

3GPP: Consiste en una agrupación de Entidades Normalizadoras(ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), para la búsqueda de documentos técnicos y normas que le den cobertura y aplicación en las redes móviles, donde incluye el acceso de radio, la red básica de transporte, calidad del servicio.

5.1.3. Estándar Itu- Imt2000:

Las comunicaciones móviles de manera técnica, es conocida como la IMT (Telecomunicaciones Móviles internacionales, en español). Sobre este estándar se han desarrollado las generaciones 3G. El cual abarca una serie de recomendaciones y cuestiones de estudio para la apropiación de las redes móviles en el mundo. Para el caso de esta investigación, se revelaran los documentos en el marco de la seguridad informática y sus requisitos técnicos.

5.1.3.1. Recomendación Itu-T Q.1701. Marco para las redes de las comunicaciones móviles internacionales -2000(IMT-2000):

Esta recomendación pertenece a la serie Q, encargada de la señalización y conmutación de la red, entregando los requisitos y protocolos de señalización para la red IMT-2000, aprobada en marzo de 1999, y se encuentra vigente.

Las redes IMT-2000, ofrecen un conjunto de capacidades de red necesarias para su funcionamiento, para el caso de la seguridad informática, los procedimientos de seguridad son los siguientes, en la tabla anexa.

Tabla 12. Capacidad de red, procedimientos de seguridad para red IMT-2000.

G)	Capacidades de red – Procedimientos de seguridad	1 Cifrado y autenticación de usuario para los modos circuito y paquetes 2 Identificación del terminal incluida la capacidad de detectar terminales robados y no autorizados 3 Autenticación mutua usuario-red 4 Soporte de mecanismos de autenticación y cifrado dependientes del servicio 5 Control del uso inadecuado de una red, es decir, impedir la utilización fraudulenta por un usuario no autorizado o por un usuario autorizado que excede su autoridad 6 Cifrado en la interfaz radioeléctrica (información de usuario y de control) 7 Intercepción legal (según los requisitos de regulaciones nacionales) 8 Privacidad de los datos relativos al usuario y al abonado (incluida la identidad de usuario) 9 Privacidad de los datos de facturación 10 Privacidad de los mensajes de usuario 11 Negociación de mecanismos de autenticación entre las redes de usuario, servidora y originaria 12 Información de eventos y limitación de eventos para soportar la prevención de fraudes

Fuente ITU-T Q.1701, página 11[25].

Según la tabla anterior, se marca el rumbo de la seguridad informáticas para las redes móviles 3G, teniendo en cuenta sus componentes básicos relacionados, representados en sus interfaces, como lo muestra la siguiente figura.

[25]International Telecommunication Union ITU. Serie Q: Conmutación Y Señalización. Requisitos y protocolos de señalización para la redIMT-2000. Marco para las redes de las telecomunicaciones móviles internacionales-2000 (IMT-2000). Recomendación UIT-T Q.1701. Comisión de Estudio 11 (1997-2000) del UIT-T. Ginebra, Suiza. 1999. 20 p.

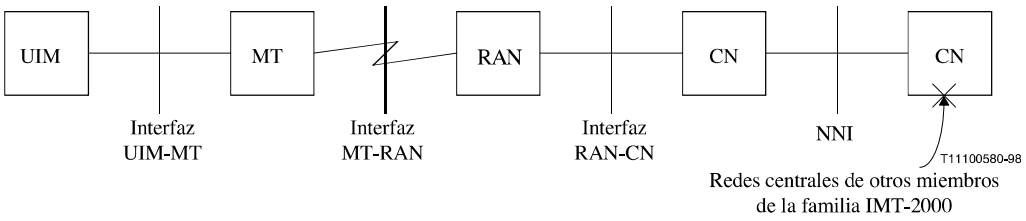

Figura 31. Interfaces físicas para un miembro de la familia IMT 2000.

Fuente ITU-T Q.1701, página 16[26].

Los dispositivos de la figura anterior, son, a saber: UMI (subsistema funcional módulo de identidad del usuario, user identity model), MT(subsistema funcional terminal móvil, mobile terminal), RAN(subsistema funcional red de acceso radioeléctrico, radio Access network), CN(subsistema funcional red central, core network).

5.1.3.2. Recomendación Itu-T Q.1702. Visión a largo plazo de las características de las redes posteriores a las redes de las comunicaciones móviles internacionales -2000(IMT-2000):

Esta recomendación pertenece a la serie Q, encargada de la señalización y conmutación de la red, entregando los requisitos y protocolos de señalización para la red IMT-2000, aprobada en junio de 2002, se encuentra vigente y ofrece una visión a largo plazo de las redes posteriores a la IMT-2000.

Para el caso de la esta recomendación contempla, que para el año 2010, la gestión de la movilidad en movimiento a altas velocidad, sobre todo el

[26]International Telecommunication Union Itu. Serie Q: Conmutación Y Señalización. Requisitos y protocolos de señalización para la redIMT-2000. Marco para las redes de las telecomunicaciones móviles internacionales-2000 (IMT-2000). RECOMENDACIÓN UIT-T Q.1701. Comisión de Estudio 11 (1997-2000) del UIT-T. Ginebra, Suiza. 1999. 20 p.

transporte, mediante el uso de IP, buscando la diversificación de los servicios de comunicaciones, entre las máquinas y las personas.

De igual manera, consideró debía existir un entorno de seguridad, con mecanismos de seguridad eficaces en entornos multimedia para el manejo de un flujo de datos alto; mecanismos de autenticación y autorización transparentes al usuario; la infraestructura de seguridad es soportada por los proveedores de servicios de comunicaciones; una red adaptativa ante el uso masivo de la red y un mecanismo de seguridad continuo, sin afectaciones de la transmisión del tráfico.

5.1.3.3. Recomendación Itu-T Q.1703. Marco de capacidades de servicio y de red desde la perspectiva de la red para los sistemas posteriores a las -2000(IMT-2000):

La seguridad informática es tomada como una capacidad esencial para el correcto funcionamiento de las aplicaciones de la red, así como la respuesta de sus servicios. Tuvo en cuenta que al momento de usar IP como su protocolo de transporte, las amenazas y vulnerabilidades que existen en internet, entraría a las redes móviles. Para ello, menciono lo servicios de seguridad que deberían tener estas redes:

Integridad, entendido como el mecanismo por el cual se asegura que el mensaje recibido es idéntico al enviado, y no ha sido modificado, reproducido, reordenado ni duplicado.

Confidencialidad, entendido como el mecanismo se mantiene los datos de usuario, en secreto a terceros.

No repudio, entendido como el mecanismo que evita que un actor de la comunicación que inicio una transmisión pueda luego negarla.

Autenticación mutua, entendido como el mecanismo que asegura que un actor es quien dice ser. Lo que busca es cada actor, verifique la identidad del otro y permita el acceso a los servicios, aplicación o acceso a la red.

Autorización, entendido como el mecanismo para controlar el acceso y uso de los recursos del usuario por parte del usuario.

Pero en la búsqueda de la seguridad informática mejorada, orientó en que las redes IMT2000, debían soportar las siguientes capacidades de gestión de seguridad: Determinación y prevención de intrusiones; denegación de intrusos, reparación de daños ocasionados, y recuperar las pérdidas producidas.

De igual manera tuvo en cuenta las amenazas informáticas genéricas, como son:

Invasión del privacidad, significado esto en la interceptación de la privacidad de datos.

Robo de servicio, significado como el acceso al sistema no autorizado, modificando o reproducción tráfico legitimo por el atacante.

Denegación del servicio (DoS, Denial of Service), significado como la perturbación del funcionamiento de los dispositivos de la red, impidiendo la oferta de servicios o de acceso al sistema.

Rastreo, significado como la supervisión del tráfico radio, para obtener información acerca del estado de la red, y buscando acceder a la misma de manera no autorizada.

Se debe tener en cuenta, que estos mecanismos corresponden a la capa de transporte, y que la implementación de la seguridad de extremo a extremo, depende de la capa de aplicación y debe ser transparente al usuario.

5.1.3.4. Recomendación Itu-T Q.1741.1.Referencias de IMT-2000 a la publicación de 1999 del sistema global para comunicaciones móviles que ha evolucionado hacia la red medular del sistema de telecomunicaciones móviles universales con la red de acceso de la red terrenal de acceso radioeléctrico del sistema de telecomunicaciones móviles universales:

En este apartado lo que se busca es mostrar las diferentes especificaciones Técnicas dadas por 3GPP, que continuamente son revisadas, y que están dadas por series. Para el caso de la seguridad informática en redes móviles, corresponde a la Serie 33, correspondientes a los aspectos relativos a la seguridad. A continuación se mencionan las especificaciones por temas, en la siguiente tabla:

Tabla 13. Especificaciones técnicas 3GPP relativas a la seguridad.

TEMA	ESPECIFICACIÒN
Arquitectura de seguridad	TS 33.102
Directrices de seguridad	TS 33.103

Requisitos de los algoritmos criptográficos	TS 33.105
Requisitos de interceptación licita	TS 33.106
Arquitectura y funciones de la interceptación licita	TS 33.107
Objetivos y principios de la seguridad	TS 33.120

Fuente. Fuente ITU-T Q.1741.1, página 150 a 153.

5.1.3.5. Recomendación Itu- T M.3210.1. Servicios de gestión de la RGT para la gestión de la seguridad de las telecomunicaciones móviles internacionales-2000 (IMT-2000):

La serie M, corresponde a la Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes, y en esta recomendación se tiene en cuenta la seguridad informática, teniendo en cuenta el servicio de gestión de la seguridad en dos ítem relevantes, uno de ellos son los aspectos de seguridad, donde se conceptúa que el operador del servicio debe implementar controles en la red para los fraudes y los atacantes, que utilizan la misma, pero sin pagar los cargos económicos que ello implica.

Y el otro aspecto relevante, es como describen el servicio de gestión, para lo cual se anexa la siguiente figura.

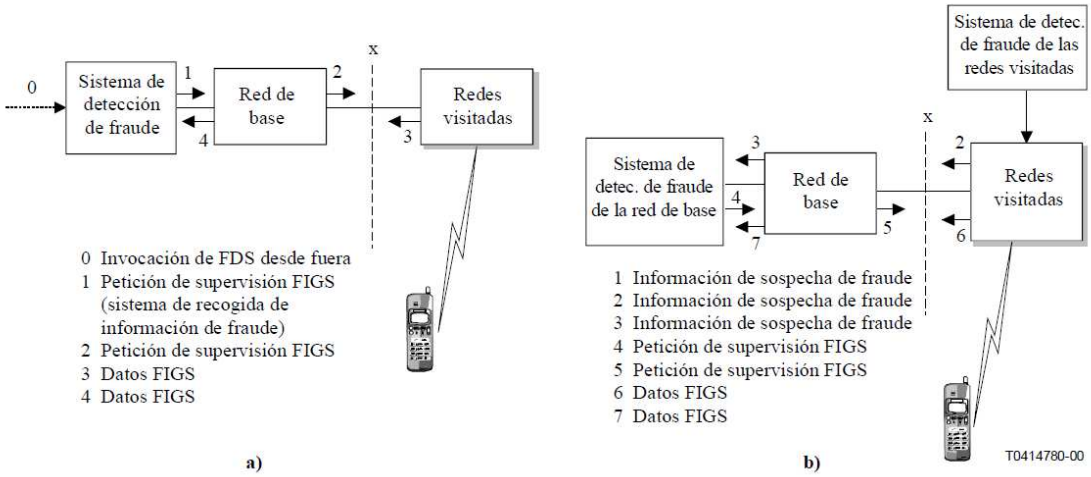

Figura 32. Servicio de gestión de la seguridad IMT-2000.

Fuente. ITU-T M.3210.1, página 4.

En la anterior imagen, se muestra como se describe el sistema de detección de fraude (FDS), cuando el atacante pasa de una red a otras y la supervisión que hace la red acerca de las actividades del atacante (abonado).

5.1.3.6. Recomendación Itu-T Y.2701.Requisitos de seguridad para las redes de la próxima generación, versión 1:

La serie Y, corresponde a la infraestructura mundial de la información, aspectos del protocolo de internet y redes de la próxima generación, y en esta recomendación se tiene en cuenta la seguridad informática, teniendo en cuenta los requisitos de seguridad que buscan proteger los siguientes componentes del entorno multired:

- La infraestructura de la red y el proveedor de servicios y sus activos, sus recursos, sus comunicaciones y sus servicios.
- Servicios y capacidades de las NGN.

- Comunicaciones de información de usuario extremo.

Para lograr la protección deseada, ha tenido en cuenta las dimensiones de la seguridad definidas en la ITU-T X.805, a saber:

- Control de acceso.
- Autenticación.
- No repudio.
- Confidencialidad de datos.
- Seguridad de las comunicaciones.
- Integridad de datos.
- Disponibilidad.
- Privacidad.
-

Para comprender mejor el enfoque dado en mencionada recomendación, se anexa la siguiente figura:

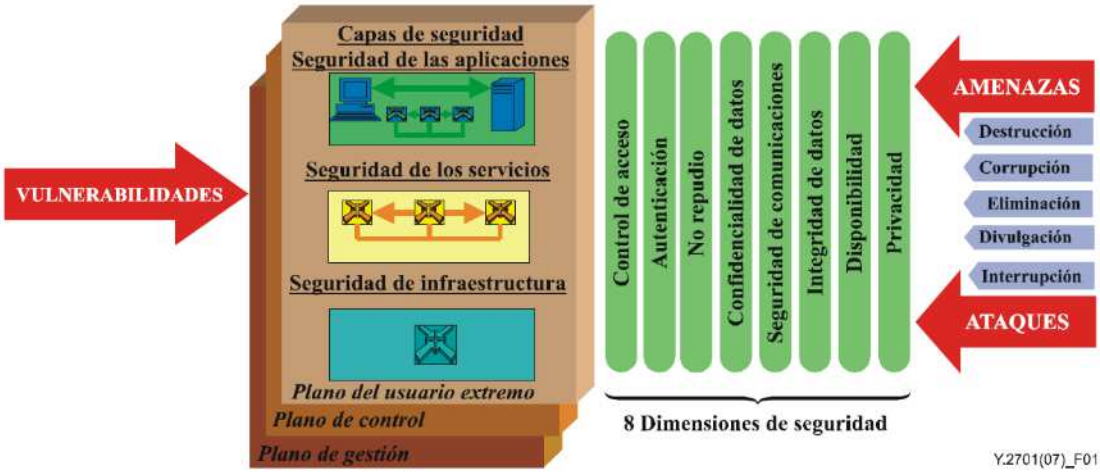

Figura 33. Arquitectura de seguridad de ITU-T X.805.

Fuente: ITU-T Y.2701, página 2.

En la figura se evidencia, los elementos claves a tener en cuenta para la formulación de la seguridad informática aplicada a las redes móviles, en donde las vulnerabilidades, afectan los servicios que ofrece la red, desde el plano de gestión hasta el plano de usuario extremo, en donde las dimensiones de seguridad, hacen frente a las amenazas y posibles ataques que pueda sufrir la arquitectura.

Para llevar este modelo a la realidad, los operadores deben identificar los activos como recursos con información de interface de red que se deben proteger, y de igual manera las amenazadas que deben minimizarse. Para comprender el concepto, se debe tener en cuenta los elementos de red, interfaces (UNI, ANI y NNI), sistemas de gestión y comunicaciones de señalización, gestión y medio/portador, los cuales se han organizado por UNI (interfaz usuario – red), por interfaz de transporte, interfaces de servicio e interfaces de gestión. Para lograr comprender la finalidad de las mismas, se muestran en las siguientes tablas.

Tabla 14. Ejemplo de activos, recursos e información UNI.

Ejemplo	Objetivos y metas
Recursos de usuario extremo: • Dispositivos de usuario • Pasarelas de la red de usuario • Pasarelas de redes institucionales	a) Proteger el equipo de usuario extremo conectado a la red (por ejemplo, terminales, red de usuario y pasarelas de redes institucionales) contra los ataques originados en la red (por ejemplo, ataques para destruir, corromper y modificar el equipo de usuario). b) Proteger contra la interrupción de servicios (por ejemplo, ataques de denegación de servicio) y garantizar la disponibilidad del servicio. c) Proteger la red de acceso no autorizado (por ejemplo, usuarios y dispositivos de usuario no autorizados).
Información de usuario extremo: • Información de abono. • Información de identidad. • Información de ubicación.	a) Proteger contra la corrupción o modificación de la información. b) Proteger contra el robo, eliminación o pérdida (por ejemplo, robo de identidad). c) Proteger contra la divulgación (por ejemplo, acceso no autorizado a la información de ubicación).
Información de proveedor de NGN Información de identidad	a) Proteger contra la corrupción o modificación de la información. b) Proteger contra el robo, eliminación o pérdida (por ejemplo, robo de identidad). c) Proteger contra la divulgación (por ejemplo, acceso no autorizado a la información de ubicación).

Fuente: ITU-T Y.2701, página 15.

Tabla 15. Ejemplo de activos, recursos e información UNI.

Ejemplo	Objetivos y metas
Interfaces UNI	a) Estrato de transporte – Proporciona la protección de seguridad al tráfico de medios/portador que atraviese las interfaces UNI. b) Estrato de servicio (control de servicio) – Proporcionar protección de seguridad a la señalización y gestión en las interfaces UNI (por ejemplo, SIP, HTTP, RDSI y H.248). c) Estrato de servicio (soporte de aplicación y servicio) – Proporciona protección y seguridad a las funciones de control de aplicación de servicios en las interfaces UNI (por ejemplo, señalización en banda).

Fuente ITU-T Y.2701, página 16.

Tabla 16. Ejemplo de activos, recursos, información de interfaces del estrato de transporte.

Ejemplos	Metas y Objetivos
Recursos del estrato de transporte: • Elementos de red de transporte (por ejemplo, encaminadores IP, nodos MPLS). • Enlaces de transmisión. • Información de encaminamiento (por ejemplo, servidores DNS). • Información del perfil de usuario de transporte (por ejemplo, bases de datos y almacén de datos de transporte).	a) Proteger todos los elementos, componentes y funciones de la red de transporte contra el acceso no autorizado. b) Proteger la integridad de los elementos, componentes y funciones de la red de transporte. c) Proteger la disponibilidad de los elementos, componentes y funciones de la red de transporte. Protección contra la interrupción de los servicios (por ejemplo, contra ataques de denegación de servicio). d) Proteger contra la divulgación de cualquier tipo de información privada de usuario o red.
Comunicaciones internas del sistema en el estrato de transporte (comunicaciones dentro de la red de un proveedor de red).	a) Proporcionar protección de seguridad al tráfico de medios/portador entre sistemas dentro de una red de proveedor. b) Proporcionar protección de seguridad a la señalización y gestión del control de transporte (por ejemplo, OSPF) dentro de una red de proveedor. c) Proporcionar seguridad a la señalización entre sistemas en el estrato de servicio (por ejemplo, servidores de aplicación) y los sistemas en el estrato de transporte (por ejemplo, encaminadores IP).
Interfaces de transporte y comunicaciones.	a) Proporcionar protección de seguridad al tráfico de medios/portador en las interfaces UNI, NNI y ANI de transporte. b) Proporcionar protección de seguridad a la señalización del control de transporte (por ejemplo, OSPF) y gestión en las interfaces UNI, NNI y ANI.

Fuente ITU-T Y.2701, página 16.

Tabla 17. Ejemplo de activos, recursos, información e interfaces del estrato de servicio.

	Ejemplos	Metas y objetivos
Estrato de servicio – Control de servicios	Estrato de servicios – Recursos o control de servicios. • Elementos de red de control de servicio (por ejemplo CSC-FE, SL-FE, MRP-FE, pasarelas, S/BC).	a) Proteger todos los elementos, componentes y funciones de red de control de servicio contra el acceso no autorizado. b) Proteger la integridad de los elementos, componentes y funciones de red de control de servicio, incluida contra la corrupción o modificación de la información. c) Proteger la disponibilidad de los elementos, componentes y funciones de red de control de servicio. Proteger contra la interrupción de los servicios (por ejemplo, contra ataques de denegación de servicio).
	Estrato de servicio – Información de control de servicio. • Información de abonado (por ejemplo, bases de datos y depósito de datos que contienen los perfiles de usuario y los perfiles de servicio). • Información de proveedor de NGN (por ejemplo, bases de datos y depósito de datos que contiene la información de encaminamiento, numeración y direccionamiento).	a) Proteger contra la corrupción o modificación de datos e información. b) Proteger contra robo, eliminación o pérdida (por ejemplo, robo de identidad). c) Proteger contra la divulgación (por ejemplo, acceso no autorizado e información privada de usuario y red).
	Estrato de servicio – Comunicación entre sistemas de control de servicio.	Proporcionar protección de seguridad en la señalización entre sistemas (por ejemplo SIP, RADIOS, Diameter) dentro de una red de un proveedor de red (por ejemplo, señalización CSCF a HSS).
	Interfaces y comunicaciones.	Proporcionar protección de seguridad a la señalización y gestión en las interfaces UNI, NNI y ANI.

Fuente ITU-T Y.2701, página 17.

Tabla 18. Ejemplo de activos, recursos, información e interfaces del estrato de servicio.

	Ejemplos	Metas y objetivos
Estrato de servicio – Soporte de aplicaciones y servicios	Estratos de servicios – Recursos de soporte de aplicaciones y servicios: • Elementos y plataformas de red de soporte de aplicaciones y servicios (por ejemplo, servidores de aplicación, bases de datos, portales web).	a) Proteger todos los elementos, componentes y funciones de red de soporte de servicios contra el acceso no autorizado. b) Proteger la integridad de los elementos, componentes y funciones de red de soportes de servicios, incluido contra la corrupción o modificación de la información. c) Proteger la disponibilidad de los elementos, componentes y funciones de red de soporte de servicios. d) Protección contra la interrupción de los servicios (es decir, contra los ataques de denegación de servicio).
	Estrato de servicios – Información de soporte de aplicaciones y servicios: • Información de aplicaciones y servicios. • Información de abono.	a) Proteger contra la corrupción o modificación de datos e información. b) Protección contra el robo, eliminación o pérdida (por ejemplo, robo de identidad). c) Protección contra la divulgación (por ejemplo, acceso no autorizado a la información privada de usuario y red).
	Interfaces.	a) Proporcionar protección de seguridad a los elementos y recursos de red para cualquier tipo de acceso de proveedor de aplicación (por ejemplo, Parlay y pasarelas de Alianza Móvil Abierta). b) Proporcionar protección de seguridad a las interfaces UNI, NNI y ANI. c) Proporcionar protección de seguridad de la señalización y gestión del tráfico en las interfaces ANI.

Fuente ITU-T Y.2701, página 18.

Tabla 19. Ejemplo de activos, recursos, información e interfaces de gestión.

Ejemplo	Metas y objetivos
Recursos de gestión • Sistemas de gestión del estrato de transporte (por ejemplo, gestión de elementos de red, sistemas de gestión de red y de gestión de servicios). • Sistemas de gestión de estratos de servicios (por ejemplo, gestión de elementos de red, sistemas de gestión de red y de gestión de servicios).	a) Proteger todos los elementos, componentes, funciones e interfaces de red de gestión contra el acceso no autorizado. b) Proteger la integridad de los elementos, componentes, funciones interfaces de red de gestión, incluida la protección contra la corrupción o modificación de la información. c) Proteger la disponibilidad de los elementos, componentes, funciones interfaces de red de gestión. Protección contra la interrupción de los servicios (es decir, contra los ataques de denegación de servicio).

Fuente ITU-T Y.2701, página 18.

Tabla 20. Ejemplo de activos, recursos, información e interfaces de gestión.

Ejemplo	Metas y objetivos
Comunicaciones entre sistemas dentro de la red de un proveedor de red.	a) Proporciona protección de seguridad al tráfico de gestión entre sistemas de gestión dentro de una red (por ejemplo, estrato de servicios). b) Proporciona la protección de seguridad al tráfico de gestión entre la red del usuario y el estrato de transporte y el estrato de servicio de un proveedor de red.
Interfaces y comunicaciones entre sistemas.	a) Proporciona seguridad a las interfaces de gestión de red internas y cualquier interfaz de gestión UNI, NNI y ANI. b) Proporciona la protección de seguridad al tráfico de gestión en las interfaces UNI, ANI y NNI.

Fuente:ITU-T Y.2701, página 19.

5.1.3.7. Recomendación Itu-T Y.2704. Mecanismos y procedimientos de seguridad en las redes de próxima generación:

En este apartado, se hace relevante la utilización de credenciales de certificados de clave pública X.509, el cual constituye un documento digital que incluye un identificador de identidad, sus atributos, una clave pública que es propiedad de dicha entidad e información de autenticación de otro tipo, como quien expide el certificado, la lista de revocación o CRL, y los plazos de vencimiento. En la siguiente tabla, se detallan algunos de los campos contenidos en un certificado de clave pública X.509.

Tabla 21. Algunos campos básicos de un certificado de clave pública X.509.

Nombre del campo	Descripción
Asunto	Identifica la entidad asociada con el certificado de clave pública (el nombre de directorio distinguido del titular del certificado)
Número de serie	Identificador único del certificado
Entidad de expedición	Identifica la entidad que firma y expide el certificado (el nombre de directorio distinguido de la CA)
Válido a partir de	Fecha y hora de inicio de la validez del certificado
Válido hasta	Fecha y hora del término de la validez del certificado
Clave pública	Clave pública del titular del certificado
Versión	Versión del certificado de clave pública X.509 codificado
Nombre alternativo del asunto	Otro identificador del titular del certificado
Puntos de distribución de CRL	Nombre o dirección del punto de distribución de CRL
Autoridad de acceso a la información	Nombre o dirección para acceder a la información acerca de la CA
Utilización de clave ampliada	Descripción de los propósitos para los cuales puede utilizarse el certificado (lista de identificadores de objetos definidos (OID) de UIT-T | ISO/CEI) [UIT-T X.660]
Políticas de aplicación	Aplicación y servicios que puede utilizar el certificado (especificados por el identificador de objetos)
Políticas de certificación	Políticas y mecanismos utilizados por la CA para la recepción de peticiones de tramitación, autorización, expedición y gestión de certificados
Algoritmo de la firma	Algoritmo identificador del algoritmo y la función de troceado utilizados por la CA para firmar el certificado (por ejemplo, SHA-1 con RSA)
Valor de la firma	La firma del certificado

Fuente: ITU-T Y.2704, página 13.

Estos elementos de la NGN, pueden utilizar certificados de clave pública para establecer asociaciones de seguridad con otros elementos de red, así mutuamente se identifican y autentican.

5.1.3.8. Recomendación Itu-T Y.2760: Marco de seguridad para la movilidad de las redes NGN:

Esta recomendación va enfocada a la capa de transporte, se tratan lo temas de requisitos de seguridad, los mecanismos adoptados y los procedimientos de gestión y control de la movilidad de las NGN.

Para el entendimiento de la funcionalidad de la seguridad en la red móvil, se contemplan las siguientes abreviaturas y acrónimos:

ABG-FE: Entidad funcional de pasarela de frontera de acceso (Access border Gateway functional entity).

AM-FE: Entidad funcional de gestión de acceso (Access management functional entity).

AN-FE: Entidad funcional de nodo de acceso (Access node functional entity).

EN-FE: Entidad funcional de nodo extremo (edge node functional entity).

MMCF: Funciones de control de gestión de movilidad (mobilitymanagement control functions).

TAA-FE: Entidad funcional de autorización y autentificación de transporte (transport authentication and authorization functional entity).

TLM-FE: Entidad funcional de gestión de ubicación de transporte (transport location management functional entity).

TUP-FE: Entidad funcional de perfil de usuario de transporte (transport user profile functional entity).

UE: Equipo de usuario (user equipment).

AR-FE: Entidad funcional de retransmisión de acceso (Access relay functional entity).

Para comprender el marco referencia de esta Recomendación, se inicia el estudio desde la Autenticación y gestión de claves, se ejemplifica con la siguiente figura:

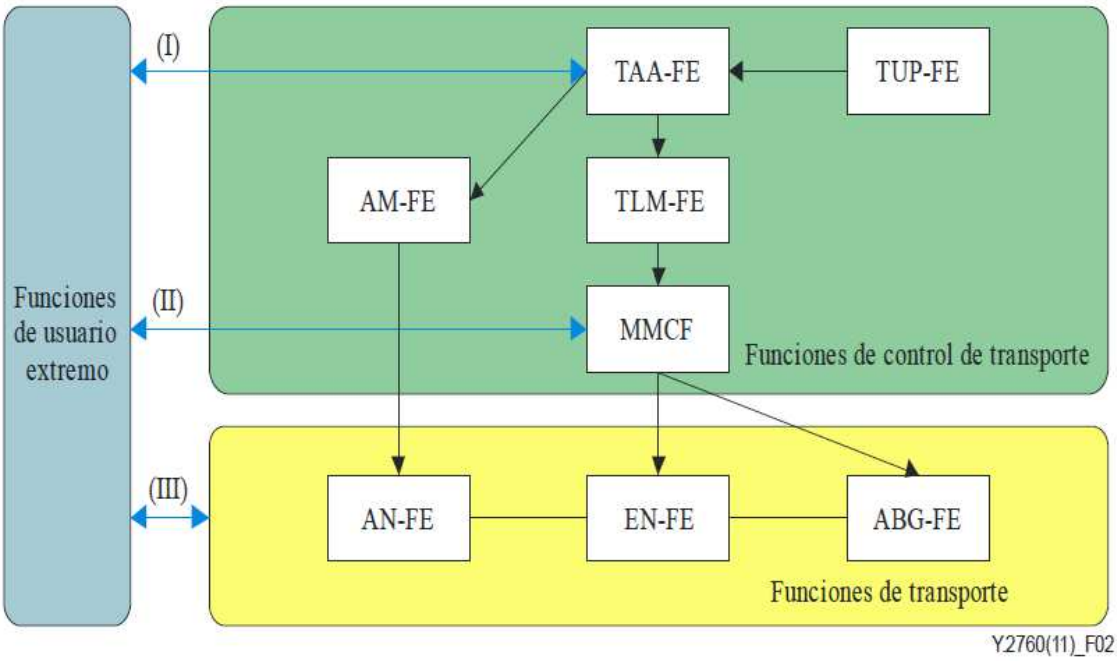

Figura 34. Marco genérico de claves para la seguridad de la movilidad en las NGN.

Fuente ITU-T Y.2760, página 8.

Se pueden identificar tres momentos en la autenticación, donde el UE, se autentica mutuamente con las diferentes instancias funcionales de la red, donde TUP-FE, envía parámetros de autenticación a TAA-FE, una vez autenticados, son generadas las claves de sesión, las cuales son empleados tanto por UE como por TAA-FE. Estas claves se pueden transmitir a entidades como AM-FE y la MMCF.

Para comprender en mayor grado la funcionalidad de autenticación, se ilustra mediante la siguiente figura, el procedimiento genérico necesario.

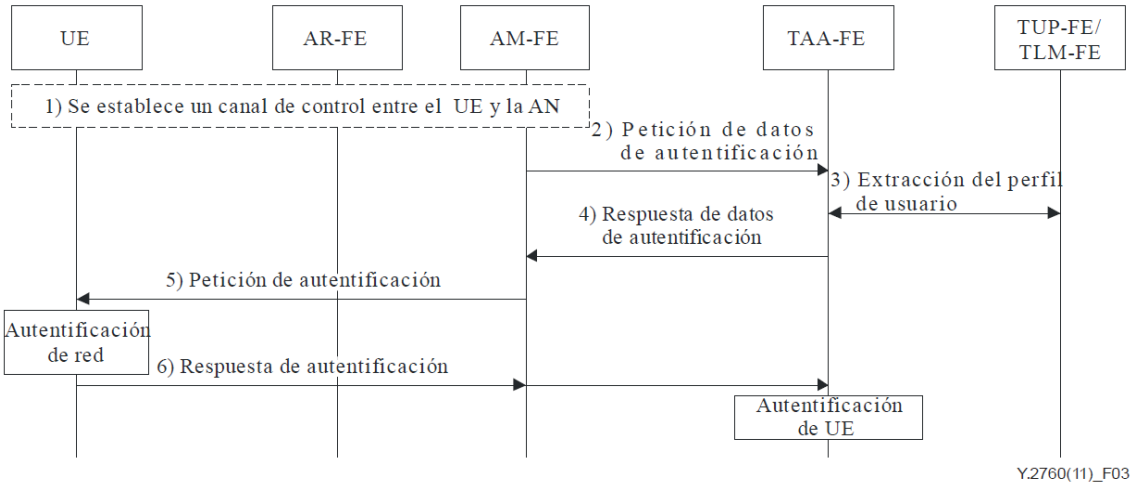

Figura 35. Procedimiento genérico de autenticación.

Fuente ITU-T Y.2760, página 9.

5.1.3.9. Recomendación Itu-T Y.3001: Redes del futuro, objetivos y metas de diseño:

En esta recomendación se recogen los cuatro objetivos, los de servicio, de datos, medioambientales y socioeconómicos. De igual manera, las doce metas de diseño: diversidad de servicios, flexibilidad funcional, virtualización de los recursos, acceso a los datos, consumo energético, universalización de servicio, incentivos económicos, gestión de red, movilidad, optimización, identificación, fiabilidad y seguridad. Esencialmente las redes del futuro se caracterizan por la virtualización y la movilidad, teniendo en cuenta la cantidad de datos y de servicios ofrecidos, donde se necesitará un control de acceso multinivel (identificación, autenticación y autorización del usuario, sin dejar de lado, los requisitos de seguridad de la UIT-T Y.2701. De igual manera, se incluye en esta recomendación la protección de la identidad en línea y de la reputación, adicionando la capacidad del mismo usuario controle las comunicaciones no solicitadas.

5.1.3.10. Recomendación Itu- T X.805. Arquitectura de seguridad para sistemas de comunicaciones de extremo a extremo:

Corresponde esta recomendación a la Serie X, redes de datos y comunicaciones entre sistemas abiertos, hacienda especial énfasis en la seguridad.

En esta recomendación se busca definir los elementos de seguridad de la arquitectura, que protejan la red de extreme a extremo de manera correcta.

Para el caso de estudio, se aplican las dimensiones de la seguridad para contrarrestar las amenazas. Se ejemplifica en la siguiente tabla:

Tabla 22. Las dimensiones de seguridad que corresponden a las amenazas.

Dimensiones de seguridad	Amenazas contra la seguridad				
	Destrucción de información y otros recursos	Corrupción o modificación de información	Robo, supresión o pérdida de información y de otros recursos	Revelación de información	Interrupción de servicios
Control de acceso	Y	Y	Y	Y	
Autenticación			Y	Y	
No repudio	Y	Y	Y	Y	Y
Confidencialidad de datos			Y	Y	
Seguridad de la comunicación			Y	Y	
Integridad de los datos	Y	Y			
Disponibilidad	Y				Y
Privacidad				Y	

Fuente ITU-T X.805, página 8.

En la tabla anterior, se define que donde se encuentre la “Y”, la dimensión de seguridad aplicada, contrarrestará la amanezca contra la seguridad.

Siguiendo con la revisión teórica de los contenidos de las normas de seguridad informática aplicada a las redes móviles, y comprender su aplicación en esta recomendación, se debe mencionar que existen tres capas de seguridad, la de infraestructura, la de servicios y la de aplicaciones; a la par a esta consideración, se encuentran los tres planos de seguridad, de gestión, de control y de usuario de extremo; la combinación de los planos y las capas de seguridad, ofrecen la visión de las ocho dimensiones de la seguridad. En consecuencias los objetivos de seguridad cambian en cada intersección de capa y plano, suponiendo medidas de seguridad diferente. Lo anterior se evidencia en la siguiente figura.

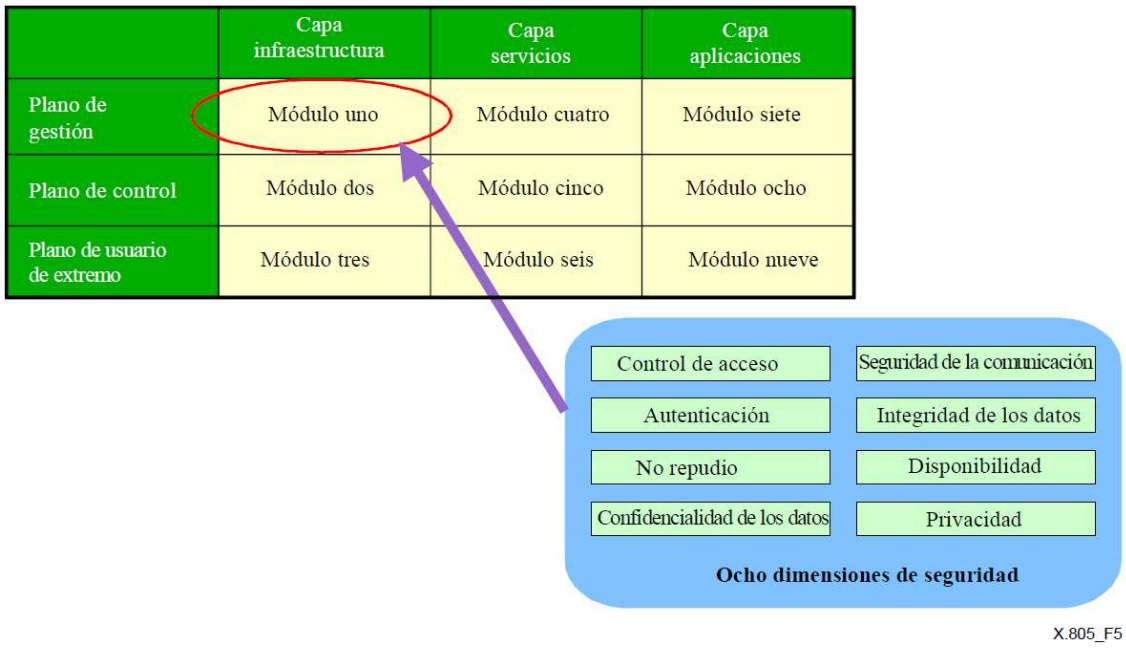

Figura 36. Arquitectura de seguridad representada en un cuadro de combinación, capa y plano.

Fuente ITU-T X.805, página 10.

Para comprender los objetivos de seguridad aplicadas en cada capa de seguridad, teniendo en cuenta las dimensiones de seguridad, se ilustra en las siguientes tablas.

Tabla 23. Aplicación de las dimensiones de seguridad a la capa de infraestructura en el plano de gestión.

Módulo 1: capa infraestructura, plano de gestión	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que las personas y los dispositivos autorizados (por ejemplo dispositivos gestionados por protocolo SNMP) son los únicos que pueden realizar actividades de gestión o administración en el dispositivo de red o el enlace de comunicaciones. Se aplica por igual a la gestión directa desde un puerto de configuración y la gestión del dispositivo a distancia.
Autenticación	Verificar la identidad de la persona o el dispositivo que realizan la actividad de gestión o administrativa en el dispositivo de red o el enlace de comunicaciones. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas o dispositivos que realizan cada actividad de gestión o administrativa en el dispositivo de red o el enlace de comunicaciones, y la acción realizada. Este registro puede utilizarse para probar quién ha originado la actividad de gestión o administrativa .
Confidencialidad de los datos	Proteger la información de configuración del dispositivo de red o el enlace de comunicaciones contra el acceso o la consulta no autorizados. Se aplica a la información de configuración que reside en el dispositivo de red o el enlace de comunicaciones, la información de configuración que se transmite al dispositivo de red o el enlace de comunicaciones, y la información de configuración duplicada para seguridad y almacenada en sistemas no conectados. Proteger la información administrativa de autenticación (por ejemplo, identificación y contraseñas de administrador) contra el acceso o la consulta no autorizados. Las técnicas que se utilizan para el control de acceso pueden contribuir a la confidencialidad de datos.
Seguridad de la comunicación	En el caso de la gestión a distancia de un dispositivo de red o un enlace de comunicaciones, garantizar que la información de gestión sólo circula entre las estaciones de gestión distantes y los dispositivos o enlaces de comunicaciones gestionados. La información de gestión no será desviada ni interceptada entre estos puntos extremo. Se incluye en esta protección la información administrativa de autenticación (por ejemplo, identificación y contraseñas de administrador).
Integridad de los datos	Proteger la información de configuración de dispositivos de red o enlaces de comunicaciones contra la modificación, la supresión, la creación y la reactuación sin autorización. Se aplica a la información de configuración que reside en el dispositivo de red o el enlace de comunicaciones, y también la información de configuración que está en tránsito o almacenada en sistemas no conectados. Se incluye en esta protección la información administrativa de autenticación (por ejemplo, identificación y contraseñas de administrador).
Disponibilidad	Garantizar que nada impedirá que las personas y los dispositivos autorizados puedan gestionar el dispositivo de red o el enlace de comunicaciones. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS), y contra ataques pasivos, por ejemplo la modificación o la supresión de la información administrativa de autenticación (por ejemplo, identificación y contraseñas de administrador).
Privacidad	Garantizar que la información que permite identificar el dispositivo de red o el enlace de comunicaciones no está disponible para personas y dispositivos no autorizados. Son ejemplos de este tipo de información la dirección IP o el nombre de dominio DNS de un dispositivo de red. La posibilidad de identificar un dispositivo de red permite, por ejemplo, dirigir un ataque.

Fuente ITU-T X.805 página 11.

Tabla 24. Aplicación de las dimensiones de seguridad a la capa de infraestructura en el plano de control.

Módulo 2 – Capa infraestructura, plano de control	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que las personas y los dispositivos autorizados son los únicos que pueden acceder a la información de control que reside en el dispositivo de red (por ejemplo, un cuadro de encaminamiento) o está almacenada en un dispositivo no conectado. Garantizar que el dispositivo de red sólo aceptará mensajes de información de control de dispositivos de red autorizados (por ejemplo, actualizaciones de encaminamiento).
Autenticación	Verificar la identidad de la persona o el dispositivo que observan o modifican información de control residente en el dispositivo de red. Verificar la identidad del dispositivo que envía información de control a un dispositivo de red. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas o dispositivos que han observado o modificado información de control en el dispositivo de red, y la acción realizada. Este registro puede utilizarse como prueba de acceso a la información de control o modificación de esa información. Crear un registro de los dispositivos emisores de mensajes de control enviados al dispositivo de red, y la acción realizada. Este registro puede utilizarse para probar que el dispositivo es el emisor del mensaje de control.
Confidencialidad de los datos	Proteger contra el acceso o la consulta no autorizados la información de control residente en un dispositivo de red o un sistema de almacenamiento no conectado. Las técnicas que se utilizan para el control de acceso pueden contribuir a la confidencialidad de la información de control que reside en el dispositivo de red. Proteger la información de control destinada a un dispositivo de red contra el acceso o la consulta no autorizados durante el transporte por la red.
Seguridad de la comunicación	Garantizar que la información de control transportada por la red (por ejemplo, actualización de encaminamiento) sólo circula entre la fuente de esa información y el destino especificado. La información de control no será desviada ni interceptada entre estos puntos extremo.
Integridad de los datos	Proteger la información de control que reside en los dispositivos de red, que está en tránsito por la red o almacenada fuera de línea, contra la modificación, la supresión, la creación y la reactuación sin autorización.
Disponibilidad	Garantizar que los dispositivos de red están siempre disponibles para recibir información de control de las fuentes autorizadas, lo que incluye una protección contra ataques deliberados como la denegación de servicio (DoS) y contra situaciones accidentales como el cambio rápido de rutas.
Privacidad	Garantizar que la información que permite identificar el dispositivo de red o el enlace de comunicaciones no está disponible para personas y dispositivos no autorizados. Son ejemplos de este tipo de información la dirección IP o el nombre de dominio DNS de un dispositivo de red. La posibilidad de identificar dispositivos de red o enlaces de comunicaciones permite, por ejemplo, dirigir un ataque.

Fuente ITU-T X.805, página 12.

Tabla 25. Aplicación de las dimensiones de seguridad a la capa de infraestructura en el plano de usuario de extremo.

Módulo 3: capa infraestructura, plano de usuario de extremo	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que las personas y los dispositivos autorizados son los únicos que pueden acceder a los datos de usuario de extremo que transitan por un elemento de red o un enlace de comunicación, o que residen en un dispositivo no conectado.
Autenticación	Verificar la identidad de la persona o el dispositivo que intentan acceder a los datos de usuario de extremo que transitan por un elemento de red o un enlace de comunicación, o que residen en un dispositivo no conectado. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas o dispositivos que han accedido a los datos de usuario de extremo que transitan por un elemento de red o un enlace de comunicación, o que residen en un dispositivo no conectado, y la acción realizada. Este registro puede utilizarse como prueba de acceso a los datos de usuario de extremo.
Confidencialidad de los datos	Proteger los datos de usuario de extremo que transitan por un elemento de red o un enlace de comunicación, o que residen en un dispositivo no conectado, contra el acceso o la consulta no autorizados. Las técnicas que se utilizan para el control de acceso pueden contribuir a la confidencialidad de los datos de usuario de extremo.
Seguridad de la comunicación	Garantizar que los datos de usuario de extremo que transitan por un elemento de red o un enlace de comunicación no son desviados ni interceptados entre estos puntos extremo sin una autorización de acceso (por ejemplo, interceptación legal).
Integridad de los datos	Proteger los datos de usuario de extremo que transitan por un elemento de red o un enlace de comunicación, o que residen en un dispositivo no conectado, contra la modificación, la supresión, la creación y la reactuación sin autorización.
Disponibilidad	Garantizar que nada impedirá que las personas (incluyendo usuarios de extremo) y los dispositivos autorizados puedan acceder a los datos de usuario de extremo que residen en un dispositivo no conectado. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS) y contra ataques pasivos, por ejemplo la modificación o la supresión de la información de autenticación (por ejemplo, identificación y contraseñas de usuario o de administrador).
Privacidad	Garantizar que los elementos de red no proporcionan información sobre las actividades del usuario de extremo en la red (por ejemplo, la posición geográfica del usuario o los sitios web visitados) a personas o dispositivos no autorizados.

Fuente ITU-T X.805 página 13.

Tabla 26. Aplicación de las dimensiones de seguridad a la capa de servicios en el plano de gestión.

Módulo 4: capa servicios, plano de gestión	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que las personas y los dispositivos autorizados son los únicos que pueden realizar las actividades de gestión o administración del servicio de red (por ejemplo dar de alta los usuarios del servicio).
Autenticación	Verificar la identidad de las personas o los dispositivos que intentan realizar actividades de gestión o administración del servicio de red. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas o dispositivos que realizan cada actividad de gestión o administrativa del servicio de red, y la acción realizada. Este registro puede utilizarse para probar que esa persona o dispositivo ha realizado la actividad de gestión o administrativa.
Confidencialidad de los datos	Proteger la información de configuración y gestión del servicio de red (por ejemplo, los valores del protocolo de seguridad IPSec de un cliente para un servicio RPV, que se pueden descargar) contra el acceso o la consulta no autorizados. Se aplica a la información de configuración y gestión que reside en dispositivos de red, que se transmite por la red o que está almacenada en sistemas no conectados. Proteger la información de gestión o administrativa del servicio de red (por ejemplo, identificación y contraseñas de usuario o de administrador) contra el acceso o la consulta no autorizados.
Seguridad de la comunicación	En el caso de la gestión a distancia de un servicio de red, garantizar que la información de gestión o administrativa sólo circula entre la estación de gestión distante y los dispositivos gestionados en el contexto del servicio de red. La información de gestión y administrativa no será desviada ni interceptada entre estos puntos extremo. Se incluye en esta protección la información de autenticación del servicio de red (por ejemplo, identificación y contraseñas de usuario o de administrador).
Integridad de los datos	Proteger la información de gestión y administrativa de los servicios de red contra la modificación, la supresión, la creación y la reactuación sin autorización. Se aplica a la información de gestión y administrativa que reside en dispositivos de red, que se transmite por la red o está almacenada en sistemas no conectados. Se incluye en esta protección la información de autenticación del servicio de red (por ejemplo, identificación y contraseñas de usuario o de administrador).
Disponibilidad	Garantizar que nada impedirá que las personas y los dispositivos autorizados puedan gestionar el servicio de red. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS), y contra ataques pasivos, por ejemplo la modificación o la supresión de la información de autenticación administrativa del servicio de red (por ejemplo, identificación y contraseñas de administrador).
Privacidad	Garantizar que la información que permite identificar los sistemas de gestión o administrativos del servicio de red no está disponible para personas y dispositivos no autorizados. Son ejemplos de este tipo de información la dirección IP o el nombre de dominio DNS de un sistema. La posibilidad de identificar los sistemas administrativos de un servicio de red permite, por ejemplo, dirigir un ataque.

Fuente ITU-T X.805, página 14.

Tabla 27. Aplicación de las dimensiones de seguridad a la capa de servicios en el plano de control.

Módulo 5: capa servicios, plano de control	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que la información de control que recibe un dispositivo de red para un servicio de red proviene de una fuente autorizada (por ejemplo, mensaje de inicio de sesión VoIP emitido por un usuario o dispositivo autorizados) antes de aceptarla. En el caso de VoIP, proteger contra la falsificación del mensaje de inicio de sesión en un dispositivo no autorizado.
Autenticación	Verificar la identidad de la fuente de información de control del servicio de red enviada a dispositivos de red que participan en ese servicio. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas o dispositivos que emiten los mensajes de control del servicio de red recibidos por un dispositivo de red que participa en ese servicio, y la acción realizada. Este registro puede utilizarse para probar que esa persona o dispositivo ha emitido el mensaje de control del servicio de red.
Confidencialidad de los datos	Proteger contra el acceso o la consulta no autorizados la información de control del servicio de red que reside en un dispositivo de red (por ejemplo, bases de datos de sesiones IPSec), transportada por la red o almacenada en sistemas no conectados. Las técnicas que se utilizan para el control de acceso pueden contribuir a la confidencialidad de la información de control que reside en el dispositivo de red, para un servicio de red.
Seguridad de la comunicación	Garantizar que la información transportada por la red para el control de un servicio de red (por ejemplo, mensajes de negociación de clave IPSec) sólo circula entre la fuente de esta información de control y el destino especificado. La información de control del servicio de red no será desviada ni interceptada entre estos puntos extremo.
Integridad de los datos	Proteger contra la modificación, la supresión, la creación y la reactuación sin autorización, la información de control de un servicio de red que reside en dispositivos de red, que transita por la red o está almacenada en sistemas no conectados.
Disponibilidad	Garantizar que los dispositivos de red que participan en un servicio de red están siempre disponibles para recibir información de control de fuentes autorizadas. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS).
Privacidad	Garantizar que la información que permite identificar los dispositivos de red y los enlaces de comunicación que participan en un servicio de red no está disponible para personas y dispositivos no autorizados. Son ejemplos de este tipo de información la dirección IP o el nombre de dominio DNS de un dispositivo de red. La posibilidad de identificar los dispositivos de red y los enlaces de comunicación permite, por ejemplo, dirigir un ataque.

Fuente ITU-T X.805, página 15.

Tabla 28. Aplicación de las dimensiones de seguridad a la capa de servicios en el plano de usuario de extremo.

Módulo 6: capa servicios, plano usuario de extremo	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que las personas y los dispositivos autorizados son los únicos que pueden acceder al servicio de red y utilizarlo.
Autenticación	Verificar la identidad del usuario o el dispositivo que intentan acceder al servicio de red y utilizarlo. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas y los dispositivos que han tenido acceso y han utilizado el servicio de red, y la acción realizada. Este registro puede utilizarse para probar que el usuario de extremo o el dispositivo han accedido al servicio de red y lo han utilizado.
Confidencialidad de los datos	Proteger contra el acceso o la consulta no autorizados los datos de usuario de extremo transportados, procesados o almacenados por un servicio de red. Las técnicas que se utilizan para el control de acceso pueden contribuir a la confidencialidad de los datos de usuario de extremo.
Seguridad de la comunicación	Garantizar que los datos de usuario de extremo transportados, procesados o almacenados por un servicio de red no son desviados ni interceptados durante el transporte entre estos puntos extremo sin una autorización de acceso (por ejemplo, interceptación legal).
Integridad de los datos	Proteger la información de usuario de extremo transportada, procesada o almacenada por un servicio de red, contra la modificación, la supresión, la creación y la reactuación sin autorización.
Disponibilidad	Garantizar que nada puede impedir el acceso al servicio de red a los usuarios de extremo y dispositivos autorizados. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS), y contra ataques pasivos, por ejemplo la modificación o la supresión de la información de autenticación del usuario de extremo (por ejemplo, identificación y contraseñas de usuario).
Privacidad	Garantizar que el servicio de red no proporciona información sobre la utilización que hace el usuario de extremo (por ejemplo, partes llamadas en un servicio VoIP) a personas y dispositivos no autorizados.

Fuente ITU-T X.805, página 16.

Tabla 29. Aplicación de las dimensiones de seguridad a la capa de aplicaciones en el plano de gestión.

Módulo 7: capa aplicaciones, plano de gestión	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que las personas y los dispositivos autorizados son los únicos que pueden realizar las actividades de gestión o administración de la aplicación de red (por ejemplo administrar buzones de usuarios en una aplicación de correo electrónico).
Autenticación	Verificar la identidad de las personas o los dispositivos que intentan realizar actividades de gestión o administración de la aplicación de red. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas o dispositivos que realizan cada actividad de gestión o administrativa de la aplicación de red, y la acción realizada. Este registro puede utilizarse para probar esa persona o dispositivo ha realizado la actividad de gestión o administrativa.
Confidencialidad de los datos	Proteger contra el acceso o la consulta no autorizados todos los ficheros que se utilizan para crear y ejecutar la aplicación de red (por ejemplo, ficheros fuente, de objetos, ejecutables o temporales, etc.) y los ficheros de configuración de la aplicación. Se aplica a los ficheros de la aplicación que residen en dispositivos de red, que se transmiten por la red o almacenados en sistemas no conectados. Proteger la información de gestión o administrativa de la aplicación en la red (por ejemplo, identificación y contraseñas de usuario o de administrador) contra el acceso o la consulta no autorizados.
Seguridad de la comunicación	En el caso de la gestión o administración a distancia de una aplicación de red, garantizar que la información de gestión o administrativa sólo circula entre la estación de gestión distante y los dispositivos que constituyen la aplicación de red. La información de gestión y administrativa no será desviada ni interceptada entre estos puntos extremo. Se incluye en esta protección la información de gestión o administrativa de la aplicación en la red (por ejemplo, identificación y contraseñas de usuario o de administrador).
Integridad de los datos	Proteger todos los ficheros que se utilizan para crear y ejecutar la aplicación de red (por ejemplo, ficheros fuente, de objetos, ejecutables o temporales) y los ficheros de configuración de la aplicación, contra la modificación, la supresión, la creación y la reactuación sin autorización. Hay que proteger los ficheros de la aplicación que residen en dispositivos de red, que se transmiten por la red o que están almacenados en sistemas no conectados. Se incluye en esta protección la información de gestión o administrativa de la aplicación en la red (por ejemplo, identificación y contraseñas de usuario o de administrador).
Disponibilidad	Garantizar que nada impedirá que las personas y los dispositivos autorizados puedan administrar o gestionar la aplicación de red. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS), y contra ataques pasivos, por ejemplo la modificación o la supresión de información administrativa de autenticación para la aplicación en la red (por ejemplo, identificación y contraseñas de administrador).
Privacidad	Garantizar que la información que permite identificar los sistemas para administración o gestión de la aplicación de red no está disponible para personas y dispositivos no autorizados. Son ejemplos de este tipo de información la dirección IP o el nombre de dominio DNS de un sistema. La posibilidad de identificar los sistemas administrativos de una aplicación de red permite, por ejemplo, dirigir un ataque.

Fuente ITU-T X.805, página 17.

Tabla 30.Aplicación de las dimensiones de seguridad a la capa de aplicaciones en el plano de control.

Módulo 8: capa aplicaciones, plano de control	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que la información de control de la aplicación recibida en un dispositivo de red que participa en la aplicación de red proviene de una fuente autorizada, antes de aceptarla (por ejemplo, un mensaje SMTP que solicita la transferencia de correo electrónico). En algunos casos habrá que impedir que un dispositivo no autorizado falsifique un cliente SMTP.
Autenticación	Verificar la identidad de la fuente de información de control de la aplicación enviada a los dispositivos de red que participan en esa aplicación de red. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas o dispositivos que emiten los mensajes de control de la aplicación recibidos por un dispositivo de red que participa en esa aplicación de red, y la acción realizada. Este registro puede utilizarse para probar que esa persona o dispositivo ha emitido el mensaje de control de la aplicación.
Confidencialidad de los datos	Proteger contra el acceso o la consulta no autorizados la información de control de la aplicación que reside en un dispositivo de red (por ejemplo, bases de datos de sesiones SSL), que se transporta por la red o está almacenada en sistemas no conectados. Las técnicas que se utilizan para el control de acceso pueden contribuir a la confidencialidad de la información de control que reside en el dispositivo de red, para una aplicación de red.
Seguridad de la comunicación	Garantizar que la información de control de la aplicación transportada por la red (por ejemplo, mensajes de negociación SSL) sólo circula entre la fuente de esta información de control y el destino especificado. La información de control de la aplicación de red no será desviada ni interceptada entre estos puntos extremo.
Integridad de los datos	Proteger la información de control de una aplicación de red residente en dispositivos de red, que transita por la red o que está almacenada en sistemas no conectados, contra la modificación, la supresión, la creación y la reactuación sin autorización.
Disponibilidad	Garantizar que los dispositivos de red que participan en una aplicación de red siempre están disponibles para recibir información de control de fuentes autorizadas. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS).
Privacidad	Garantizar que la información que permite identificar los dispositivos de red y los enlaces de comunicación que participan en una aplicación de red no está disponible para personas y dispositivos no autorizados. Son ejemplos de este tipo de información la dirección IP o el nombre de dominio DNS de un dispositivo de red. La posibilidad de identificar los dispositivos de red y los enlaces de comunicación permite, por ejemplo, dirigir un ataque.

Fuente ITU-T X.805, página 18.

Tabla 31. Aplicación de las dimensiones de seguridad a la capa de aplicaciones en el plano de usuario de extremo.

Módulo 9: capa aplicaciones, plano usuario de extremo	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que las personas y los dispositivos autorizados son los únicos que pueden acceder a la aplicación de red y utilizarla.
Autenticación	Verificar la identidad del usuario o el dispositivo que intentan acceder a la aplicación de red y utilizarla. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de los usuarios y los dispositivos que han tenido acceso y han utilizado la aplicación de red, y la acción realizada. Este registro puede utilizarse para probar que el usuario de extremo o el dispositivo han accedido a la aplicación de red y la han utilizado.
Confidencialidad de los datos	Proteger contra el acceso o la consulta no autorizados los datos de usuario de extremo transportados, procesados o almacenados por una aplicación de red (por ejemplo, el número de la tarjeta de crédito). Se incluye la protección de los datos de usuario durante el transporte entre el usuario y la aplicación. Las técnicas que se utilizan para el control de acceso pueden contribuir a la confidencialidad de los datos de usuario de extremo.
Seguridad de la comunicación	Garantizar que los datos de usuario de extremo transportados, procesados o almacenados por una aplicación de red no son desviados ni interceptados durante el transporte entre estos puntos extremo sin una autorización de acceso (por ejemplo, interceptación legal). Se incluye la protección de los datos de usuario durante el transporte entre el usuario y la aplicación.
Integridad de los datos	Proteger la información de usuario de extremo transportada, procesada o almacenada por una aplicación de red, contra la modificación, la supresión, la creación y la reactuación sin autorización. Se incluye la protección de los datos de usuario durante el transporte entre el usuario y la aplicación.
Disponibilidad	Garantizar que nada impedirá el acceso a la aplicación de red a los usuarios de extremo y los dispositivos autorizados. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS), y contra ataques pasivos, por ejemplo la modificación o la supresión de la información de autenticación del usuario de extremo (por ejemplo, identificación y contraseñas de usuario).
Privacidad	Garantizar que la aplicación de red no proporciona información sobre la utilización que hace el usuario de extremo (sitios web visitados, etc.) a personas y dispositivos no autorizados. Por ejemplo, este tipo de información sólo será revelado a las autoridades competentes y con una orden de registro.

Fuente ITU-T X.805, página 19.

5.1.3.11. Recomendación Itu-T X.1121. Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremos a extremo:

Aquí se describe las amenazas contra la seguridad en las comunicaciones móviles de datos de extremo a extremo y los requisitos de seguridad con relación al usuario móvil y al proveedor de servicio de aplicación (ASP,

application service provider). En este ítem se describe el modelo de pasarela de comunicación móvil de datos de extremo a extremo entre un usuario móvil y el ASP. Se ilustra en la siguiente figura.

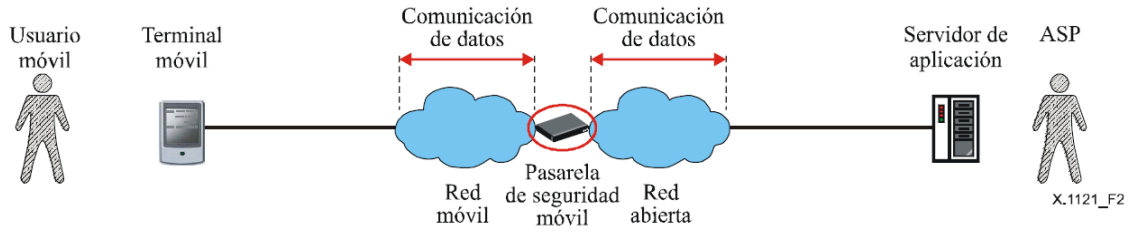

Figura 37. Modelo de pasarela de comunicación móvil de extremo a extremo entre un usuario móvil y el ASP.

Fuente ITU-T X.1121, página 4.

En el capítulo de amenazas contra la seguridad en el entorno móvil, se procede a revisar la relación entre amenazas contra la seguridad y los modelos de comunicación de extremo a extremo. Se ilustra en la siguiente tabla.

Tabla 32. Relación entre amenazas generales contra la seguridad y modelos.

Amenaza / Entidad, relación	Escucha clandestina	Perturbación de la comunicación	Inyección/ modificación	Interrupción	Acceso no autorizado	Repudio
Terminal móvil				X	X	
Servidor de aplicación		X		X	X	
Relación entre usuario móvil y terminal móvil						
Relación entre terminal móvil y servidor de aplicación	X	X	X	X		X
Pasarela de seguridad móvil				X	X	
Relación entre terminal móvil y pasarela de seguridad móvil	X	X	X	X		X
Relación entre servidor de aplicación y pasarela de seguridad móvil	X	X	X	X		X

Fuente ITU-T X.1121, página 7.

De la figura se afirma que en las relaciones generadas, existen amenazas comunes. Y en el caso del ASP y la pasarela de seguridad móvil, se haya las mismas amenazas de seguridad.

Ahora se ejemplifica la relación entre las amenazas de seguridad en sistemas móviles y modelos, con la siguiente tabla.

Tabla 33. Relación entre amenazas de seguridad en sistemas móviles y modelos.

Amenaza / Entidad, relación	Escucha clandestina	Perturbación de la comunicación	Apropiación furtiva de datos	Terminal perdido/ robado	Interrupción no premeditada	Lectura errónea/ error de entrada
Terminal móvil		X		X		
Servidor de aplicación						
Relación entre usuario móvil y terminal móvil			X			X
Relación entre terminal móvil y servidor de aplicación	X	X			X	
Pasarela de seguridad móvil		X				
Relación entre terminal móvil y pasarela de seguridad móvil	X	X			X	
Relación entre servidor de aplicación y pasarela de seguridad móvil	X	X			X	

Fuente ITU-T X.1121, página 8.

En el capítulo de requisitos de seguridad para comunicaciones móviles de datos de extremo a extremo, se procede a revisar los requisitos de seguridad y las amenazas generales contra la seguridad. Se ilustra en la siguiente tabla.

Tabla 34. Relación entre los requisitos de seguridad y las *amenazas generales contra la seguridad.*

Requisito \ Amenaza	Escucha clandestina	Perturbación de la comunicación	Inyección/ modificación	Interrupción	Acceso no autorizado	Repudio
Gestión de la identidad	X				X	X
Confidencialidad de la comunicación de datos	X					
Confidencialidad de los datos almacenados					X	
Integridad de la comunicación de datos			X			
Integridad de los datos almacenados					X	
Autenticación de la identidad			X		X	X
Autenticación del mensaje			X			
Control de acceso			X		X	
No repudio						X
Anonimato					X	
Privacidad	X				X	
Facilidad de utilización						
Disponibilidad		X		X		

Fuente ITU-T X.1121, página 15.

Es la tabla anterior, se afirma que cada requisito de seguridad obliga a tener una medida preventiva de cómo detener las amenazas de la seguridad. Ahora, se determina la relación entre los requisitos y la seguridad en sistemas móviles. Se ilustra en la siguiente tabla.

Tabla 35. Relación entre los requisitos de seguridad y las amenazas contra la seguridad en sistemas móviles.

Requisito \ Amenaza	Escucha clandestina	Perturbación de la comunicación	Apropiación furtiva de datos	Terminal perdido/ robado	Interrupción no deliberada	Lectura errónea/ introducción errónea
Gestión de la identidad	X					
Confidencialidad de la comunicación de datos	X					
Confidencialidad de los datos almacenados				X		
Integridad de la comunicación de datos						
Integridad de los datos almacenados				X		
Autenticación de la identidad				X		
Autenticación del mensaje						
Control de acceso				X		
No repudio						
Anonimato				X		
Privacidad	X		X	X		
Facilidad de utilización						X
Disponibilidad		X			X	

Fuente ITU-T X.1121, página 16.

Sin embargo, para lograr que se cumplan los requisitos de seguridad, se pueden utilizar las siguientes funciones de seguridad:

– Cifrado;
– Intercambio de claves;
– Firma digital;
– Control de acceso;
– Integridad de los datos;
– Intercambio de autenticación;
– Notarización.

Se hace necesario entonces, mostrar la relación entre los requisitos de seguridad y las funciones. Se ilustra en la siguiente tabla.

Tabla 36. Ilustración de la relación entre los requisitos de seguridad y las funciones.

Función / Requisito	Cifrado	Intercambio de claves	Firma digital	Control de acceso	Integridad de los datos	Intercambio de autenticación	Notarización
Gestión de la identidad	X	X	X			X	
Confidencialidad de la comunicación de datos	X	X		X		X	
Confidencialidad de los datos almacenados	X			X			
Integridad de la comunicación de datos	X	X	X	X	X	X	
Integridad de los datos almacenados	X		X	X	X		
Autenticación de entidad	X		X			X	
Autenticación de mensaje	X	X	X		X	X	
Control de acceso				X		X	
No repudio			X			X	X
Anonimato	X						
Facilidad de utilización				X			
Privacidad	X			X		X	
Disponibilidad				X		X	

Fuente ITU-T X.1121, página 19.

Para lograr el efectivo logro de las funciones de seguridad, se utilizan diversas tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo. Es relevante mencionar que la tecnología PKI (infraestructura de clave pública), se puede utilizar para efectuar todas las funciones de seguridad. Se ilustra en la siguiente tabla.

Tabla 37. Relación entre tecnologías de seguridad en comunicaciones móviles y modelo.

Funciones realizadas por tecnologías / Lugares en los cuales se aplican tecnologías	Terminal móvil	Servidor de aplicación /Pasarela de seguridad móvil	Relación entre usuario móvil y terminal móvil	Relación entre terminal móvil y servidor de aplicación u otras relaciones
Cifrado	X	X	X	X
Intercambio de claves				X
Firma digital	X	X		X
Control de acceso	X	X	X	X
Integridad de los datos	X	X		X
Intercambio de autenticación	X	X	X	X
Notarización				X

Fuente ITU-T X.1121, página 20.

5.1.3.12. Recomendación Itu-T X.1122. Directrices para la implementación de sistemas móviles seguros basados en la infraestructura de claves públicas:

Esta recomendación imparte directrices para el desarrollo de sistemas móviles seguros basados en la infraestructura PKI.

Para comprender el lenguaje utilizado, se utilizan las siguientes siglas:

AA Autoridad de atributos (attribute authority)

ASP Proveedor de servicio de aplicación (application service provider)

CA Autoridad de certificación (certification authority)

CMC Gestión del certificado sobre CMS (certifícate manage mentover CMS)

CMP Protocolo de gestión de certificados (certifícate management protocol)

CRL Lista de revocación de certificados (certifícate revocation list)

ID Identificador (identifier)

PIN Número de identificación personal (personal identification number)

PKI Infraestructura de claves públicas (public-key infrastructure)

POP Prueba de posesión (proof of posesión)

RA Autoridad de registro (registration authority)

RSA Algoritmo de clave pública RSA (RSA public key algorithm)

TLS Seguridad de la capa de transporte (transport layer security)

UIM Módulo de identidad de usuario (useri dentity module)

VA Autoridad de validación (validation authority)

La tecnología PKI, se utiliza para realizar las siguientes funciones de red:

– Cifrado;
– Intercambio de claves;
– Firma digital;
– Control de acceso;
– Integridad de los datos;
– Intercambio de autenticación;
– Notarización.

Teniendo en cuenta las funciones de red que utilizan la PKI, sugiere un modelo general de sistemas móviles seguros basados en esta tecnología. Se ilustra con la siguiente figura.

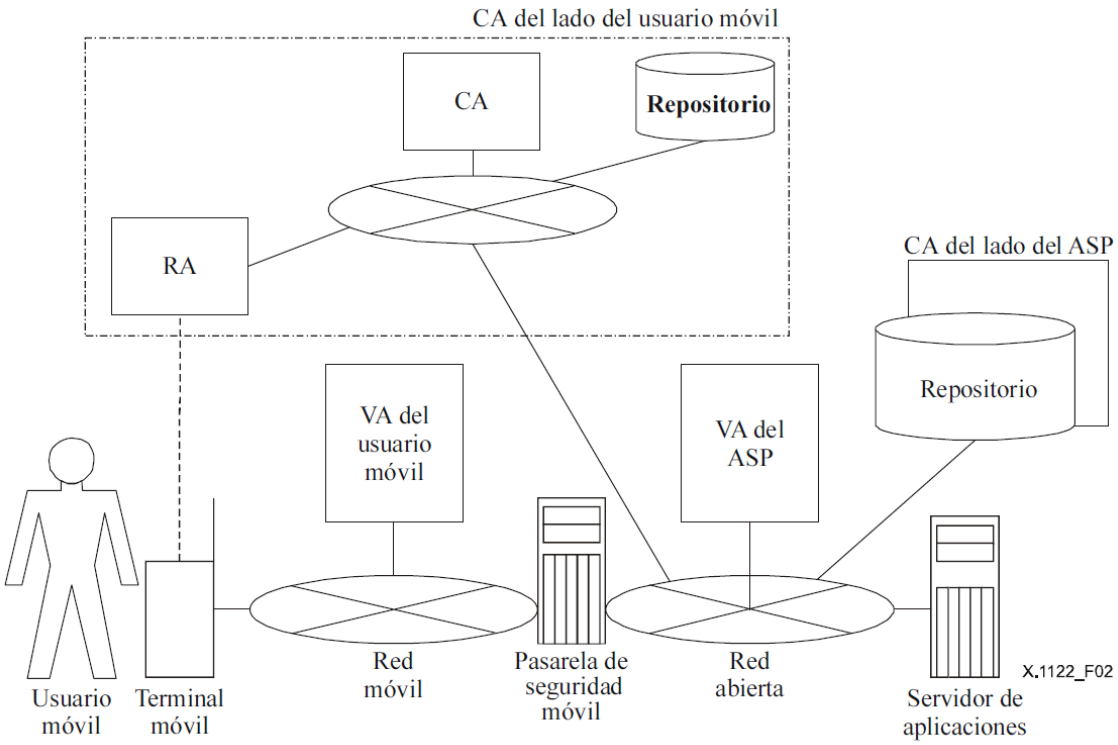

Figura 38. Modelo de pasarela de sistemas móviles seguros basados en PKI.

Fuente ITU-T X.1122, página 6.

6. TENDENCIAS EN SEGURIDAD INFORMÁTICA PARA REDES MÓVILES EN EL CONTEXTO INTERNACIONAL Y NACIONAL.

6.1. ESTADO REDES MÓVILES.

6.1.1. Estado de las Redes Móviles en América Latina.

La seguridad informática cada día adquiere mayor valor social, empresarial, y personal, redundando esto, en la mejoría de las relaciones personales, económicas y en el desarrollo tecnológico enfocado en la solución de problemáticas humanas.

En consecuencia, las redes móviles, hacen parte de ese paradigma donde la seguridad informática tiene aplicación y construye el sinnúmero de procedimientos, protocolos y estándares necesarios para lograr que la información sea confidencial, esté disponible e integra al momento de utilizarla.

La sociedad de la conectividad móvil, es un concepto que se interpreta como la sociedad que hace uso de la tecnología disponible para su beneficio, en todos los ámbitos de su humanidad, pero ello trae consigo, que los datos que utiliza y transmite diariamente aumenten de manera significativa. Para comprender los efectos reales, para el año 2014, la cantidad de usuarios móviles eran 472 millones para Latinoamérica, sin embargo para el año 2019, será de 497 millones, cifra de crecimiento alta. En consecuencia, las conexiones móviles para 2014 eran de 770 millones, para el año 2019 será de 997 millones. Esta información está relacionada con el aumento de velocidad de acceso para los dispositivos móviles, para el año 2014 era de 1.4Mbps, para el año 2019 será de 3.0Mpbs, esto invita a los usuarios a utilizar el servicio de datos móviles en

video por ejemplo, pasando de 2014 a tener un tráfico de 53%, al año 2019 en un 72%.[27]

La comprensión de estos datos, corresponde a un estudio conocido como *Cisco® Visual Networking Índex™,* de la multinacional CISCO, donde hacen las predicciones de tráfico móvil a nivel mundial. En la siguiente figura se ilustra los datos mencionados.

Figura 39. Predicción del Cisco VNI América Latina para 2019.

Fuente. http://gblogs.cisco.com/cansac/wp-content/uploads/sites/33/2015/02/infograf%C3%ADa-VNI-Latam.png

[27]Blog Cisco Cansac. Tráfico de datos móviles crecerá casi 10 veces en los próximos cinco años, predice estudio Cisco Visual Networking Índex (VNI). Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet: < http://gblogs.cisco.com/cansac/trafico-de-datos-moviles-crecera-casi-10-veces-en-los-proximos-cinco-anos-predice-estudio-cisco-visual-networking-index-vni/>

Datos que van correlacionados con la expansión de las redes móviles para la región a finales del 2014, así como las conexiones, utilizando las diferentes estándares como GSM, HSPA y LTE, en donde para América Latina, las conexiones GMS son el 62%(436 millones), HSPA son el 36%(266 millones) y LTE son el 2%(12 millones).[28]

Estas cifras enmarcan un panorama de despliegue de redes móviles, así como la tendencia a la migración hacia los estándares 3G y 4G de las conexiones para la región. Según el estudio "Economía Móvil América Latina 2014", presentado en la 42° Reunión Plenaria de la GSMA América Latina, del pasado 24 de noviembre de 2014, se informa que para septiembre de 2014, las conexiones 4G con apenas un poco más del 1%[29], representan un inicio en las nuevas redes móviles de datos a proteger.

En la siguiente figura, se ilustra la cantidad de millones de conexiones totales por generación de tecnología.

[28]4GAméricas. LTE en América Latina y el Caribe. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet: http://www.4gamericas.org/es/resources/infographics/lte-en-america-latina-y-el-caribe/>

[29]Gsma. Economía Móvil América Latina 2014. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<http://latam.gsmamobileeconomy.com/GSMA_ME_LatinAmerica_2014_ES.pdf>

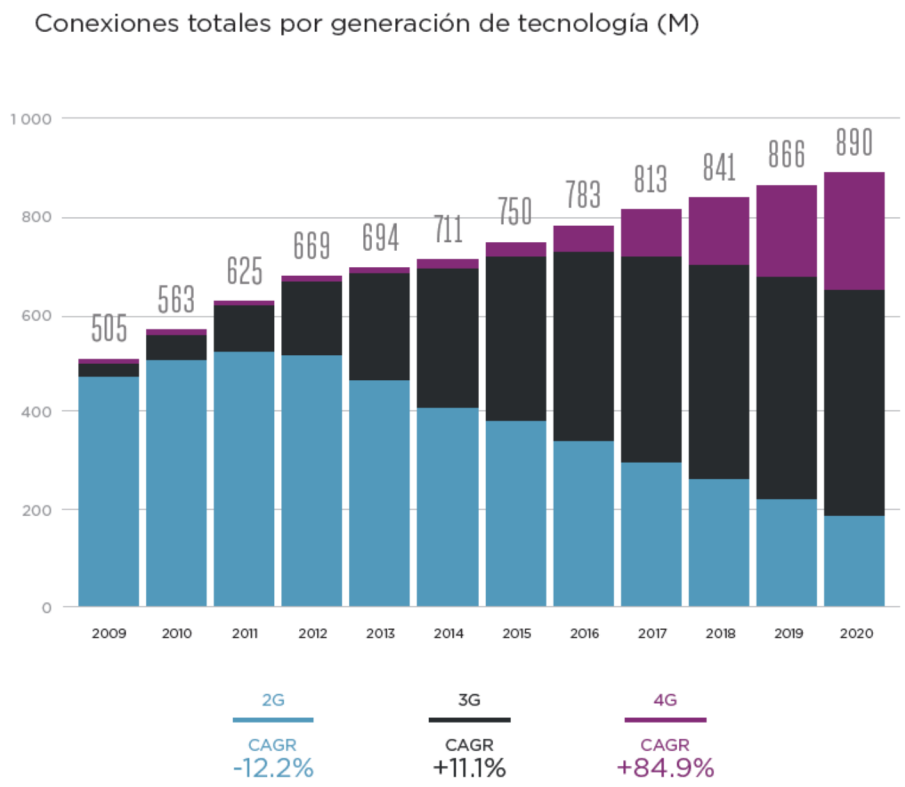

Figura 40. Conexiones totales por generación de tecnología.

Fuente: Economía Móvil América Latina 2014, GSMA, página 13.

Se concluye para este ítem, que para el año 2020, la relación de conexiones a redes 4G, aumentará de manera significativa, lo que atribuye la necesidad de que la seguridad informática aplicada a dichas redes, será vital en el desarrollo de la industria móvil así como el desarrollo económico de la región.

6.1.2. Nuevas Normas y Estándares de Seguridad Informática para Redes Móviles en el Contexto Internacional.

Se ha realizado la revisión del estado actual de las redes móviles tanto para América Latina como para Colombia, teniendo en cuenta variables como la cantidad de conexiones a las redes, estándares de las mismas, tráfico de datos utilizado en el año desde el año 2014, y con proyección al año 2019.

Ahora se hace necesario conocer cuáles serán esas nuevas normas y estándares que serán aplicados en las nuevas redes móviles, teniendo en cuento sus aspectos técnicos, como las fechas en tiempo en que las mismas serán publicadas y utilizadas por la industria móvil, y que sea beneficiada la comunidad en general.

6.1.2.1. Informe Técnico Itu- T TutSec 2014. Xstr-Pkis. Desafíos actuales y futuros para estandarización de la infraestructura de clave pública:

Este Informe Técnico explora los problemas y amenazas que enfrenta actualmente el despliegue de infraestructura de clave pública (PKI), y los nuevos retos PKI va a experimentar en áreas como la PKI inalámbrico (WIKI), la computación en nube, redes inteligentes, y de máquina a máquina (M2M) en general, el cual fue expedido el 26 de septiembre de 2014.[30]

Para la revisión de las tendencias en seguridad informáticas aquí mencionadas, se le dará relevancia a los siguientes ítems:

- Problemas de implementación de PKI.
- Introducción del concepto de un agente de confianza como un nuevo tipo de identidad en PKI.
- WTLS y su especificación alternativa para uso en redes móviles.
- IPsec.

- Introducción del concepto de un agente de confianza como un nuevo tipo de identidad en pki.

[30]International Telecommunication Union Itu. XSTR-PKIS. Desafíos actuales y futuros para estandarización de la infraestructura de clave pública. Reporte Técnico. Inglés. Comisión de Estudio 17 del UIT-T. Ginebra, Suiza. 2014. 42 p.

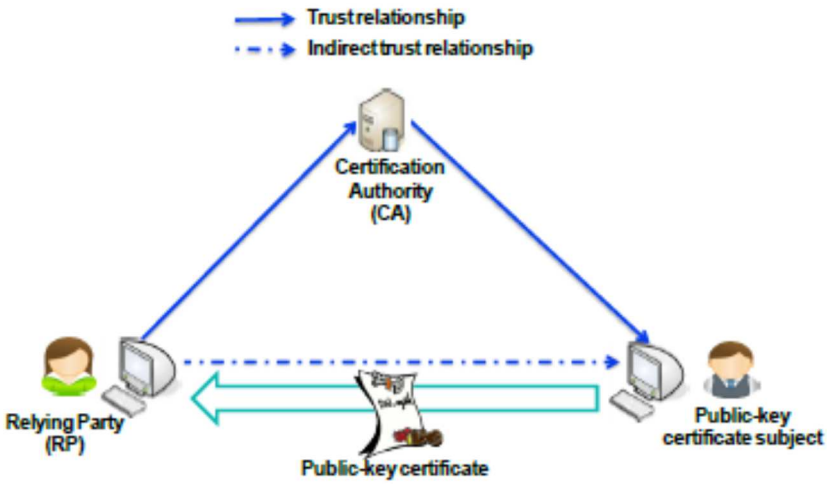

Figura 41. Modelo de confianza de 3 lados o esquinas.

Fuente. ITU- T TUT SEC 2014, página 20.

Inicia la revisión de esta tendencia, con el modelo de confianza tradicional, sin embargo el concepto de un agente de confianza aparece, como la manera de que la parte que confía en la clave, posee una relación de confianza, llamada corredor de confianza, que su función es la de comprobar en las partes del sistema, la correspondiente validación, logrando un control exhaustivo. Se ilustra en la siguiente figura.

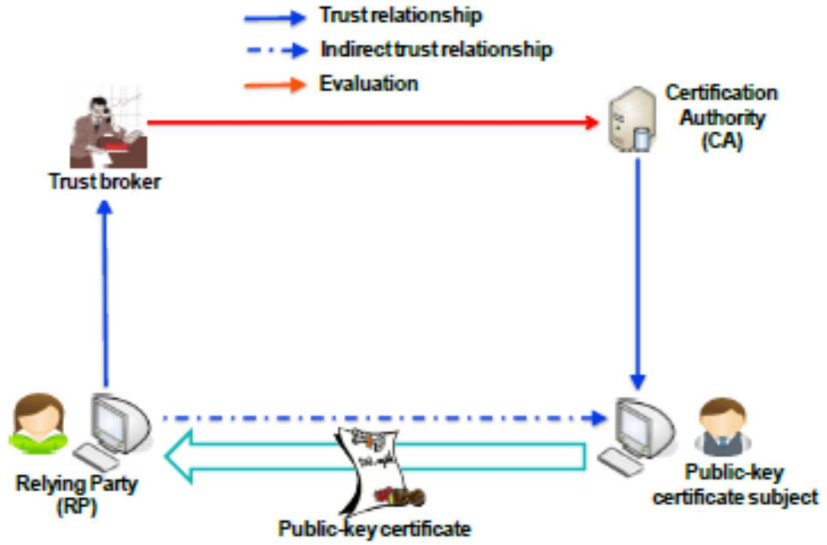

Figura 42. Modelo de confianza de 4 lados o esquinas.

Fuente. ITU- T TUT SEC 2014, página 20.

- Wtls Y Su Especificación Alternativa Para Uso En Redes Móviles: Wtlsse ha definido para un entorno móvil con limitación de almacenamiento limitada, procesamiento capacidad y ancho de banda. Como la misma limitación puede estar presente en otros entornos, la WTLS conceptos pueden ser aplicables para otros entornos de restricción, toda vez que sus estructura de datos están comprimidas, toda vez que son más pequeñas; su diseño está basado en paquetes, para ser usada en las redes basadas en paquetes, ofreciendo seguridad en la capa de transporte.

- Ipsec: Tls proporciona autenticación, integridad y confidencialidad en la capa de transporte entre dos aplicaciones, mientras que IPsec protege todas las comunicaciones entre dos sistemas de extremo en la capa de red IP.

6.1.2.2. Imt-Avanzadas

Basada en el protocolo IP, allí nacen las redes 4G, como estándar de comunicación y que tiene los siguientes requisitos:

Basado en el protocolo IP.

Interoperabilidad con los estándares inalámbricos existentes.

Velocidades de transmisión de 100 Mbps, mientras que el cliente se mueve físicamente a altas velocidades relativas a la estación, y 1 Gbps, mientras que el cliente y la estación se encuentran en posiciones relativamente fijas.

Uso dinámico y utilización de los recursos de la red para ofrecer cobertura a más usuarios simultáneos por célula.

Ancho de banda de canal escalable 5-20 MHz, opcionalmente hasta 40 MHz.

Capacidad para ofrecer alta calidad en servicio de acceso a video.

- Long term evolution – advanced, LTE-A:

Para el caso de estudio, ya se ha revisado el estándar LTE en capítulos anteriores, ahora es necesario, abordar el estándar LTE-A, en cuanto a la seguridad que ofrece para ofrecer a los futuros usuarios del servicio. Sin embargo, antesde abordar su arquitectura de seguridad, es importante mencionar que según datos de 7 de abril de 2015, en el mundo se han desplegado 56 redes LTE-A comerciales, así lo indica 4G Américas, organización comercial de la industria compuesta por proveedores y fabricantes en el gremio de las Telecomunicaciones[31], sin embargo para América Latina, no existe aún ninguna red con esta tecnología. Solo América del Norte, representado con Canadá (operadores Rogers y Bell Mobility) y Estados Unidos (operadores AT&T y Sprint)[32].

- Marco general de seguridad:

La gestión de seguridad aborda la manera en que la red LTE autentica y autoriza el uso de sus servicios a los usuarios, así como los mecanismos utilizados para entregar confidencialidad e integridad a la información enviada tanto en la interfaz radio como en otras interfaces entre equipos de red.

- Seguridad de acceso a la red:

La seguridad de acceso a la red LTE a través de una red de acceso E-UTRAN se compone de los siguientes elementos:

[31]4G Américas. Quiénes somos. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet: <http://www.4gamericas.org/es/about-us/>

[32]4G Américas. Estado LTE-Advanced a 25 de marzo de 2015. Inglés. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<http://www.4gamericas.org/files/2314/2723/0862/LTE-Advanced_3.25.15.pdf/>

Mecanismos para la autenticación mutua entre el usuario y la red. El procedimiento a través del cual se realiza la autenticación mutua, junto con la gestión de autenticación de claves, se llama EPS Authentication and Key Agreement (AKA).

Mecanismos para la determinación de las claves secretas utilizadas en los algoritmos de cifrado para la provisión de los diferentes servicios de confidencialidad e integridad, ofreciendo la ruta de validación necesaria para la utilización de los servicios de red.

Servicios de confidencialidad e integridad para la transferencia de la señalización NAS entre el equipo de usuario y la entidad MME de la red troncal EPC.

Servicios de confidencialidad e integridad para la transferencia de la señalización del protocolo RRC entre el equipo de usuario y el eNB.

Servicios de confidencialidad para la transferencia de información en el plano de usuario entre el equipo de usuario y el eNB.

- Seguridad en la infraestructura de red:

La aplicación de IPsec en la solución NDS/IP es diferente en función de cómo se encuentre estructurada la red en términos de dominios de seguridad. Un dominio de seguridad corresponde al conjunto de equipos de una red que están gestionados por la misma autoridad administrativa, que configura y determina las reglas de transmisión de datos sobre el mismo. Un ejemplo de un dominio

de seguridad podría ser la red de un mismo operador de red (una red LTE), no quedando excluida la posibilidad de un operador decida estructurar su red en varios dominios de seguridad diferentes.

6.1.2.3. Norma Etsi TS 133 303 v12.2.0

Correspondiente esta norma a la 3GPP TS 33.303 versión 12.2.0 Release 12, que origina la pauta para las redes LTE-A, la cual fue promulgada en enero de 2015[33]. La misma ofrece los aspectos de seguridad informática a tener en cuenta para los servicios basados en proximidad, pequeñas celdas, donde será posible mejor rendimiento por la expansión del rango de cobertura de la señal, en atención a la proximidad entre ellas.

La empresa *Qualcomm[34] ha* Utilizan técnicas MIMO para mejorar la capacidad de receptores en las redes LTE-A, cancelando la interferencia, reflejado en el rendimiento de las redes, lo anterior de ilustra en la siguiente figura.

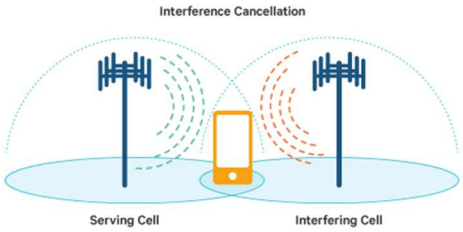

Figura 43. Receptores mejorados para rendimiento LTE-A, cancelación interferencia.

Fuente: https://www.qualcomm.com/invention/technologies/lte/advanced

[33] ETSI. Universal Mobile Telecommunications System (UMTS); LTE; Proximity-based Services (ProSe); Security aspects (3GPP TS 33.303 version 12.2.0 Release 12). Especificación Técnica. Inglés. Referencia RTS/TSGS-0333303vc20. Francia. 2015. 66 p.
[34]QUALCOMM. Sitio web. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<https://www.qualcomm.com/>

La apuesta de conectividad va mucho más allá, las redes LTE-A, permitirán ofrecer LTE Directo, LTE sin licencia, LTE broadcast para televisión terrestre, basados en la cantidad de celdas pequeñas, que ofrezcan mayor cobertura y favorezcan la proximidad de los dispositivos. Lo anterior se muestra en la siguiente figura.

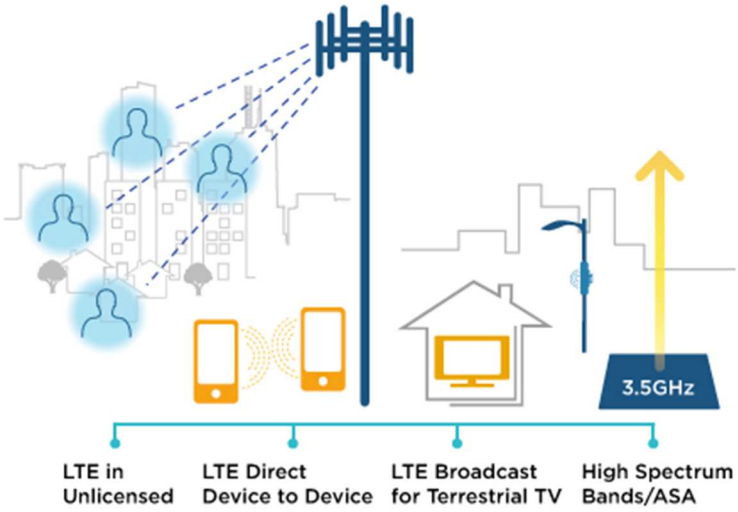

Figura 44. Nuevas propuestas de LTE-A.

Fuente: https://www.qualcomm.com/invention/technologies/lte/advanced

6.1.2.4. Estado de las Redes Móviles en América Latina en Comparativa con Colombia.

La situación del país en materia de redes móviles, se analiza desde varios aspectos, uno de ellos es el despliegue de las redes 4G, las conexiones a internet fijas y móviles, el aumento en el uso de teléfonos inteligentes (Smartphone).

En el caso del despliegue de las rede 4G, se ha detallado en el estudio "Economía Móvil América Latina 2014", presentado en la 42° Reunión Plenaria de la GSMA América Latina, del pasado 24 de noviembre de 2014, se informa que para agosto 29 de 2014, que en 18 países de la región, se había desplegado 44 redes LTE[35]. Se ilustra en la siguiente figura.

LTE en América Latina* y el Caribe

44 redes / 18 países	a 29 de agosto de 2014	
México	Movistar	1700/2100 AWS
	Nextel	1700/2100 AWS
	Telcel	1700/2100 AWS
Colombia	Avantel	2100 AWS
	Claro	2500/2690 MHz
	Movistar	1700/2100 AWS
	Tigo – UNE	1700/2100 AWS 2500/2690 MHz
Bolivia	Entel, Tigo	700 MHz
Brasil	Claro	2500/2690 MHz
	Nextel	1800 MHz
	Oi	2500/2690 MHz
	ON*	2500/2690 MHz
	Sky Telecom*	2500/2690 MHz
	TIM	2500/2690 MHz
	VIVO	2500/2690 MHz
Chile	Claro	2500/2690 MHz
	Entel	2500/2690 MHz
	Movistar	2500/2690 MHz
Ecuador	CNT Mobile	1700/2100 AWS
Paraguay	Personal	1900 MHz
	VOX	1700/2100 AWS
Peru	Movistar	1700/2100 AWS
	Claro	
Uruguay	Antel	1700/2100 AWS
	Claro	1700/2100 AWS
Venezuela	Digitel	1800 MHz
Antigua y Barbuda	Digicel*	700 MHz
Aruba	SETAR	1800 MHz
Bahamas	BTC	700 MHz
Islas Caimán	C&W Lime	700 MHz
	Digicel*	700 MHz
Costa Rica	ICE/Kolbi	2600 MHz
	Claro	1800 MHz
	Movistar	1800 MHz
República Dominicana	Claro	1700/2100 AWS
	Orange Dominicana	1800 MHz
	Tricom	1900 MHz
Puerto Rico	AT&T	1700/2100 AWS
	Claro	700 MHz
	Open Mobile	700 MHz
	Sprint	850/1900 MHz
	T-Mobile	1700/2100 AWS
Islas Vírgenes	AT&T	1700/2100 AWS
	Sprint	1900 MHz

Figura 45. LTE en América Latina y el Caribe.

Fuente: Economía Móvil América Latina 2014, GSMA, página 15.

De la figura anterior se determina que Colombia, cuenta con cuatro operadores de redes móviles con igual número de redes LTE.

[35]GSMA. Economía Móvil América Latina 2014. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<http://latam.gsmamobileeconomy.com/GSMA_ME_LatinAmerica_2014_ES.pdf>

Para el caso de las conexiones a internet fijo y móvil para el año 2013, se ha volcado a este último, en atención a factores de falta de infraestructura de banda ancha fija en varios países, sobre todo en zonas rurales. Se ilustra en la siguiente figura.

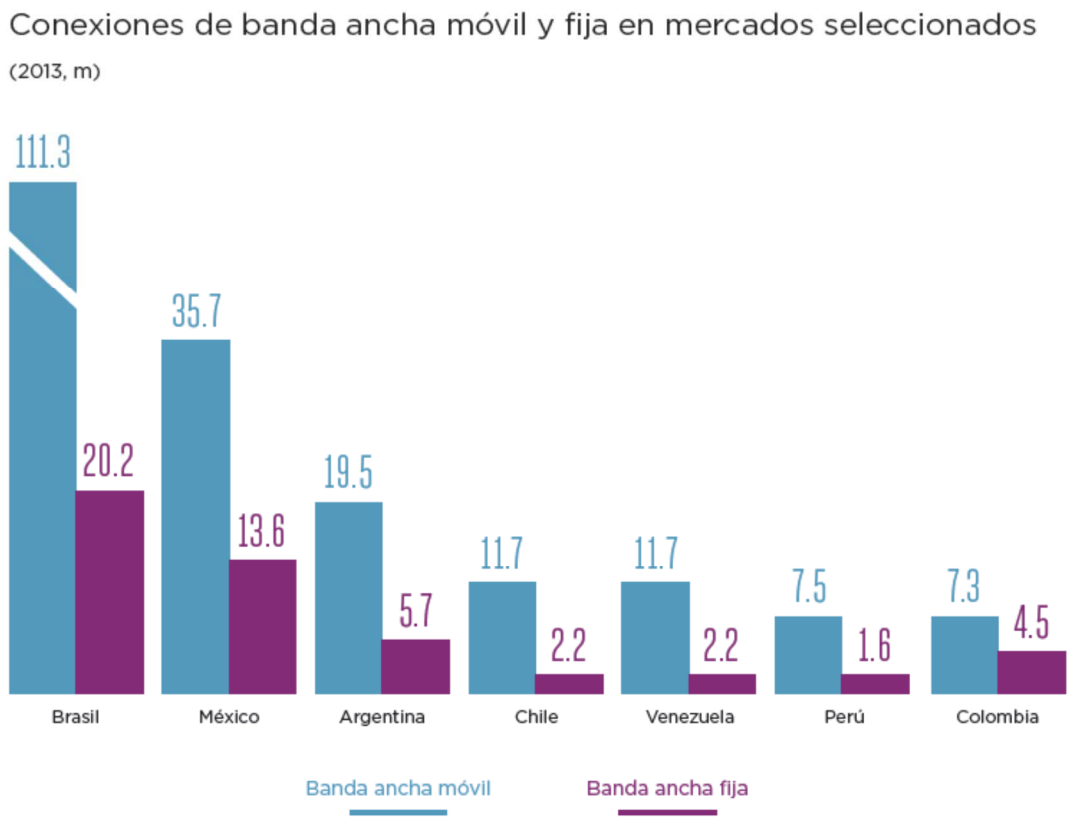

Figura 46. Conexiones de banda ancha móvil y fija en mercados seleccionados.

Fuente: Economía Móvil América Latina 2014, GSMA, página 16.

En relación a Colombia, son 7.3 millones de conexiones móviles, frente a 4.5 fijas, lo que augura un campo de crecimiento fuerte, en atención al despliegue de las redes antes mencionadas.

Y por último, el aumento en el uso de los teléfonos inteligentes (Smartphone), será clave en la utilización de las redes móviles desde el tercer trimestre el año 2014 al año 2020. En Colombia, para el año 2014, representaba el 26.9% de tasa de adopción del dispositivo mencionado, como tendencia para el cuatro trimestre de 2020, representará el 69% de la tasa de adopción. Se ilustra a continuación la comparativa con otros países de la región y con América Latina.

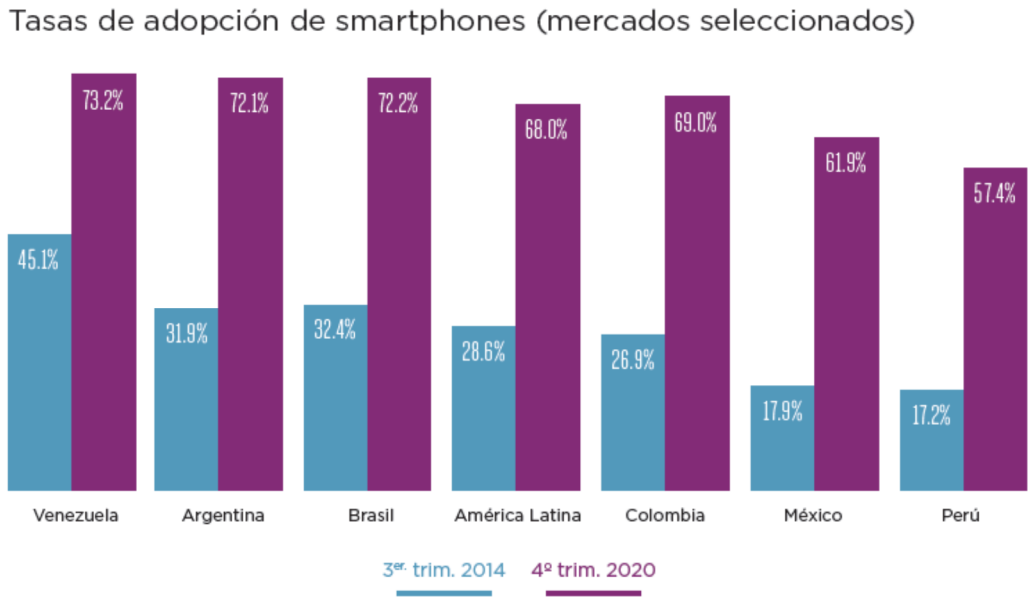

Figura 47. Tasas de adopción de smartphone.

Fuente: Economía Móvil América Latina 2014, GSMA, página 18.

7. ANALISIS DE RESULTADOS

- **Información suministrada por la Entidades de Control del Estado**.

Se ha dispuesto de unas tablas de análisis consolidadas para resumir las respuestas de las entidades del orden administrativo y judicial del país. Las cuales se muestran a continuación.

Tabla 38. Consolidado respuestas y aportes Fiscalía General de la Nación.

INVESTIGACION EXPLORATORIA			
NUEVAS TENDENCIAS EN SEGURIDAD INFORMATICA EN REDES MOVILES EN COLOMBIA			
ANÁLISIS DE INFORMACIÓN			
Institución y/o experto	Fiscalia General de la Nación		
Tipo de Institución y/o experto	Organo de investigación judicial en Colombia		
Fecha solicitud	24 de marzo de 2014		
Fecha respuesta	10 de abril de 2014		
Amparo legal	Constitución Política de Colombia, Art. 23. Derecho de petición.		
Medio de solicitud de información	Correo electrónico		
Medio de respuesta de información	Correo electrónico y oficio físico		
Tipo de archivo solicitado	Documento en formato .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg		
Tipo de archivo enviado y/o anexado	Documento en formato .xls		
Corresponde a anexo número	3		
Item	**Información solicitada**	**Respuesta aportada**	**Aporte a la investigación**
1	Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014	No consultada, en atención a la naturaleza judicial de la entidad	Determina el alcance de la entidad frente a las tendencias en el país.
2	Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.	No consultada, en atención a la naturaleza judicial de la entidad	Determina el alcance de la entidad frente a las tendencias en el país.
3	Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.	No es de competencia de la Entidad. Sin embargo en apoyo con la Dirección Nacional de Fiscalias, realizó consulta en su sistema de información, y entrego el archivo en excel "Delitos informáticos 2010-2014.	Permite identificar si se presentaron delitos informáticos, donde hubiera involucradas redes móviles.
4	Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.	No cuenta con estudios acerca de tendencias y recomendaciones en seguridad informática	Ofrece la oportunidad de consultar información sobre las tendencias a aplicar en el país.

Tabla 39. Consolidado respuestas y aportes MINTIC.

INVESTIGACION EXPLORATORIA			
NUEVAS TENDENCIAS EN SEGURIDAD INFORMATICA EN REDES MOVILES EN COLOMBIA			
ANÁLISIS DE INFORMACIÓN			
Institución y/o experto	Ministerio de Tecnologías de la Información y Comunicaciones MINTIC		
Tipo de Institución y/o experto	Entidad encargada de la regulación y orientación sobre las Tics en Colombia		
Fecha solicitud	24 de marzo de 2014		
Fecha respuesta	4 de junio de 2014		
Amparo legal	Constitución Política de Colombia, Art. 23. Derecho de petición.		
Medio de solicitud de información	Correo electrónico		
Medio de respuesta de información	Correo electrónico y oficio físico		
Tipo de archivo solicitado	Documento en formato .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg		
Tipo de archivo enviado y/o anexado	Correo electrónico y oficio físico en papel		
Corresponde a anexo número	4		
Item	**Información solicitada**	**Respuesta aportada**	**Aporte a la investigación**
1	Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014	Según el marco normativo de la Comisión de Regulación de Comunicaciones, Resoluciones 3067 de 2011, 3496 de 2011, 3503 de 2011, 4000 de 2012 y 4007 de 2012, los operadores de telefonia móvil no estan obligados a reportar dicha información en los reportes periodicos	La falta de información pública para el conocimiento general del estado de la seguridad de los datos en las redes móviles.
2	Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		La falta de información pública para el conocimiento general del estado de la seguridad de los datos en las redes móviles.
3	Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.	Según la Ley 1341, Ley 679, decreto 1524 de 2000, Ley 1356 de 2009, solo se verifica que tenga un modelo de operación y respuesta al usuario para la calidad del servicio, pero no de seguridad informática	Ofrece la oportunidad de explorar reportes internacionales sobre las normas y estandares en seguridad informática aplicados en Colombia y la legislación sobre el tema
4	Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.	Según el marco normativo de la Comisión de Regulación de Comunicaciones, Resoluciones 3067 de 2011, 3496 de 2011, 3503 de 2011, 4000 de 2012 y 4007 de 2012, los operadores de telefonia móvil no estan obligados a reportar dicha información en los reportes periodicos	Ofrece la oportunidad de explorar reportes internacionales sobre las tendencias en seguridad informática aplicados en Colombia.

Tabla 40. Consolidado respuestas y aportes SIC.

INVESTIGACION EXPLORATORIA			
NUEVAS TENDENCIAS EN SEGURIDAD INFORMATICA EN REDES MOVILES EN COLOMBIA			
ANÁLISIS DE INFORMACIÓN			
Institución y/o experto	Superintendencia de Industria y Comercio		
Tipo de Institución y/o experto	Entidad pública encargada del comportamiento de la industria y comercio en el país.		
Fecha solicitud	24 de marzo de 2014		
Fecha respuesta	31 de marzo de 2014		
Amparo legal	Constitución Política de Colombia, Art. 23. Derecho de petición.		
Medio de solicitud de información	Correo electrónico		
Medio de respuesta de información	Correo electrónico y oficio físico		
Tipo de archivo solicitado	Documento en formato .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg		
Tipo de archivo enviado y/o anexado	Documento en formato .xls		
Corresponde a anexo número	10		
Item	**Información solicitada**	**Respuesta aportada**	**Aporte a la investigación**
1	Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014	Informa que la función de la SIC es la protección de los derechos de los consumidores y control de competencia y sugiere acudir al MinTic	Permite identificar que la SIC no tiene en sus competencias, el poder sancionatorio a los operadores, en caso de que no cumplan con los parametros de seguridad informática en sus redes móviles. De igual manera, ilustran acerca de quien puede tener dicha información.
2	Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
3	Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
4	Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		

Tabla 41. Consolidado respuestas y aportes CRC.

INVESTIGACION EXPLORATORIA			
NUEVAS TENDENCIAS EN SEGURIDAD INFORMATICA EN REDES MOVILES EN COLOMBIA			
ANÁLISIS DE INFORMACIÓN			
Institución y/o experto	Comisión de Regulación de Comunicaciones		
Tipo de Institución y/o experto	Entidad pública encargada del estudio y proyección de las políticas de regulación de comunicaciones.		
Fecha solicitud	24 de marzo de 2014		
Fecha respuesta	25 de marzo de 2014, parcialmente		
Amparo legal	Constitución Política de Colombia, Art. 23. Derecho de petición.		
Medio de solicitud de información	Correo electrónico		
Medio de respuesta de información	Correo electrónico y oficio físico		
Tipo de archivo solicitado	Documento en formato .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg		
Tipo de archivo enviado y/o anexado	Documento en formato .xls		
Corresponde a anexo número	11		
Item	**Información solicitada**	**Respuesta aportada**	**Aporte a la investigación**
1	Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014	Informa acerca de que la entidad, sobre puede orintar sobre la aplicación de la normatividad para la protección del usuario, pero no tiene más información. Sin embargo informa sobre los tiempos de respuesta. A la fecha no se ha recibido respuesta.	Permite identificar que la CRC viene en proceso de mejora para que se pueda regular a los operadores móviles sobre la seguridad informática, aplicando el factor de protección al consumidor.
2	Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
3	Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
4	Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		

- **Información suministrada por las Entidades, Organizaciones expertas y operadores de servicios móviles.**

Se ha dispuesto de unas tablas de análisis consolidadas para resumir las respuestas de los operadores móviles y consultores y/o integradores de seguridad del país. Las cuales se muestran a continuación.

Tabla 42. Consolidado respuestas y aportes AVANTEL.

INVESTIGACION EXPLORATORIA			
NUEVAS TENDENCIAS EN SEGURIDAD INFORMATICA EN REDES MOVILES EN COLOMBIA			
ANÁLISIS DE INFORMACIÓN			
Institución y/o experto	AVANTEL		
Tipo de Institución y/o experto	Empresa privada, Operador móvil		
Fecha solicitud	24 de marzo de 2014		
Fecha respuesta	28 de marzo de 2014		
Amparo legal	Constitución Política de Colombia, Art. 23. Derecho de petición.		
Medio de solicitud de información	Correo electrónico		
Medio de respuesta de información	Correo electrónico y oficio físico		
Tipo de archivo solicitado	Documento en formato .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg		
Tipo de archivo enviado y/o anexado	Documento en formato .xls		
Corresponde a anexo número	12		
Item	**Información solicitada**	**Respuesta aportada**	**Aporte a la investigación**
1	Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014	Informa que dicha información es confidencial de la empresa. Menciona que son el MinTic o la CRC, los que pueden dar información sobre el tema.	Permite identificar que AVANTEL no esta obligado legalmente a entregar dicha información. Sin embargo se presenta como una oportunidad de consultar reportes internacionales acerca de los estandares a introducir en Colombia.
2	Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
3	Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
4	Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		

Tabla 43. Consolidado respuestas y aportes UNE.

INVESTIGACION EXPLORATORIA			
NUEVAS TENDENCIAS EN SEGURIDAD INFORMATICA EN REDES MOVILES EN COLOMBIA			
ANÁLISIS DE INFORMACIÓN			
Institución y/o experto	UNE		
Tipo de Institución y/o experto	Operador Móvil		
Fecha solicitud	24 de marzo de 2014		
Fecha respuesta	26 de marzo de 2014		
Amparo legal	Constitución Política de Colombia, Art. 23. Derecho de petición.		
Medio de solicitud de información	Correo electrónico		
Medio de respuesta de información	Correo electrónico y oficio físico		
Tipo de archivo solicitado	Documento en formato .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg		
Tipo de archivo enviado y/o anexado	Correo electrónico y oficio físico en papel		
Corresponde a anexo número	13		
Item	**Información solicitada**	**Respuesta aportada**	**Aporte a la investigación**
1	Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014	Informa acerca del recibido de la solicitud y los tiempos que tiene como empresa para dar respuesta. A la fecha no ha dado respuesta a la misma.	Permite identificar que UNE no esta obligado legalmente a entregar dicha información. Sin embargo se presenta como una oportunidad de consultar reportes internacionales acerca de los estandares a introducir en Colombia.
2	Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
3	Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
4	Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		

Tabla 44. Consolidado respuestas y aportes VIRGIN MOBILE.

INVESTIGACION EXPLORATORIA			
NUEVAS TENDENCIAS EN SEGURIDAD INFORMATICA EN REDES MOVILES EN COLOMBIA			
ANÁLISIS DE INFORMACIÓN			
Institución y/o experto	VIRGIN MOBILE		
Tipo de Institución y/o experto	Operador Móvil Virtual		
Fecha solicitud	26 de marzo de 2014		
Fecha respuesta	8 de abril de 2014		
Amparo legal	Constitución Política de Colombia, Art. 23. Derecho de petición.		
Medio de solicitud de información	Correo electrónico		
Medio de respuesta de información	Correo electrónico		
Tipo de archivo solicitado	Documento en formato .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg		
Tipo de archivo enviado y/o anexado	Correo electrónico		
Corresponde a anexo número	14		
Item	**Información solicitada**	**Respuesta aportada**	**Aporte a la investigación**
1	Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014	Informa que es un secreto comercial, que esta protegido por la ley colombia y andina y no están obligados legalmente para entregar dicha información.	Permite identificar que VIRGIN MOBILE no esta obligado legalmente a entregar dicha información. Sin embargo se presenta como una oportunidad de consultar reportes internacionales acerca de los estandares a introducir en Colombia.
2	Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
3	Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
4	Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		

Tabla 45. Consolidado respuestas y aportes CLARO.

INVESTIGACION EXPLORATORIA			
NUEVAS TENDENCIAS EN SEGURIDAD INFORMATICA EN REDES MOVILES EN COLOMBIA			
ANÁLISIS DE INFORMACIÓN			
Institución y/o experto	CLARO		
Tipo de Institución y/o experto	Operador Móvil		
Fecha solicitud	24 de marzo de 2014		
Fecha respuesta	25 de marzo de 2014, parcialmente		
Amparo legal	Constitución Política de Colombia, Art. 23. Derecho de petición.		
Medio de solicitud de información	Correo electrónico		
Medio de respuesta de información	Correo electrónico		
Tipo de archivo solicitado	Documento en formato .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg		
Tipo de archivo enviado y/o anexado	Correo electrónico		
Corresponde a anexo número	15		
Item	**Información solicitada**	**Respuesta aportada**	**Aporte a la investigación**
1	Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014	Informa que la solicitud esta siendo atendida por el área correspondiente. A la fecha no se ha recibido respuesta.	Permite identificar que CLARO no esta obligado legalmente a entregar dicha información. Sin embargo se presenta como una oportunidad de consultar reportes internacionales acerca de los estandares de desarrollo de estándares nuevos.
2	Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
3	Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
4	Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		

Tabla 46. Consolidado respuestas y aportes TIGO.

INVESTIGACION EXPLORATORIA			
NUEVAS TENDENCIAS EN SEGURIDAD INFORMATICA EN REDES MOVILES EN COLOMBIA			
ANÁLISIS DE INFORMACIÓN			
Institución y/o experto	TIGO		
Tipo de Institución y/o experto	Operador Móvil		
Fecha solicitud	24 de marzo de 2014		
Fecha respuesta	Sin respuesta		
Amparo legal	Constitución Política de Colombia, Art. 23. Derecho de petición.		
Medio de solicitud de información	Correo electrónico		
Medio de respuesta de información	Correo electrónico		
Tipo de archivo solicitado	Documento en formato .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg		
Tipo de archivo enviado y/o anexado	Correo electrónico		
Corresponde a anexo número	No aplica		
Item	**Información solicitada**	**Respuesta aportada**	**Aporte a la investigación**
1	Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014	Sin respuesta	Algunos factores de atención al usuario por sus canales de comunicación, no son atendidos en los tiempos señalados por la legislación colombiana.
2	Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
3	Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
4	Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		

Tabla 47. Consolidado respuestas y aportes MOVISTAR.

INVESTIGACION EXPLORATORIA			
NUEVAS TENDENCIAS EN SEGURIDAD INFORMATICA EN REDES MOVILES EN COLOMBIA			
ANÁLISIS DE INFORMACIÓN			
Institución y/o experto	MOVISTAR		
Tipo de Institución y/o experto	Operador Móvil		
Fecha solicitud	24 de marzo de 2014		
Fecha respuesta	Sin respuesta		
Amparo legal	Constitución Política de Colombia, Art. 23. Derecho de petición.		
Medio de solicitud de información	Correo electrónico		
Medio de respuesta de información	Correo electrónico		
Tipo de archivo solicitado	Documento en formato .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg		
Tipo de archivo enviado y/o anexado	Correo electrónico		
Corresponde a anexo número	No aplica		
Item	**Información solicitada**	**Respuesta aportada**	**Aporte a la investigación**
1	Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014	Sin respuesta	Algunos factores de atención al usuario por sus canales de comunicación, no son atendidos en los tiempos señalados por la legislación colombiana.
2	Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
3	Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
4	Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		

Tabla 48. Consolidado respuestas y aportes GIDAM

INVESTIGACION EXPLORATORIA			
NUEVAS TENDENCIAS EN SEGURIDAD INFORMATICA EN REDES MOVILES EN COLOMBIA			
ANÁLISIS DE INFORMACIÓN			
Institución y/o experto	Universidad del Magdalena		
Tipo de Institución y/o experto	GRUPO DE INVESTIGACION EN DESARROLLO Y APLICACIONES MOVILES		
Fecha solicitud	24 de marzo de 2014		
Fecha respuesta	22 de octubre de 2014		
Amparo legal	Constitución Política de Colombia, Art. 23. Derecho de petición.		
Medio de solicitud de información	Correo electrónico		
Medio de respuesta de información	Correo electrónico y oficio físico		
Tipo de archivo solicitado	Documento en formato .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg		
Tipo de archivo enviado y/o anexado	Correo electrónico y oficio físico en papel		
Corresponde a anexo número	17		
Item	**Información solicitada**	**Respuesta aportada**	**Aporte a la investigación**
1	Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014	Informa que la seguridad informática no hace parte de sus lineas de investigación. Sin embargo, menciona parte de la normativa en Colombia, aplicables al tema de hurto informático.	Permite demostrar el poco estudio sobre estos temás en grupos de investigación de Universidades del país, lo que ofrece a esta investigación un factor de proponderancia para que sea referente en este campo.
2	Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
3	Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
4	Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		

Tabla 49. Consolidado respuestas y aportes GECTI.

INVESTIGACION EXPLORATORIA			
NUEVAS TENDENCIAS EN SEGURIDAD INFORMATICA EN REDES MOVILES EN COLOMBIA			
ANÁLISIS DE INFORMACIÓN			
Institución y/o experto	Universidad de Los Andes		
Tipo de Institución y/o experto	GRUPO DE INVESTIGACIÓN EN COMERCIO ELECTRÓNICO, TELECOMUNICACIONES E INFORMÁTICA- GECTI.		
Fecha solicitud	26 de marzo de 2014		
Fecha respuesta	22 de septiembre de 2014		
Amparo legal	Constitución Política de Colombia, Art. 23. Derecho de petición.		
Medio de solicitud de información	Correo electrónico		
Medio de respuesta de información	Correo electrónico		
Tipo de archivo solicitado	Documento en formato .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg		
Tipo de archivo enviado y/o anexado	Correo electrónico		
Corresponde a anexo número	18		
Item	**Información solicitada**	**Respuesta aportada**	**Aporte a la investigación**
1	Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014	Informa que no han realizado investigaciones sobre los temás planetados.	Permite demostrar el poco estudio sobre estos temás en grupos de investigación de Universidades del país, lo que ofrece a esta investigación un factor de proponderancia para que sea referente en este campo.
2	Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
3	Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
4	Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		

Tabla 50. Consolidado respuestas y aportes GIIT.

INVESTIGACION EXPLORATORIA			
NUEVAS TENDENCIAS EN SEGURIDAD INFORMATICA EN REDES MOVILES EN COLOMBIA			
ANÁLISIS DE INFORMACIÓN			
Institución y/o experto	Universidad ICESI		
Tipo de Institución y/o experto	GRUPO DE INVESTIGACIÓN DE INFORMÁTICA Y TELECOMUNICACIONES		
Fecha solicitud	26 de marzo de 2014		
Fecha respuesta	22 de septiembre de 2014		
Amparo legal	Constitución Política de Colombia, Art. 23. Derecho de petición.		
Medio de solicitud de información	Correo electrónico		
Medio de respuesta de información	Correo electrónico		
Tipo de archivo solicitado	Documento en formato .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg		
Tipo de archivo enviado y/o anexado	Correo electrónico		
Corresponde a anexo número	19		
Item	**Información solicitada**	**Respuesta aportada**	**Aporte a la investigación**
1	Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014	Informa que no han realizado investigaciones sobre los temás planetados.	Permite demostrar el poco estudio sobre estos temás en grupos de investigación de Universidades del país, lo que ofrece a esta investigación un factor de proponderancia para que sea referente en este campo.
2	Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
3	Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
4	Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		

Tabla 51. Consolidado respuestas y aportes 4G AMÉRICAS

INVESTIGACION EXPLORATORIA			
NUEVAS TENDENCIAS EN SEGURIDAD INFORMATICA EN REDES MOVILES EN COLOMBIA			
ANÁLISIS DE INFORMACIÓN			
Institución y/o experto	4G AMÉRICAS		
Tipo de Institución y/o experto	Organización internacional con sede en Estados Unidos, con enfoque comercial de la industria compuesta por proveedores de servicios y fabricantes de telecomunicaciones. La misión de la organización es fomentar el progreso de las tecnologías de banda ancha móvil por medio de la promoción de LTE, LTE Avanzado y especificaciones para 5G.		
Fecha solicitud	8 de abril de 2015		
Fecha respuesta	8 de abril de 2015		
Amparo legal	Solicitud de información respetuosa		
Medio de solicitud de información	Correo electrónico		
Medio de respuesta de información	Correo electrónico		
Tipo de archivo solicitado	Documento en formato .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .gpeg		
Tipo de archivo enviado y/o anexado	Correo electrónico		
Corresponde a anexo número	21		
Item	**Información solicitada**	**Respuesta aportada**	**Aporte a la investigación**
1	Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014	Informa acerca de documentos relevantes para el estudio de tendencias internacionales.	Permite conocer fuentes de consulta sobre las tendencias en cuanto a seguridad informática a nivel internacional.
2	Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
3	Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		
4	Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.		

8. DEFINICIÓN DE LOS SISTEMAS DE SEGURIDAD INFORMÁTICA PARA REDES MÓVILES.

8.1. NORMAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA APLICABLES A LAS REDES MÓVILES.

Se ha realizado un recorrido por las normas internacionales que regulan el sector de las redes móviles desde el enfoque de la seguridad informática aplicada a su infraestructura, con el objetivo de ofrecer al usuario una experiencia tecnológica segura, con características de servicio, como la velocidad de navegación óptima, la disponibilidad de contenidos multimedia y la posibilidad de movilizarse y obtener la cobertura de la señal necesaria, para continuar conectado al mundo virtual.

8.1.1. Tipología de Red Móvil para Colombia.

Para el caso de Colombia, es claro que en sus redes móviles, la tipología utilizada está dividida en dos grandes tipos: Redes 2G y 3G, que soportan los servicios de voz y datos, y las Redes 4G LTE, que su diseño permite su funcionamiento sobre las redes con conmutación de paquetes, así lo determinó el contrato CRC número 050 de 2014, de la Unión Temporal Axion - Telbroad Telecomunicaciones IT, “Consultoría para el uso compartido de infraestructura”. Lo anterior se ilustra en la siguiente figura.

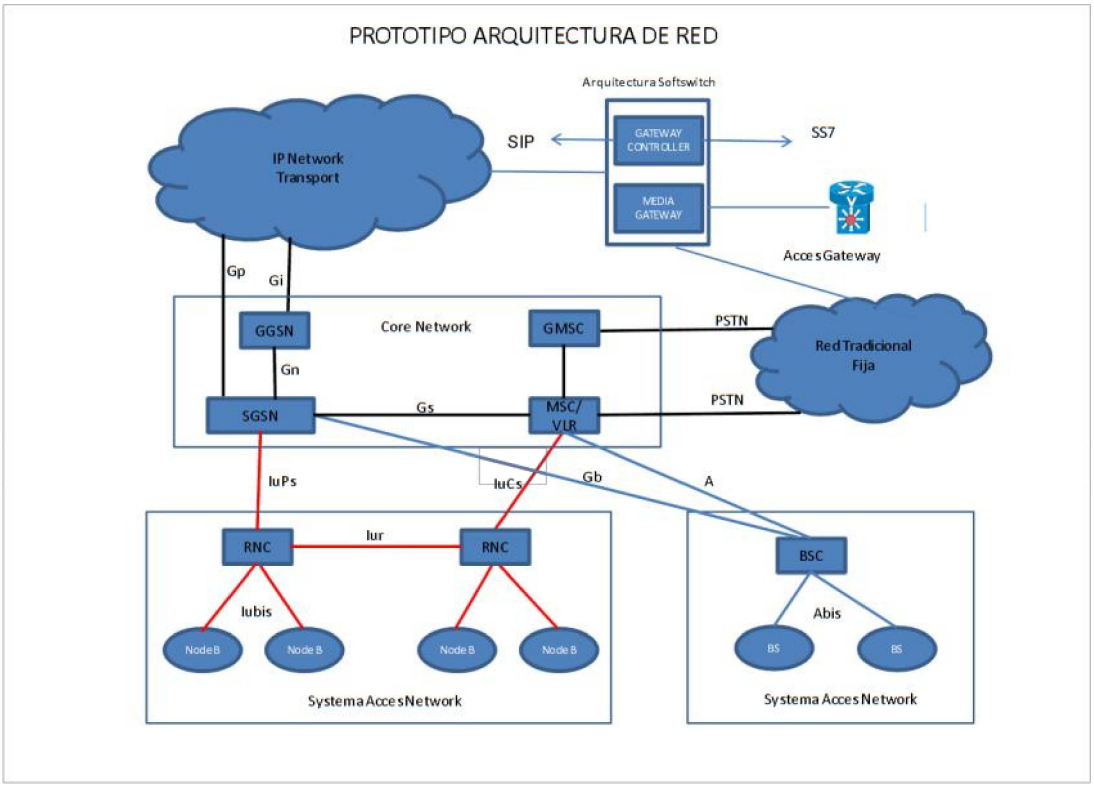

Figura 48. Prototipo de redes 2G y 3G utilizadas en Colombia.

Fuente: Contrato CRC 050 de 2014 Unión Temporal Axion - Telbroad Telecomunicaciones IT, “Consultoría para el uso compartido de infraestructura”, página 36.

Por el lado de las redes 4G LTE, que viene en crecimiento en Colombia, con cuatro operadores móviles, ofreciendo el servicio, que busca el transporte de los datos y la voz mediante la red IP. La siguiente figura, muestra la tipología de la red 4G utilizada en Colombia, aplicándose lo contenido en las normas internacionales ITU, en relación con 3GPP para el desarrollo del entorno de seguridad informática necesario para proteger el proceso de comunicación de datos y voz sobre toda la infraestructura.

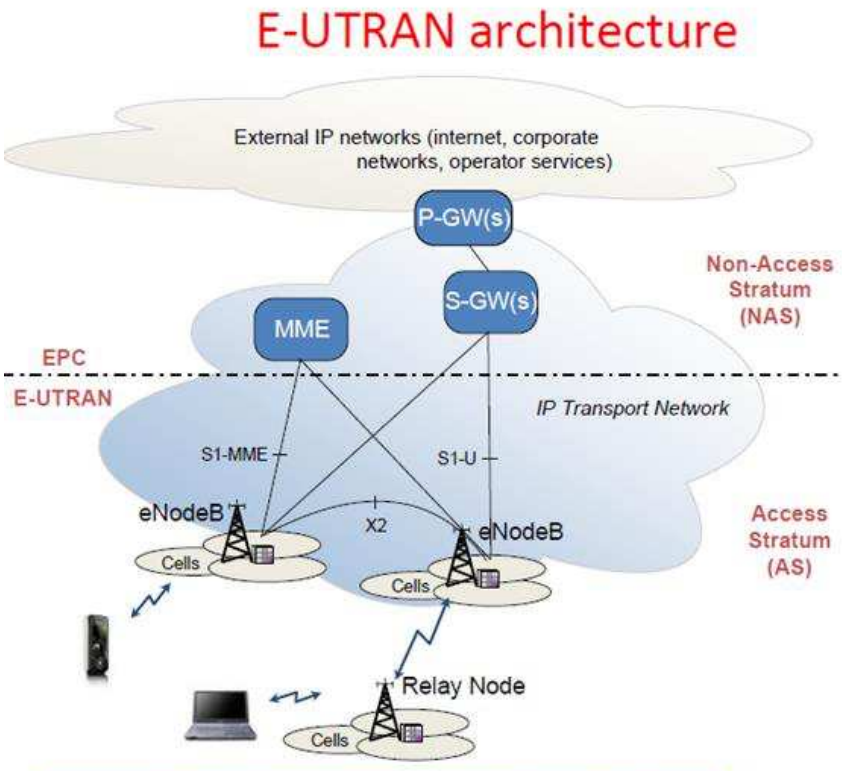

Figura 49. Prototipo de redes 4G utilizadas en Colombia.

Fuente. Contrato CRC 050 de 2014 Unión Temporal Axion - Telbroad Telecomunicaciones IT, “Consultoría para el uso compartido de infraestructura”, página 37.

8.1.2.Normas Legales Aplicables a la Seguridad Informática en las Redes Móviles para Colombia.

Mediante el documento “Aspectos regulatorios asociados a la ciberseguridad” de septiembre de 2009, la Comisión de Regulación de Comunicaciones de Colombia dedica los capítulos 5 al 8 para conocer el estado de las seguridad en las redes móviles en el país. De la revisión y análisis, se encuentra que la Recomendación ITU T X.1121, basada en la descripción de las amenazas de seguridad en las redes móviles de datos de extremo a extremo, y la Recomendación ITU T X.1122, que define dos modelos de PKI, la general y la

modo pasarela, que conecta la red móvil con la red abierta, son dos recomendaciones ya tratadas en los estudio de normas internacionales.

En el año 2011, mediante la Resolución 3502 de 2011, de fecha 11 de diciembre de 2011, "por la cual se establecen las condiciones regulatorias relativas a la neutralidad en internet, en cumplimiento de lo establecido en el artículo 56 de la Ley 1450 de 2011", les recuerda a los operadores móviles la obligación de implementar modelos seguridad que eviten el acceso no autorizado, la interrupción, el repudio o la interferencia deliberada en la transmisión de los datos, descritos en las Recomendaciones ITU-T X.1121 y X.1122 y para el caso del acceso a internet , solo deben aplicar lo previsto en la Recomendación ITU- T X.700.

Sin embargo las tendencias sobre seguridad informática para Colombia se enmarcan en el documento "Agenda Regulatoria 2015-2016", de octubre de 2014, de la Comisión de Regulación de Comunicaciones, donde se han identificado los temas que según las recomendaciones ITU, se deben abordar en cuanto a seguridad se refiere en el futuro próximo del país. Se ilustra en la siguiente figura.

Área temática	Potenciales proyectos a incluir AR 2015 - 2016
Protección del usuario	• Medidas para combatir el hurto, falsificación y mercado gris de dispositivos móviles.
Promover condiciones de libre y leal competencia	• Modelos actuales de interconexión y cómo se aplican en una nueva era de acceso a Internet de banda ancha y redes de nueva generación.
Desarrollo de infraestructura	• Condiciones regulatorias para facilitar el despliegue de redes de nueva generación. • Transición de IPV4 a IPV6. • Medidas para garantizar las comunicaciones en emergencias.
Internet, Contenidos y aplicaciones	• Desarrollo del Internet de las cosas. • Condiciones para promover la ciberseguridad. • Servicios de Cloud Computing. • Banca Móvil.

Figura 50. Tendencias sobre seguridad informática en las redes móviles para Colombia durante los años 2015 – 2016.

Fuente: Agenda Regulatoria 2015-2016, CRC, página 8.

En este marco, se ha logrado identificar lo que viene para las redes móviles en el país en materia de seguridad informática.

8.1.3. Guía para la Protección de Datos en Redes Móviles de Datos.

A la par a la realización del estudio sobre el nivel de desarrollo y confianza de la seguridad informática en las redes de datos móviles en el país, y aprovechando los resultados del mismo, se ha elaborado una guía para dar a conocer las diferentes usos y aplicaciones, los riesgos a los que están expuestas y desarrollar un catálogo de buenas prácticas y recomendaciones, para el manejo de la información y los datos en las redes de datos móviles.

El dispositivo, como el smartphone, tableta o ipad, debe ser usado como interfaz de ingreso de datos. Al contener o almacenar datos en el mismo, y existen conexión a redes móviles de datos, diferente a la celular, pueden acceder a los mismos sin que el usuario se entere de tal situación.

Se debe utilizar mecanismos adicionales al número celular, como por ejemplo, pin, contraseñas haciendo uso de caracteres especiales (#, $).

Utilizar protocolos de transmisión de datos, cifrados como el SSLv3.

A la hora de adquirir equipos móviles, tener cuidado donde son comprados, que cumplan con la normatividad colombiana y que se tenga factura de la transacción.

Al momento de descargar aplicaciones para los ambiente de sistema operativo sea android, IOS, blackberry OS, Symbian OS, Windows Phone, no usar las conocidas Markets alternativas o tiendas de app, toda que allí no existen

protocolos de seguridad, no se conoce la procedencia de la aplicación, y en muchos casos corresponde a Malware que corrompe le estado original del sistema y deja el mismo vulnerables a ataques informáticos.

Evitar el conocido ejecutar “rotue”, “flashing” o “jailbreak” en los dispositivos. Lo anterior afecta la integridad de la seguridad implementada de la arquitectura de cada sistema operativo móvil.

La actualización que se recomienda por los fabricantes de los sistemas operativos móviles, debe ser ejecutada. Posponer esta actividad, puede afectar gravemente el rendimiento del dispositivo.

Realizar de forma periódica las copias de seguridad de los datos contenidos en los dispositivos móviles.

Los enlaces contenidos en mensajes SMS, que llegan al buzón del dispositivo móvil, no se deben abrir.

El uso de herramientas como Bluetooth o Wifi, se debe activar solo cuando sea necesario.

La instalación de herramientas para la detección de malware se hace necesaria.

En el dispositivo debe estar configurada la autenticación del usuario.

Conocer el número de IMEI (International Mobile EquipmentIdentity), que permite al usuario, en conjunto con la operadora móvil desactivar el dispositivo en caso de robo o pérdida del mismo. Para conocerlo basta marcar *#06#.

Activación de la funcionalidad de borrado remoto, debido a que los dispositivos por su tamaño son susceptibles de perdida y por ende de los datos sensibles tanto del usuario como de la empresa o sector para el cual trabaja.

Conexión VPN obligatoria, cuando el dispositivo quiera acceder a recursos propios para la empresa para la cual trabaja. Esto generará controles parametrizados de la navegabilidad de los usuarios en la red interna de la empresa y los servicios y recursos que está aprovechando

Establecer contraseñas seguras, en combinación de letras, números y símbolos, tanto al inicio del dispositivo móvil como cuando se deja de usar por algún tiempo.

En cuanto a las cámaras y micrófonos integrados en los dispositivos móviles es importante bloquear la captura de imágenes o sonidos que afecten la privacidad del usuario. Lo anterior se puede realizar mediante cintas aislantes u otros accesorios que mejoren la privacidad de los usuarios.

Realizar periódicamente copias de seguridad o backup del contenido del dispositivo móvil.

9. CONCLUSIONES

Al finalizar la investigación, se ha determinado que no existe la suficiente socialización de la información acerca de las formas en que se protege la información en las redes móviles de los usuarios.

En el campo de la industria de la redes móviles, se determinó que la ley colombiana no obliga a quienes comercializan los servicios de conectividad a redes móviles a informar a los usuario de cómo y de qué manera, y bajo que estándares y protocolos administran los datos confidenciales de los usuarios y tampoco a informar si han tenido incidentes de seguridad informática en sus redes.

En el campo de gobierno y control de entidades, no existen estudios técnicos a profundidad acerca de la seguridad informática en las redes móviles en Colombia, en razón a que las autoridades de control como el Ministerio de Tics y la Superintendencia de Industria y Comercio, no cuentan con las herramientas jurídicas necesarias para obtener de los operadores de los servicios, reportes detallados e informe técnicos acerca de cómo se despliegan sus redes móviles de datos, como son protegidos los datos de los usuarios y si se han presentado incidentes de seguridad informática.

En el campo legislativo, al no existir una legislación profunda sobre la seguridad informática aplicable a las redes móviles en Colombia, el ente investigador y acusador como lo es la Fiscalía General de la Nación, enmarca las conductas y posibles delitos informáticos en base a la legislación actual, dejando vacíos en la judicialización de estos delitos.

En el campo académico, los grupos de investigación de Universidades de Colombia consultados, no existen trabajos acerca de la seguridad informática en redes móviles.

Sin embargo, la información acerca de las normas, estándares y protocolos de seguridad informática utilizados para la transmisión de los datos en Colombia, se obtuvo gracias a la investigación exploratoria realizada.

De igual manera, se pudo identificar, las nuevas tecnologías que se aplicarán a las redes móviles en Colombia, mostrando la ruta a seguir frente al uso de las mismas y la oportunidad de conocer los conceptos clave para la protección de la información de los usuarios y lograr la confidencialidad, integridad y disponibilidad de los datos.

10. RECOMENDACIONES

Las recomendaciones se enfocan en que el Gobierno de Colombia, presente leyes a consideración del poder legislativo, que entregue las herramientas jurídicas necesarias al Ministerio de TICS, a la Superintendencia de Industria y Comercio, y la Fiscalía General de la Nación, para poder conocer en detalle los protocolos y estándares utilizados, así como el tratamiento de la información confidencial de los usuarios por parte de los operadores de las redes móviles en el país, donde estén obligados a reportar los incidentes de seguridad presentados, los usuarios afectados y la información, sin que con ello se menoscabe la seguridad nacional, ni la seguridad de los datos de los demás usuarios de las redes móviles.

También se hace necesario que las Universidades del país, incentiven la investigación acerca de la seguridad informática aplicada a las redes móviles, en atención a que cada vez más se hace uso de las mismas, para la transmisión de los datos y que ofrezca a la comunidad científica como a la sociedad herramientas de autoprotección de la información y las precauciones necesarias en el uso de los dispositivos móviles sobre dichas redes.

11. BIBLIOGRAFIA

International Telecommunication Union ITU. Serie Y: Infraestructura mundial de la Información, aspectos del protocolo Internet y redes de la próxima generación. Redes de la próxima generación – Marcos y modelos arquitecturales funcionales. Visión general de las redes de próxima generación. Recomendación UIT-T Y.2001. Comisión de Estudio 13 (2005-2008) del UIT-T. Ginebra, Suiza. 2005. 10 p.

International Telecommunication Union ITU. Serie Y: Infraestructura mundial de la Información, aspectos del protocolo Internet y redes de la próxima generación. Requisitos de seguridad para las redes de la próxima generación, versión 1. Recomendación UIT-T Y.2701. Comisión de Estudio 13 (2005-2008) del UIT-T. Ginebra, Suiza. 2007. 32 p.

International Telecommunication Union ITU. Serie Y: Infraestructura mundial de la Información, aspectos del protocolo Internet y redes de la próxima generación. Redes de la próxima generación – Seguridad. Mecanismos y procedimientos de seguridad para las NGN. Recomendación UIT-T Y.2704. Comisión de Estudio 13 del UIT-T. Ginebra, Suiza. 2010. 50 p.

International Telecommunication Union ITU. Serie Y: Infraestructura mundial de la Información, aspecto s del protocolo Internet y redes de la próxima generación. Redes de la próxima generación – Seguridad. Marco de seguridad para la movilidad en las NGN. Recomendación UIT-T Y.2760. Comisión de Estudio 13 del UIT-T. Ginebra, Suiza. 2011. 29 p.

International Telecommunication Union ITU. Serie Q: Conmutación y señalización. Requisitos y protocolos de señalización para la red IMT-2000.

Marco para las redes de las telecomunicaciones móviles internacionales-2000 (IMT-2000). Recomendación UIT-T Q.1701. Comisión de Estudio 11 (1997-2000) del UIT-T. Ginebra, Suiza. 1999. 20 p.

International Telecommunication Union ITU. Serie Q: Conmutación y señalización. Visión a largo plazo de las características de las redes posteriores a las redes de las comunicaciones móviles internacionales - 2000(IMT-2000). Recomendación UIT-T Q.1702. Comisión de Estudio SSG (2001-2004) del UIT-T. Ginebra, Suiza. 2002. 7 p.

International Telecommunication Union ITU. Serie Q: Conmutación y señalización. Marco de capacidades de servicio y de red desde la perspectiva de la red para los sistemas posteriores a las IMT-2000. Recomendación UIT-T Q.1703. Comisión de Estudio SSG (2001-2004) del UIT-T. Ginebra, Suiza. 2004. 45 p.

International Telecommunication Union ITU. Serie X: Redes de datos y comunicación entre sistemas abiertos. Seguridad. Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo. Recomendación UIT-T X.805. Comisión de Estudio 17 (2001-2004) del UIT-T. Ginebra, Suiza. 2003. 16 p.

International Telecommunication Union ITU. Serie X: Redes de datos y comunicación entre sistemas abiertos. Seguridad de las telecomunicaciones. Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremos a extremo. Recomendación UIT-T X.1121. Comisión de Estudio 17 (2001-2004) del UIT-T. Ginebra, Suiza. 2004. 16 p.

International Telecommunication Union ITU. Serie X: Redes de datos y comunicación entre sistemas abiertos. Seguridad de las telecomunicaciones. Directrices para la implementación de sistemas móviles seguros basados en la infraestructura de claves públicas. Recomendación UIT-T X.1122. Comisión de Estudio 17 (2001-2004) del UIT-T. Ginebra, Suiza. 2004. 24 p.

International Telecommunication Union ITU. Serie Q: Conmutación y señalización. Referencias de IMT-2000 a la publicación de 1999 del sistema global para comunicaciones móviles que ha evolucionado hacia la red medular del sistema de telecomunicaciones móviles universales con la red de acceso de la red terrenal de acceso radioeléctrico del sistema de telecomunicaciones móviles universales. Recomendación UIT-T Q.1741. Comisión de Estudio SSG (2001-2004) del UIT-T. Ginebra, Suiza. 2002. 153 p.

International Telecommunication Union ITU. Serie M: Rgt y mantenimiento de redes. Sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales. Red de gestión de las telecomunicaciones. Servicios de gestión de la RGT para la gestión de la seguridad de las telecomunicaciones móviles internacionales-2000 (IMT-2000). Recomendación UIT-T M.3210.1.1741. Comisión de Estudio 4 (2001-2004) del UIT-T. Ginebra, Suiza. 2001. 22 p.

International Telecommunication Union ITU. XSTR-PKIS. Desafíos actuales y futuros para estandarización de la infraestructura de clave pública. Reporte técnico. Inglés. Comisión de Estudio 17 del UIT-T. Ginebra, Suiza. 2014. 42 p.

International Telecommunication Union ITU. XSTR-PKIS. Desafíos actuales y futuros para estandarización de la infraestructura de clave pública. Reporte técnico. Inglés. Comisión de Estudio 17 del UIT-T. Ginebra, Suiza. 2014. 42 p.

ETSI. Universal Mobile Telecommunications System (UMTS); LTE; Proximity-based Services (ProSe); Security aspects (3GPP TS 33.303 version 12.2.0 Release 12). Especificación técnica. Inglés. Referencia RTS/TSGS-0333303vc20. Francia. 2015. 66 p.

Comisión de Regulación de Comunicaciones. República de Colombia. Contrato CRC 050 de 2014- Consultoría para el uso compartido de infraestructura. Análisis técnico y económico para la compartición de infraestructura en la red de telecomunicaciones. Unión Temporal Axion-Telbroad. Bogotá D.C. 19 de diciembre de 2014. 226 p.

Comisión de Regulación de Comunicaciones. República de Colombia. Agenda Regulatoria 2015-2016. Borrador para comentarios. Relaciones de Gobierno y Asesoría. Bogotá D.C. Octubre de 2014. 30 p.

Comisión de Regulación de Comunicaciones. República de Colombia. Agenda Regulatoria 2015-2016. Relaciones de Gobierno y Asesoría. Bogotá D.C. Diciembre de 2014. 17 p.

ERICSSON AB. Introduction of high-speed data in GSM/GPRS networks. Ericsson AB. 2003. AE/LZT 123 7058 R2. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet: <http://www.satnac.org.za/proceedings/2003/plenary/EricssonEDGE.pdf>

Seminario de redes SS7/GSM/(E)GPRS. (Argentina). Memorias. Tektronix. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet:<http://www.ladeprofesional.com.ar/seminariok15-gsm-gprs.pdf>

TELECO, Inteligencia en Telecomunicaciones (Brasil). Rev 21 de febrero abril de 2015. [Citado en 21 de febrero de 2015].Disponible en internet: <http://www.teleco.com.br/imagens/es_imagens/figura1_tutorialgsm.gif>

Colombia, Congreso de la República. Ley 37 (6, enero, 1993). Por la cual se regula la prestación del servicio de telefonía móvil celular, la celebración de contratos de sociedad y de asociación en el ámbito de telecomunicaciones y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C. 1993. P. 1-8.

AUGUSTI, Ramón. BERNARDO, Francisco. CASADEVALL, Fernando. FERRÚS, Ramón. PÉREZ-ROMERO, Jordi. SALLENT, Oriol. LTE: Nuevas tendencias en comunicaciones móviles. Fundación Vodafone. España. 2010. ISBN: 84-934740-4-5. 431 p. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<https://proyectolte.files.wordpress.com/2012/09/lte-nuevas-tendencias.pdf>

Qualcomm. Sitio web. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<https://www.qualcomm.com/>

4g Américas. Estado LTE-Advanced a 25 de marzo de 2015. Inglés. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<http://www.4gamericas.org/files/2314/2723/0862/LTE-Advanced_3.25.15.pdf/>

4g Américas. Quiénes somos. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet: <http://www.4gamericas.org/es/about-us/>

Gsma. Economía Móvil América Latina 2014. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<http://latam.gsmamobileeconomy.com/GSMA_ME_LatinAmerica_2014_ES.pdf>

4g Américas. LTE en América Latina y el Caribe. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet: http://www.4gamericas.org/es/resources/infographics/lte-en-america-latina-y-el-caribe/>

Blog Cisco Cansac. Tráfico de datos móviles crecerá casi 10 veces en los próximos cinco años, predice estudio Cisco Visual Networking Índex (VNI). Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet: <http://gblogs.cisco.com/cansac/trafico-de-datos-moviles-crecera-casi-10-veces-en-los-proximos-cinco-anos-predice-estudio-cisco-visual-networking-index-vni/>

Capítulo II. Aspectos generales del sistema de telefonía móvil umts de tercera generación. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet: <http://www.tierradelazaro.com/cripto/UMTS.pdf>

Universitat de Valencia. GPRS. España. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en internet: <http://www.uv.es/~montanan/redes/trabajos/GPRS.doc>

Diseño, integración y optimización de estaciones bases de segunda generación. GSM. España. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015].Disponible en

internet:<http://bibing.us.es/proyectos/abreproy/11980/fichero/CAP%CDTULO+3+-+FUNDAMENTOS+GSM+Y+UMTS%252F3.3+GSM.pdf>

International TelecommunicationUnion ITU. Visión general. Ginebra, Suiza. Rev 30 de marzo de 2015. [Citado en 30 de marzo de 2015]. Disponible en internet:<http://www.itu.int/es/about/Pages/overview.aspx>

Marketing news. Infografía: la explosión de los smartphone en Colombia 2014. Bogotá. D.C. Rev 15 de abril de 2014. [Citado en 15 de abril de 2014].Disponible en internet:<http://www.marketingnews.com.co/infografia-la-explosion-de-los-smartphones-en-colombia-2014/>

Redes móviles, Zdenek Becvar, Pavel Mach, Ivan Pravda. Rev. 15 de abril de 2015. [Citado en 15 de abril de 2014].Disponible en internet:< improvet.cvut.cz/project/download/C4ES/Redes_moviles.pdf >

12. ANEXOS

Anexo 1. Cuadro SPOA, consolidado delitos informáticos ley 1273 de 2009, desde el año 2010-2014 en redes de telecomunicaciones, Fiscalía General de la Nación.

DELITO	2010-2014
Obstaculización ilegitima del sistema informático o red de telecomunicación art 269b ley 1273 de 2009	96
Obstaculización ilegitima del sistema informático o red de telecomunicación art 269b ley 1273 de 2009, agravado por aprovecharse de la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. Art. 269h n3	2
Obstaculización ilegitima del sistema informático o red de telecomunicación art 269b ley 1273 de 2009, agravado por obtener provecho para sí o para un tercero. Art. 269h n5	2
Obstaculización ilegitima del sistema informático o red de telecomunicación art 269b ley 1273 de 2009, agravado por ser con fines terroristas o generando riesgo para la seguridad o defensa nacional. Art. 269h n6	2
Obstaculización ilegitima del sistema informático o red de telecomunicación art 269b ley 1273 de 2009, agravado por utilizar como instrumento a un tercero de buena fe art. 269h n7	2
TOTAL	**104**

Anexo 2.Legislación Informática de República de Colombia

Ley 1273 de 5 de enero de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Código procesal penal de 1987, que tutela la inviolabilidad del domicilio y regula en su artículo 376 las escuchas telefónicas.

Ley de Protección de datos de 1988.

Anexo 3. Respuesta Fiscalia General de la Nación

FISCALIA
GENERAL DE LA NACION

Bogotá, D.C., abril 10 de 2014

Evidentix: No.852217

Señor
WILMAR LIBERTO COPETE MARÍN
Calle 25 No. 7-48 piso 11 Barrio Lago – Pereira
Teléfono 3113939488 - 3207544436
Pereira – Risaralda.

REFERENCIA: Respuesta Derecho de Petición WILMAR COPETE MARÍN.

Teniendo en cuenta su solicitud allegada a nuestro sitio Web desde la cuenta de correo wilmar.copete@unad.edu.co el día 24 de marzo de 2014 a las 05:52pm y radicada con el numero GDPQ – No. 20146110461302 de fecha 25-03-2014, en la que requiere "En atención al proyecto de tesis de mi especialización en seguridad informática llamado "NUEVAS TENDENCIAS DE SEGURIDAD INFORMATICA EN LAS REDES DE DATOS MÓVILES EN COLOMBIA", solicito a ustedes de manera respetuosa la siguiente información" , seguido de su solicitud enumera dos interrogantes; por lo anterior me permito dar respuesta citando cada uno de los interrogantes y se dará respuesta de manera sucesiva así:

1- "Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas los usuarios (ciudadanos que han denunciado en cuanto a cantidad de delitos, tipo de delitos, zonas de influencia método de ataque –pc, Tablet, teléfono móvil, Smartphone- y las empresas, compañías tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en el país desde años 2010 a 2014."

Por no ser de las funciones del grupo de delitos informáticos el manejo de la estadística se direccionó este primer ÍTEM A La Dirección Nacional de Fiscalías a razón que pueden realizar esta consulta estadística en el Sistema de información Judicial de la Fiscalía General de La Nación Sistema Penal Acusatorio SPOA – (Ley 906 de 2004), esta dependencia en oficio Numero DNF 11804 anexa un CD-R Marca PRINCO 700MB/80Min, Color Blanco con numero en el anillo interno P414192111501111 y rotulado con la inscripción manuscrita en color rojo "Delitos Informático 2010-2014."

En la anterior estadística de acuerdo a la conducta punible, se enmarca de acuerdo a los preceptos de LEY 1273 DE 2009, discriminado la región del País en el que se cometió la vulneración del bien jurídico tutelado; es de aclarar que para determinar el medio por el cual se comete la conducta no da mayor relevancia a la estadística si no al investigador el sus labores de judicialización y no se cuenta con esta estadística.

2- "Tendencia, estudios y recomendaciones en seguridad informática tanto para usuarios (ciudadanos) y de las empresas, compañías tanto nacionales como extranjeras

(operadores de telefonía móvil y datos en sus diferentes redes de datos móviles en el país desde el año 2010 a 2014."

En lo que respecta a este ÍTEM La Fiscalía General De La Nación no cuenta con un programa en tendencias estudios y recomendaciones en seguridad informática dirigido a sus clientes externos toda vez que sus funciones están encaminadas en la misión institucional "La Fiscalía General de la Nación ejerce la acción penal y elabora y ejecuta la política criminal del Estado; garantiza la tutela judicial efectiva de los derechos de los intervinientes en el proceso penal; genera confianza y seguridad jurídica en la sociedad mediante la búsqueda de la verdad, la justicia y la reparación."

Anteponiendo los preceptos de nuestra Constitución Política de Colombia Art 250: Corresponde a la Fiscalía General de la Nación, de oficio o mediante denuncia o querella, investigar los delitos y acusar a los presuntos infractores ante los juzgados y tribunales competentes. Se exceptúan los delitos cometidos por miembros de la Fuerza Pública en servicio activo y en relación con el mismo servicio. Para tal efecto la Fiscalía General de la Nación deberá:

1. Asegurar la comparecencia de los presuntos infractores de la ley penal, adoptando las medidas de aseguramiento. Además, y si fuere del caso, tomar las medidas necesarias para hacer efectivos el restablecimiento del derecho y la indemnización de los perjuicios ocasionados por el delito.

2. Calificar y declarar precluidas las investigaciones realizadas.

3. Dirigir y coordinar las funciones de policía judicial que en forma permanente cumplen la Policía Nacional y los demás organismos que señale la ley.

4. Velar por la protección de las víctimas, testigos e intervinientes en el proceso.

5. Cumplir las demás funciones que establezca la ley.

El Fiscal General de la Nación y sus delegados tienen competencia en todo el territorio nacional.

La Fiscalía General de la Nación está obligada a investigar tanto lo favorable como lo desfavorable al imputado, y a respetar sus derechos fundamentales y las garantías procesales que le asisten.

Por ultimo si llegara a ser importante para futuras consultas; me permito comunicarle que la Fiscalia General De la Nación cuenta con un Grupo de Delitos Informáticos el cual realiza investigación y otras de cómputo forense que es la que está directamente relacionada con este tipo de delitos.

CUERPO TÉCNICO DE INVESTIGACIÓN - GRUPO DE DELITOS INFORMÁTICOS
CARRERA 28 No. 17A – 00, OFICINA 125, BOGOTÁ D.C.
CONMUTADOR 4088000 EXT. 3110 FAX 3111
www.helber.corredor@fiscalia.gov.co

FISCALIA
GENERAL DE LA NACIÓN

URL de consulta: http://web/oficinas/nuestra_entidad/nuestra_entidad.asp#funciones

Anexo: Un (1) CD-R Marca PRINCO 700MB/80Min, Color Blanco con numero en el anillo interno P414192111501111 y rotulado con la inscripción manuscrita en color rojo "Delitos - Informáticos 2010-2014."

Cordialmente,

HELBER CORREDOR CASTIBLANCO
Técnico Investigador I
Código 14873

Vo. Bo.

ADOLFO HERNANDO VASQUEZ TELLEZ
Coordinador Nacional Grupo Delitos Informáticos.

CUERPO TÉCNICO DE INVESTIGACIÓN - GRUPO DE DELITOS INFORMÁTICOS
CARRERA 28 No. 17A – 00, OFICINA 125, BOGOTÁ D.C.
CONMUTADOR 4088000 EXT. 3110 FAX 3111
www.helber.corredor@fiscalia.gov.co

Anexo 4. Respuesta Ministerio de Tecnologías de la Información y Comunicación de Colombia- MinTic

MinTIC
Ministerio de Tecnologías de la Información y las Comunicaciones

PROSPERIDAD PARA TODOS

002053

Código TRD: 221.101.001
PQRSD - 2014

Bogotá,

MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
FECHA: 4/6/2014 HORA: 10:34:29 FOLIOS: 1
REGISTRO NO: **730938**
DESTINO: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
DIRECCION: CALLE 14 NO. 14 - 23 SUR

Señor
WILMAR LIBERTO COPETE MARÍN
Docente ECBTI
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
Manzana 10 A Casa 11 Belmonte.
Pereira.
Risaralda

Asunto: Respuesta al Radicado 598544. Solicitud de información para su tesis de especialización en seguridad informática.

Respetado Señor Copete.

Por medio de la presente, esta Subdirección da respuesta al radicado del asunto.

Respecto de las preguntas de los numerales 1, 2 y 4, en los cuales solicita información relacionada con la situación y diagnóstico en cuanto a seguridad informática de los operadores de telefonía móvil y de datos tanto nacionales como extranjeros, haciendo énfasis en la infraestructura, despliegue, cobertura, mantenimiento, tendencias, estudios y protocolos de seguridad informática en el período 2010 - 2014, nos permitimos responder que el marco normativo[1] que regula los reportes periódicos de información por parte de los Prestadores de Redes y Servicios de Telecomunicaciones (PRST) no les obliga a entregar los datos que permitan consolidar el informe que usted requiere. En consecuencia, sugerimos dirigirse directamente a ellos para hacer su solicitud. Puede realizar la consulta de los datos de contacto de los PRST de su interés a través en la página web www.mintic.gov.co en las pestañas "Sector TIC" y "Registro TIC".

La Dirección de Estándares y Arquitectura de T.I. de este Ministerio, respondió la pregunta del numeral 3 de la siguiente manera:

> *"El ministerio TIC en la dirección de vigilancia y control, tiene una herramienta (matriz de obligaciones), que contiene los ámbitos jurídicos, técnicos y financieros que les aplican a los PRST y PRSTM, entre estas normas están la ley 1341, ley 679 de 2001, decreto 1524 de 2002, ley 1356 de 2009, regulación de la CRC, entre otros. De acuerdo al art. 2.3 - del capítulo técnico de la resolución -- CRC 3067 de 2011; el ministerio TIC, debe verificar que el operador tenga un modelo de*

[1] Comisión de Regulación de Comunicaciones. Resoluciones 3067 de 18-may-2011, 3496 de 15-dic-2011, 3503 de 19-dic-2011, 4000 de 09-nov-2012 y 4007 de 16-nov-2012

Edificio Murillo Toro, Carrera 8a. entre calles 12 y 13
Código Postal: 111711 , Bogotá, Colombia
T: +57 (1) 3443460 Fax: 57 (1) 344 2248
www.mintic.gov.co
www.vivedigital.gov.co

vive digital Colombia

MinTIC
Ministerio de Tecnologías de la Información y las Comunicaciones

PROSPERIDAD PARA TODOS

002055

Código TRD: 221.101.001
PQRSD - 2014

MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
FECHA: 30/5/2014 HORA: 16:59:28 FOLIOS: 3
REGISTRO NO: 730378
TRAMITE A: DIRECCION DE ESTANDARES Y ARQ DE T.I.JORGE FERNANDO BEJARANO

Bogotá D.C.,

Doctor
JORGE FERNANDO BEJARANO.
Director de Estándares y Arquitectura de TI.
MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.
Carrera 8 entre calles 12 A y 12 B.
Ciudad.

Asunto: Traslado del Radicado 598544. Solicitud de información para la tesis de especialización en seguridad informática del Señor Wilmar Copete.

Respetado Doctor Bejarano,

Por medio de la presente esta Subdirección le traslada el radicado del asunto para contestar el punto tercero por considerarlo de su competencia. Solicitamos el favor de contestar de manera directa al peticionario, pues, por nuestra parte, ya le hemos contestado de manera directa las preguntas de los numerales 1, 2 y 4.

Cordialmente,

GLORIA PATRICIA PERDOMO RANGEL
Subdirectora de Industria de Comunicaciones.

Anexo: Radicado 598544 (2 folios).
CC: Wilmar Liberto Copete M. Manzana 10 A, Casa 11 Belmonte, Pereira, Risaralda.

Elaboró: Iván Rosero – Subdirección de Industria de Comunicaciones MIntic (16-may-2014).
Revisó: Gloria Amparo Rico – Asesora Jurídica de la Subdirección para la Industria de Comunicaciones Mintic.

Anexo 5. Respuesta Superintendencia de Industria Comercio.

Industria y Comercio
SUPERINTENDENCIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
RAD: 14-064590- -00001-0000 Fecha: 2014-03-31 13:31:00
DEP: 72 G.ATENCIUDADANO
TRA: 317 DP-PETICION EVE: SIN EVENTO
ACT: 440 RESPUESTA Folios: 1

Bogotá D.C.,

72

Señor
WILMAR LIBERTO COPETE MARIN
wilmar.copete@unad.edu.co

Asunto: Radicación: 14-064590- -00001-0000
Trámite: 317
Evento: 0
Actuación: 440
Folios: 1

Estimado(a) Señor:

En atención a su comunicación radicada bajo el número del asunto, relacionada con su proyecto de tesis, me permito informarle que de conformidad con las atribuciones conferidas por mandato legal a la Superintendencia de Industria y Comercio, en especial por el decreto 4886 de 2011, corresponde a esta entidad, entre otras funciones, velar por el cumplimiento de las normas sobre Protección del Consumidor, de acuerdo con lo establecido en la Ley 1480 de 2011 – Estatuto del Consumidor - dar cumplimiento a las disposiciones relativas a la calidad, la idoneidad, las garantías, las marcas, las leyendas, las propagandas y la fijación pública de precios de bienes y servicios y la responsabilidad de sus productores, expendedores y proveedores; así como a la Protección de la Competencia y Prácticas Comerciales Restrictivas; de igual forma administrar el Sistema Nacional de la Propiedad Industrial y tramitar y decidir los asuntos relacionados con la misma.

De acuerdo con la consulta planteada por usted, le sugerimos que se acerque a la entidad competente en el tema que sería el Ministerio de Tecnología de la Información y las comunicaciones .

Le agradecemos por darnos la oportunidad de atenderlo y le recordamos que cualquier sugerencia, reclamo o inconformidad con la respuesta dada por esta entidad la puede enviar al correo electrónico contactenos@sic.gov.co.

Para obtener mayor información sobre el desarrollo de las funciones de esta Superintendencia, puede dirigirse a la página de internet www.sic.gov.co. Adicionalmente, puede comunicarse con el centro de atención telefónica en Bogotá, al número 5920400 y en el ámbito nacional a la línea gratuita 018000 – 910165, de lunes a viernes de las 7:00h a las 19:00h y los sábados de las 8:00h a las 13:00h.

Anexo 6.Respuesta Comisión de Regulación Comunicaciones- CRC.

Respuesta Automatica Re: Derecho de petición Solicitud respetuosa de información

Atención Cliente CRC <atencioncliente@crcom.gov.co> 25 de marzo de 2014, 8:
Para: wilmar.copete@unad.edu.co

La Comisión de Regulación de Comunicaciones -CRC- ha recibido su comunicación. Sin embargo, le aclaramos que frente a los inconvenientes que se puedan presentar entre los proveedores y los usuarios, por la prestación de servicios de comunicaciones, esta Entidad solamente puede orientar a los usuarios sobre la normatividad que aplica en cada caso particular, de acuerdo con lo dispuesto en el Régimen de Protección a Usuarios.

Dado lo anterior, le informamos que usted recibirá respuesta a su comunicación en los próximos días, de acuerdo al tipo de solicitud:

Derecho de petición de documentos	10 días hábiles
Peticiones, quejas, reclamos o sugerencias	15 días hábiles
Consultas o conceptos	30 días hábiles

Igualmente, le manifestamos que cuando un usuario tiene un inconveniente o inconformidad frente a los servicios de comunicaciones, debe presentar su reclamación directamente al proveedor que le presta el servicio para que le dé respuesta dentro de los 15 días hábiles siguientes a su presentación.

Para solicitar información adicional, puede comunicarse con las personas encargadas del proceso de Atención al Cliente al Teléfono +57 (1) 3198300 ext. 8314.

Anexo 7. Respuesta AVANTEL

Respuesta Caso 6690644 WILMAR L. COPETE MARIN

1 mensaje

Aleida Montana <amontana@avantel.com.co> 28 de marzo de 2014, 9:03
Para: wilmar.copete@unad.edu.co

Señor
WILMAR L. COPETE MARIN
Pereira (Risaralda)

Asunto: Derecho de Petición Solicitud información.

Respetado Señor Copete:

En atención a requerimiento presentado el día 25 de marzo de 2014, con el que se está solicitando información para el proyecto de tesis de su especialización en seguridad informática llamado "Nuevas Tendencias de Seguridad Informática en las Redes de Datos Móviles en Colombia", al respecto nos permitimos comunicarle que esta información es confidencial de la Compañía. El Ministerio de Comunicaciones o la CRC son las fuentes oficiales de dicha información.

Esperamos con lo anterior dar respuesta oportuna a su solicitud.

Por disposición de la Comisión de Regulación de Comunicaciones en su Res 3066, Art. 47.2 del 18 de mayo de 2011, el siguiente párrafo debe ser incluido en esta comunicación:

"Señor usuario, dentro de los siguientes diez (10) días hábiles contados a partir de que usted tiene conocimiento de esta decisión, si lo elige, usted puede presentar recurso de reposición y en subsidio de apelación. Lo anterior, significa que usted puede presentar nuevamente una comunicación mediante la cual manifieste su inconformidad con la presente decisión, en los casos en que la misma le sea desfavorable total o parcialmente, con el fin de que volvamos a revisar su caso particular.

Igualmente, si así lo quiere, en el mismo momento que presente la comunicación antes mencionada, puede expresar su interés de que su caso sea revisado y resuelto de fondo por la autoridad de vigilancia y control, es decir, por la Superintendencia de Industria y Comercio –SIC-, en el evento en que la decisión frente a su petición o queja sea confirmada o modificada y nuevamente le sea desfavorable.

Tenga en cuenta, que la comunicación referida, puede presentarla en forma verbal o escrita, a través de nuestras oficinas físicas de atención al usuario, nuestra página Web, nuestra página de red social o a través de nuestra línea gratuita de atención al usuario".

Convencidos que nuestro crecimiento está reflejado en su satisfacción, quedamos a la espera de cualquier inquietud. Si requiere mayor información con gusto lo atenderemos en nuestra línea de Servicio al Cliente (1) 3 350350 en Bogotá y para el resto del país esta disponible la línea gratuita 018000519530 o desde su AVANTEL marcando el *350 o ingresando a la página www.avantel.com.co soporte en línea Chat.

Caso 6690644

Cordialmente

Servicio al Cliente

Anexo 8. Respuesta UNE

Oficina Virtual UNE

1 mensaje

Oficina Virtual UNE. <servicioalcliente@une.com.co> 26 de marzo de 2014, 10:09
Responder a: "Oficina Virtual UNE." <servicioalcliente@une.com.co>
Para: "wilmar.copete@unad.edu.co" <wilmar.copete@unad.edu.co>

Señor (a) WILMAR LIBERTO COPETE MARIN

Correo electrónico: wilmar.copete@unad.edu.co

Canal utilizado para la atención: Virtual

Motivo de la atención: Peticiones

Servicio: UNE - No Aplica

Asunto: Constancia de presentación de PQR - Recibida el día 2014-03-25 13:12:41

Respetado usuario,

Hemos recibido de manera exitosa su PQR escrita a través de Oficina Virtual de Servicio al Cliente de UNE, la cual queda registrada con la Peticiones Número 3612140001198216 y radicado interno 1-2CUN1K3.

La respuesta le será enviada dentro de los próximos 15 días hábiles contados desde el día siguiente a su radicación a esta dirección de correo electrónico para efectos de notificación, de lo contrario procede el reconocimiento del silencio administrativo positivo a partir del siguiente día hábil de la fecha de compromiso, Resolución 3066 de 2011.

En caso de requerir información sobre su PQR, le solicitamos comunicarse con nuestra línea de atención nacional 01 8000 42 22 22, o línea en Medellín 444 41 41, o en nuestra página WEB en el enlace http://www.une.com.co/consultapqr/, informando el número con el cual ha quedado registrado su requerimiento. Para productos de Larga Distancia puede marcar 01 8000 515 150 o a través de nuestra página www.une.com.co/empresas en la sección Contáctenos, donde con gusto le atenderemos.

UNE le brinda la forma más cómoda y segura de pagar los servicios de telecomunicaciones de su hogar y/o empresa. Inscriba su factura en http://www.une.com.co/apps/facturaweb/ y realice cada mes sus pagos desde su computador, ahorrando costos de desplazamientos, tiempo y mensajería.

Nota: Este correo es de carácter informativo, le agradecemos no responderlo.

Cordialmente,

Anexo 9. Respuesta VIRGIN MOBILE.

Caso No. 1379641
CUN: 4852-14-0000005548

Bogotá D.C., Abril 08 de 2014

Señor
WILMAR COPETE
E-mail: wilmar.copete@unad.edu.co
Teléfono de contacto: 3207544436 - 3113939488
Bogotá D.C.

Asunto: Inconformidad por Otros Servicios.

Respetado Señor Wilmar:

En respuesta a su requerimiento del día 26/03/2014, donde nos indica que En atención al proyecto de tesis de mi especialización en seguridad informática llamado "NUEVAS TENDENCIAS DE SEGURIDAD INFORMÁTICA EN LAS REDES DE DATOS MÓVILES EN COLOMBIA.", solicito a ustedes de manera respetuosa la siguiente información.

1. Situación y diagnóstico de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras(operadores de telefonía móvil y datos) en cuanto a la seguridad informática implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.

2. Situación y diagnóstico en cuanto a la infraestructura, despliegue, cobertura, mantenimiento y protocolos de seguridad informática en cuanto a las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) implantada en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.

3. Hallazgos en cuanto a los ataques informáticos, delitos informáticos y diferentes incidentes de seguridad informática que han sido víctimas las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.

4. Tendencias y estudios de seguridad informática de las empresas, compañías, tanto nacionales como extranjeras (operadores de telefonía móvil y datos) en sus diferentes redes de datos móviles en el país desde los años 2010 a 2014.

Al respecto le informamos que el derecho de petición y de acceso a la información pública, de acuerdo con los principios que rigen la función pública en Colombia se encuentran regulados en los 20, 23, 74 y 209 de la Carta Constitucional colombiana. Empero, en este caso, su petición se encuentra dirigida a una entidad privada que aunque presta el servicio público de telecomunicaciones móviles, evidencia que su petición no se enmarca dentro de la información que debe suministrarle. En efecto, no deben confundirse función pública y función administrativa con servicio público, pues si bien el servicio público de telecomunicaciones satisface una necesidad de interés general a cargo de particulares, bajo la vigilancia y control del Estado, la mayoría de las actividades adelantadas por la Prestadores de Redes y Servicios de Telecomunicaciones no implican el ejercicio de función pública o administrativa alguna, en cuanto no corresponden al ejercicio de competencias atribuidas a los órganos y servidores del Estado1.

De manera especial la jurisprudencia y la doctrina 2 ha señalado que las empresas de telecomunicaciones sólo desempeñan funciones públicas o administrativas cuando adoptan decisiones "... *frente a peticiones, quejas, reclamos y recursos de los usuarios de los servicios..* ", situación que no es la suya porque ni siquiera tiene la calidad de suscriptor o usuario de los servicios provistos por VIRGIN MOBILE.

De otro lado la recientemente expedida ley 1712 de 2014 o Ley de Transparencia y del Derecho de Acceso a la Información Pública y su revisión constitucional realizada a través de Sentencia C-274 de 2013, adoptan la postura doctrinaria y jurisprudencial señalada anteriormente y señalan claramente que el acceso a este tipo de información por pertenecer al ámbito propio, particular y privado de VIRGIN MOBILE COLOMBIA SAS, puede ser negada.

---

1 *"...no se pueda confundir el ejercicio de función públicas, con la prestación de servicios públicos, supuestos a los que alude de manera separada el artículo 150 numeral 23 de la Constitución que asigna al Legislador competencia para expedir las leyes llamadas a regir una y otra materia"* (Sentencia Corte Constitucional C-037 de 2003). De otro lado *"...La prestación de los servicios públicos no constituye una función pública y solamente algunas de las actividades que se llevan a cabo durante su desarrollo pueden llegar a ser calificadas de tales...*, esto es p.e. *"... cuando ejercen su posición de dominio frente al usuario y cuando se ejercen facultades especiales para la prestación de los servicios, como cuando se aplican políticas de contribuciones y subsidios..." (Consejo de Estado, Sentencia del 17 de febrero de 2005. M.P. Alier Hernández)*

2 En ese sentido, véanse las posturas doctrinales de Carlos Alberto Atehortúa Rios. **Régimen Legal de los Servicios Públicos domiciliarios** y **Servicios Públicos: Proveedores y Régimen de controles** y Alberto Montaña Plata. **El concepto de Servicio Público en el derecho Administrativo** y la jurisprudencia del Consejo de Estado, Sección Tercera, Sentencia de diecisiete (17) de febrero de dos mil cinco (2005). Actor: RODRIGO VILLAMIL VIRGÜEZ Demandado: NACION - MINISTERIO DE COMUNICACIONES Y OTROS.

Por las razones anotadas y además por constituir un secreto comercial debidamente protegido por la ley colombiana y la normatividad andina, VIRGIN MOBILE SAS no puede suministrarle la información solicitada.

Señor Copete, dentro de los siguientes diez (10) días hábiles contados a partir de que usted tenga conocimiento de esta decisión, si lo elige, usted puede presentar recurso de reposición y en subsidio de apelación. Lo anterior, significa que usted puede presentar nuevamente una comunicación mediante la cual manifieste su inconformidad con la presente decisión, en los casos en que la misma le sea desfavorable total o parcialmente, con el fin de que volvamos a revisar su caso particular.

Igualmente, si así lo quiere, en el mismo momento que presente la comunicación antes mencionada, puede expresar su interés de que su caso sea revisado y resuelto de fondo por la autoridad de vigilancia y control, es decir, por la Superintendencia de Industria y Comercio –SIC-, en el evento en que la decisión frente a su petición o queja sea confirmada o modificada y nuevamente le sea desfavorable.

Tenga en cuenta, que la comunicación referida, puede presentarla en forma verbal o escrita, a través de nuestra página web, nuestra página de red social o a través de nuestra línea gratuita de atención al usuario.

Es un gusto poder brindarle nuestros servicios y asesoría cada vez que los necesite. Lo invitamos a contactarnos a través de nuestra línea gratuita de atención 01 8000 937171 opción 1, línea fija en Bogotá D.C. 5931060 o desde el celular marcando al *111

Cordialmente,

Proyectado por: Elkin Rico

Erika Quiroz Duarte
Supervisora de Servicio al Cliente
Virgin Mobile Colombia

www.virginmobile.co

Carrera 15 No. 93 a - 84, piso 5. Bogotá, Colombia.
Teléfono: 636 5143

Anexo 10. Respuesta CLARO.

18/4/2014 Correo de Universidad Nacional Abierta y a Distancia - UNAD - Derecho de petición Solicitud respetuosa de información

Cordial Saludo,

Le informamos que Claro ha recibido su solicitud y en este momento está siendo atendida por el área correspondiente.

En caso de respuesta a este correo por favor responder a cliente.co@claro.com.co, solo allí serán atendidas sus solicitudes.

Gracias por haberse puesto en contacto con Claro Soluciones Fijas. Recuerde que ahora usted decide de qué quiere llenar su empresa y eso es CLARO.

Cordialmente,

Ingeniero de Soporte Técnico

Michell Cristina Bautista

Telmex Colombia S. A.
Mi nuevo correo electrónico es:
cliente.co@claro.com.co

Para mayor información comuníquese a los siguientes teléfonos en Bogotá +57(1) 7480456, Cali +57(2) 4882456, Medellín +57(4) 6044456, Barranquilla +57(5) 3870456 y resto del país 01 8000 186456 o a través del correo cliente.co@claro.com.co

Anexo 11. Respuesta Grupo De Investigación en Desarrollo Aplicaciones Móviles de la Universidad de Magdalena.

Wilmar Liberto Copete Marin <wilmar.copete@unad.edu.co>

Derecho de petición

Grupo de Inv en Desarrollo Electronico y Aplicaciones Moviles <gideam@unimagdalena.edu.co> 22 de octubre de 2014, 11:21
Para: Wilmar Liberto Copete Marin <wilmar.copete@unad.edu.co>
Cc: Luis Leonardo Camargo Ariza <lcamargoa@unimagdalena.edu.co>, Jorge Gomez Rojas <jgomez@unimagdalena.edu.co>

Buenos días.

Apreciado Prof. Copete Marin, es para nosotros un gusto atender sus requerimientos y solicitudes. En primera instancia nos disculpamos por la demora en la respuesta pero es debida a que en nuestras líneas de investigación no está la seguridad informática en forma explicita. Sin embargo durante este tiempo compartimos algunos comentarios de su solicitud que poseemos. La información adicional es posible obtenerla a través del Ministerio de las TIC quién posee una base de datos robusta de este tipo de información.

La seguridad informática, es el área que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta, incluyendo la información obtenida. Luego, su finalidad es asegurar que los recursos del sistema de información de una organización sean empleados de forma correcta, de acuerdo a las políticas establecidas, y que el acceso a la información, así como su modificación, sólo le sea permitida a las personas capacitadas y autorizadas.

En la actualidad la seguridad informática se ha visto muy comprometida debido a la gran cantidad de robos de información a usuarios que no tienen un sitio definido para ingresar a sus correos electrónicos, o redes sociales, y demás páginas informáticas que requieran de un usuario y contraseña, según una encuesta realizada por el Ministerio de Tecnologías de la Información y las Comunicaciones el 71% de los colombianos accede a Internet desde su casa y el 20% en cafés Internet.

El robo de la información informática compromete en gran parte a la suplantación de identidad, uso de la información robada con fines de devastar la integridad de la persona, hurtar sus bienes cibernéticos como lo es una cuenta bancaria, publicar comentarios ofensivos en páginas sociales tales como Facebook, Twitter para arruinar su reputación o crear conflictos con sus allegados. Todo esto es debido a que los usuarios están obligados a digitar sus datos de ingreso a dichas páginas.

La legislación colombiana comenzó a prestar más importancia a la violación de la seguridad informática ya que esta ha ido en aumento durante los últimos años; a conocer las leyes que rigen el tema de hurto informático:
2.2.1 Ley 599 De 2000
Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
2.2.1.1 Artículo 269: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
2.2.1.2 Artículo 269 A: acceso abusivo a un sistema informático sin autorización.
2.2.1.3 Articulo 269 B: obstaculización ilegitima de sistema informático o red de telecomunicaciones sin estar facultado.
2.2.1.4 Articulo 269 C: interceptación de datos informáticos sin orden judicial.
2.2.1.5 Articulo 269 D: daño informático sin estar facultado para ello.

2.2.1.6 Artículo 269 E: uso de software malicioso sin estar facultado para ello.
2.2.1.7 Articulo 269 F: violación de datos personales sin estar facultado para ello.
2.2.1.8 Articulo 269 G: suplantación de sitios web para capturar datos personales sin estar facultado para ello.
2.2.1.9 Articulo 269 H: las penas imponibles se aumentaran de la mitad a las tres cuartas partes.
2.2.1.10 Articulo 269 I: hurto por medio informático.
2.2.1.11 Artículo 197: utilización ilícita de redes de comunicaciones. Artículo modificado por el artículo 8 de la Ley 1453 de 2011. El nuevo texto es el siguiente: El que con fines ilícitos posea o haga uso de equipos terminales de redes de comunicaciones o de cualquier medio electrónico diseñado o adaptado para emitir o recibir señales, incurrirá, por esta sola conducta, en prisión de cuatro (4) a ocho (8) años.

Esperamos que sea de su interés y ayuda la información con la que contamos para su proyecto. Adicionalmente colocamos a su disposición el contacto de los expertos con los que cuenta el grupo de investigación para que pueda solventar cualquier duda adicional y así ud pueda acordar con ellos una asesoría.

LUIS LEONARDO CAMARGO ARIZA
lcamargoa@unimagdalena.edu.co

JORGE GOMEZ ROJAS
jgomez@unimagdalena.edu.co

Le saluda cordialmente,

GRUPO DE INVESTIGACIÓN EN DESARROLLO ELECTRÓNICO Y APLICACIONES MÓVILES

Reconocido y categorizado C ante COLCIENCIAS
Programa de Ingeniería Electrónica | Facultad de Ingeniería | Universidad del Magdalena
GIDEAM@unimagdalena.edu.co
Teléfono: +57 5 4217940 Ext.292 Dirección: Carrera 32 No 22 - 08 Santa Marta D.T.C.H. - Magdalena | Código Postal 470004

Anexo 12. Respuesta Grupo de Investigación en Comercio Electrónico, Telecomunicaciones E Informática- Gecti. Universidad de Los Andes

Wilmar Liberto Copete Marin <wilmar.copete@unad.edu.co>

Derecho de petición

Nelson Remolina Angarita <nremolin@uniandes.edu.co> 22 de septiembre de 2014, 14:52
Para: Wilmar Liberto Copete Marin <wilmar.copete@unad.edu.co>

Muchas gracias por su email.

No hemos realizado investigaciones sobre los temas mencionados por usted.

Le sugerimos contactar la comisión de regulación de comunicaciones y el Ministerio de TIC con miras a indagar si ellos tienen los datos e información que Ud requiere.

Cordialmente,

Nelson Remolina

Anexo 13. Respuesta Grupo de Investigación de Informática y Telecomunicaciones- Universidad Ecesi.

UNAD
Universidad Nacional Abierta y a Distancia

Wilmar Liberto Copete Marin <wilmar.copete@unad.edu.co>

Derecho de petición

Andres Navarro Cadavid <anavarro@icesi.edu.co> 22 de septiembre de 2014, 14:41
Para: Wilmar Liberto Copete Marin <wilmar.copete@unad.edu.co>

Cordial saludo,

NO disponemos de la información que usted requiere.

Cordialmente

Andres Navarro Cadavid Ph.D.

Director grupo de Investigación i2T

Departamento TIC

Universidad Icesi

Cali - Colombia

Tel. (57) 2 555 2334 - Móvil: (57) 300 6775409

Anexo 14. Respuesta 4GAméricas.

Wilmar Liberto Copete Marin <wilmar.copete@unad.edu.co>

Derecho de petición Solicitud respetuosa de información.

Jose Otero <jose.otero@4gamericas.org> 8 de abril de 2015, 20:34
Para: Wilmar Liberto Copete Marin <wilmar.copete@unad.edu.co>

Estimado Wilmar,

Gracias por su interés en recibir información de 4G Americas. Desafortunadamente el tipo de datos que solicita excede el alcance de 4G Americas. De todas formas, lo invito a revisar todo los documentos que hemos publicado sobre tecnologías inalámbricas en los pasados años en la siguiente dirección:
http://www.4gamericas.org/en/resources/white-papers/

Presentaciones de 4G Americas las puede encontrar en la siguiente dirección:
http://www.4gamericas.org/en/resources/presentations/

Asimismo, le recomiendo las siguientes páginas que considero podrían ser de utilidad para su investigación:

- http://www.informationweek.com/whitepaper/Security/Encryption
- http://www.sophos.com/en-us/products/your-needs/industry-case-studies/government/uk.aspx

Por último, sugiero que consulte documentos de la UIT y CITEL sobre el tema de seguridad en redes móviles donde seguramente podrá encontrar las presentaciones que han dado los delegados de Colombia a los foros de discusión organizados por esas entidades.

Si puedo asistirlo en temas relacionados al alcance de 4G Americas en el futuro, no dude en contactarme a la brevedad.

Cordialmente,

Jose F. Otero

Director América Latina & Caribe

4G Americas