CONTRATO INTERADMINISTRATIVO 301 DE 2010

Ministerio de Tecnologías de la Información y las Comunicaciones
República de Colombia

ESTUDIO DE VULNERABILIDAD Y RIESGO DE LAS REDES E INFRAESTRUCTURA DE TELECOMUNICACIONES EN ZONAS VULNERABLES EXPUESTAS A EVENTOS NATURALES DESASTROSOS

INFORME FINAL

Versión 2.0

Diciembre de 2010

Centro de Investigación de las Telecomunicaciones CINTEL
Avenida Calle 100No. 19 - 61 Piso 8º, Tel: 6353538 Fax: 6353338
Bogotá D.C.

CONTENIDO

ABSTRACT 1

1 RESUMEN EJECUTIVO 2

2 PRESENTACIÓN 8

2.1 ASPECTOS GENERALES 12

2.2 EL ENTORNO GEOGRÁFICO NACIONAL Y LOS DESASTRES NATURALES 13

2.2.1 Fenómenos Hidrometeorológicos 16

2.2.2 Fenómenos Geológicos 18

2.2.3 Fenómenos Volcánicos 18

2.2.4 Vulnerabilidad Y Riesgo 19

2.3 NORMAS, PLANES Y DOCUMENTOS SOBRE TELECOMUNICACIONES EN EMERGENCIAS 24

2.3.1 La Ley 46 De 1988 25

2.3.2 El Decreto Ley 919 de 1989 25

2.3.3 El Decreto 93 de 1998 26

2.3.4 EL CONPES 3146 DE 2001 28

2.3.5 La Ley 1341 de 2009 31

2.4 ASPECTOS SOBRE LA IMPORTANCIA DEL ESTUDIO 32

3 MODELO DE VULNERABILIDAD Y RIESGOS 35

3.1 Definición y aspectos generales del modelo seleccionado 36

3.2 Definición de niveles de adversidad al riesgo 44

3.3 Definición de umbrales de tolerancia 46

3.4 Definición del universo de riesgos..... 50

3.5 Identificación de riesgos modelo 55

3.6 Calificación de Amenazas por Vulnerabilidades y su priorización..... 57

3.7 Escenarios basados en escenarios hipotéticos 59

3.8 Tablas de riesgo 60

3.9 Definición de los criterios de impacto vs relevancia de impacto 63

3.10 Descripción del modelo ajustado..... 64

3.11 Descripción de la usabilidad del modelo y guías de uso 65

4 DIAGNÓSTICO DE AMENAZAS NATURALES..... 69

4.1 GENERALIDADES 71

4.1.1 DEFINICIONES DE AMENAZA NATURAL 71

4.1.2 Definiciones de amenaza, riesgo, vulnerabilidad y exposición..... 78

4.1.3 Delimitación general de la zona de estudio 79

4.2 DIAGNÓSTICO DE AMENAZA SÍSMICA: QUINDÍO, ARMENIA 82

4.2.1 Delimitación de la zona de estudio 82

4.2.2 Caracterización de la zona de estudio por amenaza sísmica..... 85

4.2.3 Generalidades de las condiciones socio económicas y políticas 87

4.2.4 Valoración de la amenaza sísmica 90

4.2.5 Priorización de la amenaza sísmica 96

4.3 DIAGNÓSTICO DE AMENAZA VOLCÁNICA: TOLIMA, CAJAMARCA 98

4.3.1 Delimitación de la zona de estudio 98

4.3.2 Caracterización de la zona por amenaza volcánica 101

4.3.3 Generalidades de las condiciones socio económicas y políticas 103

4.3.4 Valoración de la amenaza volcánica 105

4.3.5 Priorización y zonificación de la amenaza volcánica 106

4.4 DIAGNÓSTICO DE AMENAZA POR TSUNAMI: NARIÑO, TUMACO 109

4.4.1 Delimitación de la zona de estudio 109

4.4.2 Generalidades de las condiciones socio económicas y políticas 111

4.4.3 Valoración de la amenaza por Tsunami 112

4.4.4 Priorización y zonificación de la amenaza por tsunami 114

4.5 DIAGNÓSTICO DE AMENAZA POR INUNDACIÓN: SUCRE, LA MOJANA 117

4.5.1 Delimitación de la zona de estudio 117

4.5.2 Valoración de la amenaza por inundación 118

4.5.3 Priorización y zonificación de la amenaza por inundación 120

5 DIAGNÓSTICO DE VULNERABILIDAD DE REDES BÁSICAS DE TELECOMUNICACIONES 125

5.1 REDES Y SERVICIOS VITALES DE TELECOMUNICACIONES 127

5.1.1 Determinación de las redes y servicios vitales de telecomunicaciones 127

5.1.2 Descripción, topología general de los servicios vitales de telecomunicaciones y sus elementos básicos 140

5.2 VULNERABILIDAD DE LAS REDES VITALES DE TELECOMUNICACIONES 189

5.3 VULNERABILIDAD FÍSICA DE LOS ELEMENTOS DE LAS REDES VITALES DE TELECOMUNICACIONES 199

5.3.1 Edificaciones 199

5.3.2 Torres - Antenas 219

5.3.3 Armarios, Gabinetes y Shelters 236

5.3.4 Redes Aéreas de fibra óptica y de cobre 241

5.3.5 Redes Subterráneas de fibra óptica y de cobre 251

5.3.6 Posibles daños de las redes subterráneas de fibra óptica y cobre 253

5.3.7 Estimativos de vulnerabilidad física de los diferentes elementos de las redes de telecomunicaciones según tipo de amenaza 254

5.4 VULNERABILIDAD FUNCIONAL DE LOS SERVICIOS DE TELECOMUNICACIONES VITALES 257

5.4.1 Servicio Portador 260

5.4.2 Servicio de Telefonía Pública Básica Conmutada e INTERNET fijo xDSL 267

5.4.3 Servicio de Telefonía móvil celular (GSM & UMTS) e INTERNET móvil 278

5.4.4 Servicio de Radiodifusión sonora AM & FM 285

5.4.5 Servicio de Televisión Radiodifundida 290

5.4.6 Servicio de televisión por cable 295

5.4.7 Servicio de Móvil Marítimo 299

5.4.8 Servicio de Móvil Aeronáutico 306

5.4.9 Servicio de radioaficionados 313

5.4.10 COMPARTEL 315

5.4.11 Redes de comunicaciones de emergencia 319

5.4.12 Redes de Telemetría 322

6 APLICACIÓN DEL MODELO EN LAS ZONAS Y PARA LAS AMENAZAS DEFINIDAS 328

6.1 EVENTO ANALIZADO: SISMO 331

6.1.1 Generalidades caso de estudio 331

6.1.2 Infraestructura de Telecomunicaciones en Riesgo 331

6.2 EVENTO ANALIZADO: VOLCÁN MACHÍN 337

6.2.1 Generalidades caso de estudio 337

6.2.2 Infraestructura de Telecomunicaciones en Riesgo 337

6.3 EVENTO ANALIZADO: TSUNAMI 344

6.3.1 Generalidades caso de estudio 344

6.3.2 Infraestructura de Telecomunicaciones en Riesgo 344

6.4 EVENTO ANALIZADO: INUNDACIÓN 349

6.4.1 Generalidades caso de estudio 349

6.4.2 Infraestructura de Telecomunicaciones en Riesgo 350

7 CONCLUSIONES Y RECOMENDACIONES PARA LA PROTECCIÓN DE LA INFRAESTRUCTURA, MEDIDAS DE MITIGACIÓN Y BUENAS PRÁCTICAS 355

7.1 MEDIDAS DE MITIGACIÓN 357

7.2 BUENAS PRÁCTICAS 362

7.2.1 Buenas prácticas en Estados Unidos de Norteamérica 362

7.2.2 Buenas prácticas en la Unión Europea 366

8 ANEXO 1 INFORMACIÓN SOLICITADA A OPERADORES ... 368

9 ANEXO 2 MEJORES PRACTICAS ESTADOS UNIDOS DE NORTEAMERICA 375

10 ANEXO 3 MEJORES PRACTICAS VOLUNTARIAS EUROPEAS 384

11 REFERENCIAS 392

TABLA DE TABLAS

Tabla 1. Análisis de la Amenaza 89

Tabla 2. Determinación de los Valores de Amenaza. 91

Tabla 3. Valores intensidades en Armenia 93

Tabla 4. Comparación de las Escalas de Mercalli y Richter 93

Tabla 5. Tabla de valores hipotéticos de probabilidad de ocurrencia de un sismo en la zona de estudio. 95

Tabla 6. Tabla de resultados ejemplo de la calificación de la amenaza sísmica para un servicio específico 97

Tabla 7 Tabla de valoración de la vulnerabilidad y el riesgo por volcán 105

Tabla 8. Tabla de resultados ejemplo de la calificación de la amenaza volcánica para un servicio específico 106

Tabla 9 Tabla de resultados ejemplo de la priorización de la amenaza volcánica para un servicio específico 107

Tabla 10 Tabla de valoración de la vulnerabilidad y el riesgo por tsunami 115

Tabla 11 Tabla de resultados ejemplo de la priorización de la amenaza por Tsunami para un servicio específico 115

Tabla 12. Tabla de resultados ejemplo de la calificación de la amenaza por inundación para un servicio específico 119

Tabla 13 Tabla de valoración de la vulnerabilidad y el riesgo por inundación 121

Tabla 14 Tabla de resultados ejemplo de la priorización de la amenaza por inundación para un servicio específico 122

Tabla 15 Evolución de la penetración de TPBCL, celular y acceso a internet 128

Tabla 16 Redes vitales consideradas para el estudio 132

Tabla 17 Familias xDSL 163

Tabla 18Elementos de Red GPRS 167

Tabla 19 Bandas de frecuencia atribuidas al servicio de Móvil Marítimo 178

Tabla 20 Bandas de frecuencia atribuidas al servicio de Móvil Aeronáutico 181

Tabla 21 Bandas atribuidas a Radioaficionados 183

Tabla 22Valoración de las principales vulnerabilidades intrínsecas en redes de Telecomunicaciones en Europa 191

Tabla 23 Vulnerabilidades de redes de Telecomunicaciones ante amenazas naturales consideradas en el presente estudio 193

Tabla 24 Principales causas para que las Telecomunicaciones fallen ante situaciones de desastre 194

Tabla 25. Elementos básicos del sistema de telecomunicaciones 196

Tabla 26 Tipos de edificaciones 200

Tabla 27 Eventos sísmicos – Posible daños a edificaciones 208

Tabla 28 Volcán – Nube de Cenizas – Posibles daños a edificaciones- Proyecto AELG-19 210

Tabla 29 Volcán – Nube de Cenizas - Posible daños a edificaciones 211

Tabla 30 Volcán – Flujos de lava, material piroclástico y lodos - Posible daños a edificaciones 211

Tabla 31 Volcán – Caída de material piroclástico y proyectiles - Posible daños a edificaciones 212

Tabla 32 Tsunami – Golpes de Ola y Fuerzas laterales provenientes de corrientes de agua y material arrastrado y licuación del terreno - Posible daños a edificaciones 213

Tabla 33 Tsunami – Inundación de agua salobre - Posible daños a edificaciones 213

Tabla 34 Inundaciones – Posible daños a edificaciones 215

Tabla 35 Eventos sísmicos – Posibles daños a equipos de telecomunicaciones dentro de edificaciones 216

Tabla 36 Volcán – Nube de Cenizas – Posible afectación a equipo de telecomunicaciones - Proyecto AELG-19 217

Tabla 37 Volcanes – Posibles daños a equipos de telecomunicaciones dentro de edificaciones 218

Tabla 38 Tsunami – Posibles daños a equipos de telecomunicaciones dentro de edificaciones 218

Tabla 39 Inundaciones – Posibles daños a equipos de telecomunicaciones dentro de edificaciones 219

Tabla 40 Eventos sísmicos – Posibles daños a Torres 225

Tabla 41 Eventos sísmicos – Posibles daños a Antenas 225

Tabla 42 Volcán – Nube de Cenizas – Posible afectación de torres, mástiles, redes aéreas y antenas - Proyecto AELG-19 226

Tabla 43 Volcanes – Posibles daños a Torres 226

Tabla 44 Volcanes – Posibles daños a Antenas 227

Tabla 45 Tsunami – Posibles daños a Torres 227

Tabla 46 Tsunami – Posibles daños a Antenas 227

Tabla 47 Inundaciones de agua dulce – Posibles daños a torres y antenas 227

Tabla 48 Volcán – Nube de Cenizas – Posible afectación a sistemas de telecomunicaciones por polución del espectro radioeléctrico - Proyecto AELG-19 232

Tabla 49 Volcán – Nube de Cenizas – Posible afectación a sistemas de telecomunicaciones por polución del espectro radioeléctrico 235

Tabla 50 Eventos sísmicos – Posibles daños a armarios, gabinetes y shelters 239

Tabla 51 Volcán – Nube de Cenizas – Posible afectación de armarios, gabinetes y shelters - Proyecto AELG-19 239

Tabla 52 Volcanes – Posibles daños a armarios, gabinetes y shelters 240

Tabla 53 Tsunami – Posibles daños a armarios, gabinetes y shelters 240

Tabla 54 Inundaciones de agua dulce – Posibles daños a armarios, gabinetes & shelters 240

Tabla 55 Eventos sísmicos – Posibles daños a torres de transmisión eléctrica soporte de redes aéreas de telecomunicaciones 246

Tabla 56 Eventos sísmicos – Posibles daños a postes soporte de redes aéreas de telecomunicaciones 246

Tabla 57 Eventos sísmicos – Posibles daños a redes aéreas de fibra óptica, coaxial y cobre 247

Tabla 58 Volcán – Nube de Cenizas – Posible afectación de torres eléctricas y postes - Proyecto AELG-19 248

Tabla 59 Volcanes – Posibles daños a torres eléctricas soporte de redes aéreas de telecomunicaciones 248

Tabla 60 Volcanes – Posibles daños a postes soporte de redes aéreas de telecomunicaciones 249

Tabla 61 Volcanes – Posibles daños a redes aéreas de fibra óptica, coaxial y cobre 249

Tabla 62 Tsunami – Posibles daños a torres eléctricas soporte de redes aéreas de telecomunicaciones 249

Tabla 63 Tsunami – Posibles daños a postes soporte de redes aéreas de telecomunicaciones 250

Tabla 64 Tsunami – Posibles daños a redes aéreas de fibra óptica, coaxial y cobre 250

Tabla 65 Inundaciones de agua dulce – Posibles daños a torres, postes y redes aéreas de fibra óptica, coaxial y cobre 250

Tabla 66 Eventos sísmicos – Posibles daños a redes subterráneas de fibra óptica y cobre 253

Tabla 67 Volcán – Posibles daños a redes subterráneas de fibra óptica y cobre 253

Tabla 68 Tsunami – Posibles daños a redes subterráneas de fibra óptica y cobre 254

Tabla 69 Inundaciones de agua dulce – Posibles daños a redes subterráneas de fibra óptica y cobre 254

Tabla 70 Vulnerabilidad física de redes de telecomunicaciones ante amenazas sísmicas . 255

Tabla 71 Vulnerabilidad física de redes de telecomunicaciones ante amenazas volcánicas 255

Tabla 72 Vulnerabilidad física de redes de telecomunicaciones ante amenaza de tsunami 256

Tabla 73 Vulnerabilidad física de redes de telecomunicaciones ante amenaza de inundación 256

Tabla 74. Elementos de Infraestructura en riesgo por amenaza de sismo. 331

Tabla 75. Zona de Influencia del estudio para volcán 337

Tabla 76. Elementos de Infraestructura en riesgo por amenaza de volcán. 337

Tabla 77. Elementos de Infraestructura en riesgo por amenaza de tsunami. 344

Tabla 78. Municipio de la zona de estudio de inundación. 349

Tabla 79. Elementos de Infraestructura en riesgo por amenaza de inundación 350

Tabla 80 Evaluación de las buenas prácticas por la industria americana de telecomunicaciones 363

Tabla 81 Información de redes vitales de telecomunicaciones para la elaboración del modelo de vulnerabilidad 370

TABLA DE FIGURAS

Figura 1. Mapa Oficial de la República de Colombia 14

Figura 2. Modelo de datos Cartografía 1:500.000 47

Figura 3. Modelo de datos CINTEL 48

Figura 4. Tipos de volcanes 74

Figura 5 Velocidad y altura de un Tsunami 76

Figura 6 Modelo de propagación de un tsunami en el Pacífico sudeste, nueve horas después de su generación 77

Figura 7 Mapa Físico de Colombia 80

Figura 8 Ubicación general de la zona de estudio 81

Figura 9 Mapa General de Amenaza Sísmica Departamento de Quindío. 83

Figura 10 Mapa de municipios afectados 83

Figura 11. Microzonificación Sísmica de Armenia 84

Figura 12. Mapa de Intensidades. Armenia 84

Figura 13. Mapa de Daños. Armenia 85

Figura 14 Ecoregión del Eje Cafetero. Mapa sintético de fallas activas y probablemente activas 87

Figura 15 Participación de la población urbana y rural en Armenia 1938-2005 88

Figura 16 Ocurrencia de Sismos en la Zona: 96

Figura 17 Mapa de Amenaza Sísmica sobre la Infraestructura 97

Figura 18 Área de cubrimiento total de la influencia del Volcán Machín 98

Figura 19 Población directamente afectada: Cajamarca 100

Figura 20 Población directamente afectada 3d: Cajamarca 101

Figura 21 Mapa de Amenaza Volcánica sobre la Infraestructura 108

Figura 22 Zona de estudio la amenaza por tsunami 109

Figura 23 Curvas de Nivel del Municipio de Tumaco. 110

Figura 24 Delimitación preliminar de amenaza por Tsunami 111

Figura 25 Zonas de Inundación en Tumaco 112

Figura 26 Mapa de Amenaza por Tsunami sobre la Infraestructura 116

Figura 27 Mapa de Zonificación de amenaza por inundación preliminar 117

Figura 28. Régimen de lluvias en el Caribe Continental 119

Figura 29 Mapa de Amenaza por Inundación sobre la Infraestructura. Municipio de San Marcos 123

Figura 30 Mapa de Amenaza por Inundación sobre la Infraestructura. La Mojana 124

Figura 31 Evolución de la penetración de TPBCL, celular y acceso a internet 130

Figura 32 Audiencia de medios (%) 131

Figura 33 TIC Línea Vital en la Sociedad Moderna 133

Figura 34 TIC en la Administración de Desastres 136

Figura 35 Sectores, productos y servicios críticos en Holanda 137

Figura 36 Vitalidad directa e indirecta - Holanda 139

Figura 37Contribución y dependencia - Holanda 140

Figura 38 Topología servicio Portador 142

Figura 39 Redes de servicio Portador en Colombia 143

Figura40 Elementos básicos de la red de TPBCL 146

Figura 41. Arquitectura de Redes de Nueva Generación 149

Figura 42 Comunicaciones Móviles (Celular, PCS, Trunking, Wi MAX) - Bandas de frecuencia atribuidas 151

Figura 43 Subsistemas del sistema GSM 152

Figura 44 Arquitectura básica del sistema GSM 153

Figura 45. Componentes del Subsistema BSS. 155

Figura 46 Componentes e interfaces del Subsistema NSS de GSM (dominio CS) 157

Figura 47 Arquitectura de Red BICC 160

Figura 48 Arquitectura de Red 3GPP R4 160

Figura 49 Alcance y velocidad de transmisión de datos en los sistemas XDSL (para un sólo par sin regenerador/amplificador) 164

Figura 50. Interfaces GPRS 168

Figura 51Arquitectura UMTS 170

Figura 52 Topología general de red de los servicios de radiodifusión sonora A.M. y F.M.... 172

Figura 53 Bandas atribuidas al servicio de televisión radiodifundida 173

Figura 54 Topología general de red de los servicios de televisión radiodifundida 174

Figura 55 Topología general de red de los servicios de televisión por cable 175

Figura 56 Servicio Móvil Marítimo - Topología general de red 178

Figura 57 Servicio Móvil Aeronáutico - Topología general de red 181

Figura 58 Estaciones de radioaficionado 184

Figura 59 COMPARTEL - Topología general de red 185

Figura 60 Redes de emergencia – Topología general de red 186

Figura 61 Redes de Telemetría - Topología general de red..... 188

Figura 62 Ceniza Volcánica 209

Figura 63Volcán Eyjafjallajökull - Nube de Cenizas 233

Figura 64 Esquema de red agregado del servicio portador..... 265

Figura 65 Esquema funcional general del servicio portador..... 266

Figura 66 Esquema de red agregado del servicio de TPBCL e INTERNET fijo xDSL..... 276

Figura 67 Esquema funcional general del servicio portador de TPBCL e INTERNET fijo xDSL 277

Figura 68 Esquema de red agregado del servicio de telefonía móvil celular e INTERNET móvil. 283

Figura 69 Esquema funcional general del servicio Telefonía móvil celular (GSM & UMTS) e INTERNET móvil 284

Figura 70 Esquema de red agregado del servicio de radiodifusión sonora AM & FM. 288

Figura 71 Esquema funcional general del servicio de radiodifusión sonora AM & FM 289

Figura 72 Esquema de red agregado del servicio de televisión radiodifundida. 293

Figura 73 Esquema funcional general del servicio de televisión radiodifundida 294

Figura 74 Esquema de red agregado del servicio de televisión por cable. 297

Figura 75 Esquema funcional general del servicio de televisión por cable 298

Figura 76 Esquema de red agregado del servicio de móvil marítimo 304

Figura 77 Esquema funcional general del servicio de móvil marítimo..... 305

Figura 78 Esquema de red agregado del servicio de móvil aeronáutico..... 311

Figura 79 Esquema funcional general del servicio de móvil aeronáutico..... 312

Figura 80 Esquema de red agregado del servicio de radioaficionados..... 314

Figura 81 Esquema funcional general del servicio de móvil aeronáutico..... 314

Figura 82 Esquema de red agregado de COMPARTEL..... 317

Figura 83 Esquema funcional general de COMPARTEL..... 318

Figura 84 Esquema de red agregado de las redes de emergencia 322

Figura 85 Esquema funcional general de las redes de emergencia..... 322

Figura 86 Esquema de red agregado de TELEMETRÍA 326

Figura 87 Esquema funcional general de las redes de telemetría 327

ESTUDIO DE VULNERABILIDAD Y RIESGO DE LAS REDES E INFRAESTRUCTURA DE TELECOMUNICACIONES EN ZONAS VULNERABLES EXPUESTAS A EVENTOS NATURALES DESASTROSOS

Abstract

Las telecomunicaciones en el mundo moderno se han convertido en parte esencial de la vida cotidiana, requiriéndose en un número cada vez mayor de actividades, desde las mismas labores personales, del hogar, de oficina, hasta en las operaciones de defensa y seguridad nacional, como en la prestación de importantes servicios públicos de telecomunicaciones nacionales e internacionales, en aplicaciones comerciales e industriales, en las diversas radiocomunicaciones aeronáuticas, marítimas y terrestres, y de las mismas comunicaciones de las entidades del Estado y del Gobierno. Los servicios de telefonía tanto fija como móvil, el internet, las aplicaciones de banda ancha, las radiocomunicaciones privadas y corporativas, la radio y la televisión, etc., son una muy buena prueba de ello.

Por su importancia, el papel transcendental que desempeñan las telecomunicaciones en las situaciones de catástrofe ha sido reconocido en numerosos documentos internacionales, declaraciones, convenios, y tratados, que comprometen a los Estados al aporte y desarrollo de las telecomunicaciones en situaciones de socorro, desastres y catástrofes. Igualmente, a nivel nacional, así como en diversas normas, decretos y resoluciones, es reconocida la importancia de las telecomunicaciones y su aporte en las situaciones de emergencia y desastre. Tanto así que se insta, se estimula y obliga a que éstas se encuentren siempre disponibles al público y a las autoridades y para que sirvan también como soporte a otros sectores, así como para el ejercicio de actividades de socorro y seguridad pública.
Pero las telecomunicaciones, como infraestructura, son igualmente vulnerables a los embates de los fenómenos de la naturaleza y las redes pueden quedar colapsadas, interrumpidas o inutilizadas en las catástrofes naturales, generando otra emergencia adicional a la misma catástrofe natural.
Este estudio se elaboró con el fin de dar cumplimiento a las normas nacionales, estimular el conocimiento sobre riesgos de origen natural y antrópico, incentivar programas para la incorporación de la prevención y reducción de riesgos en la planificación, orientar las acciones del Sector de Telecomunicaciones en relación con los métodos de análisis de la vulnerabilidad, evaluación de amenazas y riesgos, orientar las acciones del Sector de Telecomunicaciones para apoyo al Sistema Nacional para la Prevención y Atención de Desastres SNPAD, fomentar el aporte de las telecomunicaciones en situaciones de emergencias y desastres e impulsar el fortalecimiento de las redes de telecomunicaciones para resistir los impactos de los fenómenos adversos de la naturaleza y mitigar los efectos de un posible evento desastroso.
El "estudio de vulnerabilidad y riesgo de las redes e infraestructura de telecomunicaciones en zonas vulnerables expuestas a eventos naturales desastrosos" servirá principalmente como modelo general para orientar las acciones del Sector de Telecomunicaciones en relación con los métodos de análisis de vulnerabilidad y evaluación de amenazas y riesgos, para la protección de la infraestructura.
El Ministerio de Tecnologías de la Información y las Comunicaciones, como organismo rector de las telecomunicaciones en Colombia y como coordinador responsable del sector de las comunicaciones ante el SNPAD, tiene el compromiso de fomentar el fortalecimiento de las redes de telecomunicaciones, con el fin de auto-soportarse, en situaciones de emergencias y desastres y mitigar los efectos de un posible evento desastroso, y como apoyo al SNPAD así como a la población vulnerable.

Como resultado del estudio se concluye de manera general que todos los operadores deben aplicar políticas asociadas a una gestión integrada del riesgo enfocándose en planes de mitigación y contingencia de aquellos elementos de red que están bajo amenaza natural y que son altamente vulnerables a esta amenaza.
Una gestión integrada del riesgo permitirá establecer planes de acción en el corto y mediano plazo orientados a disminuir la vulnerabilidad de las redes y servicios vitales de telecomunicaciones con el fin de garantizar la continuidad del servicio en situaciones de crisis. A largo plazo, propenderá por involucrar las buenas prácticas usadas en el sector en lugares como Estados Unidos y la Unión Europea.

PAGINA EN BLANCO

1 RESUMEN EJECUTIVO

En la República de Colombia, ubicada en el extremo septentrional de América del sur con un perímetro aproximado de 9.242 km, con una población proyectada por el DANE para el 2010 en 45.838.748 habitantes y con costas sobre el océano Atlántico y sobre el océano Pacífico, la población y toda la infraestructura se encuentra sometida en mayor o menor grado a diferentes tipos de amenazas, tanto de origen antrópico como natural, debido a las características geológicas y geográficas de su territorio, al cambio climático y a las condiciones sociales, económicas, culturales y políticas del país, que han determinado históricamente la ubicación de los asentamientos urbanos y su tipología constructiva.

Tomando en consideración lo anterior y que las telecomunicaciones son un servicio vital para la actual sociedad, el Ministerio de Tecnologías de la Información y las Comunicaciones, como máximo ente rector de las telecomunicaciones en Colombia y como parte del Sistema Nacional para la Prevención y Atención de Desastres (SNPAD), tomó la determinación de realizar el presente estudio con el objetivo de orientar las acciones del sector con relación a los métodos de análisis de la vulnerabilidad y evaluación de amenazas y riesgos de la infraestructura de telecomunicaciones y apoyar al Sistema Nacional para la Prevención y Atención de Desastres SNPAD. Como resultado del estudio, se pretende impulsar e incentivar:

- El aporte de las telecomunicaciones en situaciones de emergencias y desastres.
- El fortalecimiento de la infraestructura de telecomunicaciones
- La protección de redes y la continuidad de los servicios públicos.
- El desarrollo y actualización de planes de emergencia y contingencia.

El alcance definido para el presente estudio es la elaboración de un modelo de evaluación de riesgo de la infraestructura de telecomunicaciones en zonas vulnerables expuestas a eventos naturales desastrosos y su aplicación a nivel de piloto para el caso de ocurrencia de cuatro eventos naturales seleccionados:

- Volcán: Para este evento se tomó como caso de estudio el volcán Machín, que está ubicado en el municipio de Cajamarca (Coordenadas Geográficas WGS 75° 21´ 15,35" y 4° 29´0.53"), en cuya zona de influencia se encuentran ubicados 30 municipios de los departamentos de Tolima, Quindío y Valle del Cauca con una población total proyectada para el 2010 de 1'410.841 habitantes y cuyas condiciones de actividad lo presentan como una gran amenaza latente para los municipios circunvecinos.
- Tsunami: Se tomó como caso de estudio, dada su alta exposición a este fenómeno ya que forma parte del cinturón de fuego del Pacífico, la población de San Andrés de Tumaco (Coordenadas Geográficas WGS 78° 45´59.7 W y 1° 48 34,43 N), con una población total proyectada para el 2010 de 179.000 habitantes ubicada en el departamento de Nariño.
- Sismo: La ciudad de Armenia (Coordenadas Geográficas WGS 84), con una población proyectada para el 2010 de 288,880 habitantes, capital del departamento de Quindío, fue tomada como caso de estudio para este evento, ya que en esta zona se materializó el fenómeno de este tipo que ha tenido mayor impacto en la población en la historia reciente de Colombia.
- Inundación: La zona de la Mojana sucreña ubicada al sur del municipio de Sucre cuyo centro está determinado por las coordenadas geográficas WGS 74° 41´3.19"W y 8° 35´59.23N y que está conformada por 21 municipios de los departamentos de Sucre, Bolívar y Córdoba con una población aproximada proyectada para el 2010 de 764.891 habitantes, se tomó como caso de estudio de este fenómeno

dado que las condiciones geomorfológicas de la zona condicionan a que se presenten inundaciones en condiciones de pluviosidad normal.

Metodológicamente, el estudio se abordó realizando un diagnóstico de la vulnerabilidad de las redes de telecomunicaciones ante las amenazas seleccionadas, para lo cual se procedió inicialmente a identificar los servicios vitales de telecomunicaciones dentro de la perspectiva de su penetración e importancia funcional, para luego identificar la topología de red típica de estos y los elementos físicos vulnerables a las amenazas naturales tratadas. Una vez identificados estos elementos de red, se procedió al análisis de su vulnerabilidad física y funcional y de los servicios de telecomunicaciones, cuyos resultados se pusieron en conocimiento del sector con el fin de iniciar una dinámica que permitiera mediante la participación de los expertos sectoriales la cuantificación de la vulnerabilidad de los elementos de red y de los servicios conexos. Esta cuantificación deberá ser de elaboración progresiva dada su extensión y complejidad.

Por otro lado, paralelamente se realizó el diagnóstico de las amenazas naturales en los casos de estudio y zonas geográficas definidas. Con base en la información de INGEOMINAS, IDEAM, IGAC, OSSO, OCHA, DANE, FOREC entre otras, se determinaron las zonas con amenaza natural por sismo, volcán, inundación y tsunami, incluyendo probabilidades de ocurrencia por fases del evento natural, alarmas o estimados de ocurrencia.

Con los anteriores insumos se elaboró el modelo de evaluación riesgos, el cual corresponde a una gestión integrada del riesgo que incluye varias etapas desde la planeación, identificación, análisis, calificación cualitativa, priorización y categorización, terminando en recomendaciones de acciones de mitigación y contingencia, obteniendo como resultado recomendaciones

de acción. Para obtener el modelamiento de los elementos de la red afectados, el modelo se basó en el peor escenario para cada evento natural donde se cruzó la información usando un sistema de información geográfica.

El modelo fue aplicado en los casos de estudio ya mencionados, con base en la información suministrada por los prestadores de los servicios de telecomunicaciones considerados como vitales, generando resultados cualitativos y cuantitativos de los elementos de infraestructura de telecomunicaciones en riesgo.

Del análisis de vulnerabilidad física y funcional de la infraestructura de telecomunicaciones, se desprenden una serie de recomendaciones orientadas a la disminución del riesgo de la infraestructura de telecomunicaciones ante diferentes tipos de amenaza y específicamente de las tratadas en este estudio, las cuales se orientan a la disminución de la vulnerabilidad, disminuyendo la exposición a las amenazas mediante la reubicación de los elementos de infraestructura y/o aumentando su resistencia ante las amenazas que se presenten. Estas acciones deberán resultar en el fortalecimiento de la infraestructura de telecomunicaciones básica para el mantenimiento y elevación de los estándares de bienestar de la sociedad colombiana, fin último de este estudio.

PÁGINA EN BLANCO

2 PRESENTACIÓN

Dado el papel fundamental que tienen los sistemas de telecomunicaciones para el desarrollo de las diferentes labores en la sociedad y al considerar que dichos sistemas son vulnerables a los fenómenos naturales desastrosos, el Ministerio de Tecnologías de la Información y las Comunicaciones, como organismo rector de las telecomunicaciones en Colombia, como coordinador responsable del sector de las comunicaciones ante el Sistema Nacional de Prevención y Atención de Desastres SNPAD, y ante el compromiso de fomentar el fortalecimiento de las redes de telecomunicaciones con el fin de que estas se auto soporten en situaciones de emergencias y desastres, consideró necesario llevar a cabo un *"estudio de vulnerabilidad y riesgo de las redes e infraestructura de telecomunicaciones en zonas vulnerables expuestas a eventos naturales desastrosos".* De acuerdo con lo anterior, con el fin de llevar a cabo el estudio, el Ministerio de Tecnologías de la Información y las Comunicaciones y el Centro de Investigación de las Telecomunicaciones - CINTEL, suscribieron el contrato interadministrativo 301.

En este sentido, el presente documento corresponde al informe de final del proyecto el cual incluye el modelo de vulnerabilidad y riesgo, el diagnóstico sobre amenazas naturales, el diagnóstico de vulnerabilidad de redes básicas de telecomunicaciones, la aplicación del modelo y las conclusiones y recomendaciones. El estudio propende por estimular el conocimiento sectorial sobre los riesgos de origen natural y antrópico de la siguiente manera:

- Incentivar programas para la incorporación de la prevención y reducción de riesgos en la planificación.

- Orientar las acciones del Sector de Telecomunicaciones en relación con los métodos de análisis de la vulnerabilidad y evaluación de amenazas y riesgos.
- Orientar las acciones del Sector de Telecomunicaciones para apoyo al Sistema Nacional para la Prevención y Atención de Desastres SNPAD
- Fomentar el aporte de las telecomunicaciones en situaciones de emergencias y desastres.
- Impulsar el fortalecimiento de la infraestructura de telecomunicaciones y líneas vitales para resistir los impactos de los fenómenos adversos de la naturaleza y mitigar los efectos de un posible evento desastroso.
- Incentivar la protección de redes y la continuidad de los servicios públicos.
- Permitir el desarrollo y actualización de planes de emergencia y contingencia.

2.1 ASPECTOS GENERALES

Las amenazas naturales se pueden describir como aquellos fenómenos no provocados por el hombre que pueden ocasionar un perjuicio para el mismo. El planeta, por sus condiciones especiales y características físicas que lo conforman es capaz de albergar la vida, sin embargo y contradictoriamente esta capacidad también genera riesgos contra la misma. Los fenómenos naturales suceden todos los días, son de todo tipo y magnitud como la lluvia, la evaporación, los aumentos de caudal, los vientos, la radiación solar, etc.; sin embargo, solo aquellos fenómenos que ocurren donde se encuentran asentados los seres humanos y sus intereses económicos son los que representan algún grado de amenaza. Las amenazas naturales por consecuencia se circunscriben a aquellas que generen un impacto directo o indirecto a los intereses del hombre, las cuales pueden ser originadas por uno o varios fenómenos conjugados, los cuales se pueden catalogar dependiendo del tipo del medio que los crea como lo atmosférico, lo hidrológico y lo geológico.

El presente estudio se enmarca en evaluar la amenaza natural por sismo, erupción volcánica, tsunami e inundación, a la que está sometida la infraestructura vital de telecomunicaciones que le presta servicio a un determinado grupo de personas.

2.2 EL ENTORNO GEOGRÁFICO NACIONAL Y LOS DESASTRES NATURALES[1]

La República de Colombia se encuentra situada en el extremo noroccidental de Suramérica, es el único país del subcontinente con costas sobre los océanos Atlántico y Pacífico, con una superficie terrestre de 1.141.748 km.2 y 928.660 km.2 de dominios marítimos. Con cerca de 45 millones de habitantes. En el año 2006, Colombia tenía la tercera mayor población en Suramérica.

[1] **Documento de Alcance - Atención de desastres del Ministerio de Tecnologías de la Información y las Comunicaciones elaborado en 2010.**

Figura 1. Mapa Oficial de la República de Colombia

Fuente: IGAC

El territorio colombiano se encuentra localizado en una zona de alta complejidad tectónica, donde las placas Suramericana, de Nazca y del

Caribe generan una alta actividad sísmica y volcánica. Por su situación geográfica, con dos mares, llanuras, selvas tropicales y una importante cadena montañosa, el territorio se ve afectado continuamente por los siguientes fenómenos naturales:

- Hidrometeorológicos: inundaciones, deslizamientos, granizadas, avalanchas, vendavales, mares de leva, tormentas, huracanes, tornados, sequías, incendios forestales.
- Geológicos: Fallas, sismos, tsunamis.
- Volcánicos: Actividad que implica erupciones de material fundido (magma) generado en el interior de la Tierra, con manifestaciones de columnas de gases, cenizas, caída de piroclastos, flujos de lava, proyectiles, etc., que llegan a afectar poblaciones, agricultura e infraestructura.
- Antrópicos: Se incluyen estos eventos originados por el ser humano, como el derrame de hidrocarburos, sustancias nocivas, explosiones, incendios, etc., eventos catastróficos que pueden llegan a afectar a las regiones y a la población que habita en zonas vulnerables, causando alteraciones de tipo ambiental, social y económico.

Adicionalmente, los asentamientos subnormales en zonas en las que pueden ocurrir fenómenos naturales originan los “disparadores” de los grados de amenaza sobre la población allí asentada.

2.2.1 Fenómenos Hidrometeorológicos[2]

Los desastres de origen hidrometeorológico son los más frecuentes en Colombia con un 97.38% de los casos, seguidos por los terremotos (1.86%), mares de leva (0.49%) y erupciones volcánicas (0.27%).

La temporada invernal de 1988 fue una de las que más daños ha producido en la historia del país: afectó directamente alrededor de 400.000 personas de 283 municipios, deterioró 15.000 kilómetros de carreteras, destruyó cerca de 7.000 viviendas y dañó parcialmente otras 23.000. En el año 2007, por efecto del fenómeno de la Niña, se inundaron cerca de 400 municipios del país incluida La Mojana Sucreña y las riberas del río Sinú. En el año 2008, las fuertes lluvias afectaron 207 municipios en 27 de los 32 departamentos colombianos, que dejaron cerca de 124.500 damnificados, 25.436 familias afectadas, 12.333 viviendas dañadas, cultivos destruidos, varios muertos, heridos y desaparecidos. En el 2010, se presentaron niveles históricos donde las inundaciones afectaron a más de 1´300.000 personas en todo el territorio, en 714 municipios afectados de 28 departamentos y el distrito capital. Adicionalmente, los eventos del 2010 produjeron impactos económicos como la disminución esperada de exportación de carbón, entre otros.

La temporada invernal del 2010 ha cambiado los máximos de precipitación reportados en Colombia hasta la fecha, causando aumentos no esperados en el caudal de los ríos, así como se han registrado topes máximos en las capacidades de las represas del país, superando en muchos casos el 100%

[2] **Documento de Alcance - Atención de desastres del Ministerio de Tecnologías de la Información y las Comunicaciones elaborado en 2010.**

de capacidad de almacenamiento de las mismas, situación que ha ocasionado que estas deban liberar más agua hacia los ríos.

De otra parte, la deforestación de las cuencas, los bajos resultados de la ejecución de los planes y programas ambientales en el territorio, los asentamientos en zonas de inundación natural de los cuerpos de agua, la sedimentación y muchas otras variables han ocasionado la peor tragedia en el país a causa de una temporada invernal prolongada.

Los ríos que con mayor frecuencia se desbordan en Colombia son: el Magdalena, Cauca, Sinú, Atrato, Bogotá, Tunjuelito, Meta, Nechí, San Jorge, San Juán y Ariari. Las lluvias de más de 100 mm de precipitación en 24 horas llegan causar desastres hidrometeorológicos con excepción de las regiones del Chocó, la selva del Amazonas y el piedemonte llanero (Pedraza, William, 2010), zonas en las cuales la baja densidad poblacional condiciona a que no se presenten desastres de mayor magnitud.

En la historia nacional conocida han pasado sobre o cerca de las islas colombianas del Caribe 56 sistemas tropicales: 30 tormentas tropicales, 21 huracanes y 5 depresiones tropicales. Cerca del departamento de la Guajira han transitado 22 sistemas desde 1877 hasta el año 2007.

2.2.2 Fenómenos Geológicos[3]

Colombia se encuentra en el cinturón de fuego del pacífico, una zona donde se presentan en promedio 30 mil sismos al año. El Terremoto de Armenia, Quindío (ocurrido el 25 de enero de 1999), uno de los más desastrosos en la historia del país, destruyó una importante parte de la ciudad con gran afectación y pérdida de vidas humanas (1.230 muertos, 3.900 desaparecidos, 5.300 heridos, 50.000 edificaciones averiadas y 200.000 personas afectadas).

En materia de Tsunamis, se resalta el sismo de San Andrés de Tumaco, Nariño en 1906, que con una magnitud de 8.8 grados (uno de los sismos más grandes de subducción en el mundo) ocasionó la pérdida de 2.500 vidas humanas por Tsunami. Tumaco, en la costa pacífica, es la región colombiana más propensa a los fenómenos de Tsunamis.

2.2.3 Fenómenos Volcánicos[4]

En Colombia se conoce la existencia de 38 volcanes ubicados en la Cordillera Central, quince (15) de los cuales se encuentran activos: Cerro Bravo, Nevado del Ruiz, Nevado de Santa Isabel, Nevado del Taluna, Machín, Nevado del Huila, Puracé, Pan de azúcar, Sotará, Doña Juana, Galeras, Azufral, Cumbal, Chiles y Cerro Negro. Los volcanes de mayor actividad son el Huila, el Galeras y el Ruiz y los más peligrosos el volcán

---

[3] Documento de Alcance - Atención de desastres del Ministerio de Tecnologías de la Información y las Comunicaciones elaborado en 2010.

[4] Documento de Alcance - Atención de desastres del Ministerio de Tecnologías de la Información y las Comunicaciones elaborado en 2010.

cerro Machín y el cerro Bravo. Varios de estos volcanes han tenido erupciones, algunas de las cuales han sido de carácter catastrófico. El Volcán Nevado del Ruiz en 1985 causó la mayor tragedia en pérdida de vidas en la historia de Colombia con cerca de 20.000 muertos y destruyó, por tercera vez desde su fundación, la ciudad de Armero en similares circunstancias.

2.2.4 Vulnerabilidad y Riesgo[5]

En los casos de catástrofes, las redes de telecomunicaciones, tanto fijas como móviles, pueden verse afectadas en su estructura o en su funcionamiento, ya sea porque el evento catastrófico destruyó la estructura física de toda o una parte de la red, de forma que se imposibilita realizar una comunicación efectiva, o el suceso desastroso arruinó los enlaces necesarios para la configuración de la red, o por el incremento inusitado de tráfico de llamadas, lo que satura y sobrecarga la red pública telefónica y la imposibilita para su operación en condiciones normales.

Dependiendo del peligro yacente, de la exposición y de la vulnerabilidad de los elementos, los eventos catastróficos pueden afectar en diversos grados y niveles las redes e infraestructura de telecomunicaciones como equipos, cables, plantas de energía, su infraestructura conexa (edificaciones, casetas, torres de antena, postes, ductos y demás obras civiles), y/o afectar otros servicios públicos de soporte de las telecomunicaciones, como el servicio de energía eléctrica.

---

[5] Documento de Alcance - Atención de desastres del Ministerio de Tecnologías de la Información y las Comunicaciones elaborado en 2010.

Las redes e infraestructura de telecomunicaciones ubicadas en zonas de amenazacon probabilidad de ocurrencia de eventos naturales desastrosos, se encuentran expuestas al riesgo y éste puede ser mayor, si aquellas son vulnerables y/o no se encuentran debidamente protegidas.

La definición de riesgo (R) hace referencia a la probabilidad de que a un elemento o sistema determinado le ocurra algún daño con consecuencias económicas, técnicas, sociales o ambientales.

La expresión conceptual más conocida para expresar el riesgo es: R = A * V, ó

$$\text{Riesgo} = \text{Amenaza o Peligro} \times \text{Vulnerabilidad}$$

Esta expresión se obtiene de relacionar el peligro o amenaza (A) con la vulnerabilidad (V) de los elementos expuestos. En esta expresión, A (amenaza) es entendida como un peligro latente asociado con un fenómeno físico y se refiere a la probabilidad de ocurrencia de un evento con una cierta intensidad, en un sitio específico y en un periodo de tiempo determinado y V (vulnerabilidad) es entendida como la predisposición intrínseca o característica del elemento o grupo de elementos de ser dañados o afectados total o parcialmente como consecuencia de la ocurrencia de un fenómeno de intensidad determinada.

Sin embargo, existen otras definiciones de riesgo ampliamente aceptadas, las cuales en su mayoría definen que el riesgo es también la función que existe entre la probabilidad de ocurrencia de un evento incierto o materialización del riesgo y el impacto que puede tener la materialización del evento frente a los intereses del analizados; dichos intereses pueden ser la prestación de un servicio, la continuidad del negocio o hasta los objetivos de un proyecto.

Riesgo = Probabilidad X Impacto

En este orden de ideas, el presente estudio incluyó el análisis del impacto sobre el servicio, que puede generar el peor escenario de un evento natural catastrófico sobre los elementos de la red vital de telecomunicaciones definida en el capítulo 5.1 REDES Y SERVICIOS VITALES DE TELECOMUNICACIONES.

Independiente de las incertidumbres del fenómeno a considerar (terremoto, erupción volcánica, tsunami, inundación, etc.) o del conocimiento que se tenga acerca de ese fenómeno, la cuantificación de la Amenaza o Peligro (P) suele hacerse en términos probabilísticos, y expresarse como la probabilidad de una variable aleatoria X que exceda a un valor Xo en un lapso de tiempo t (Pedraza, William, 2010).

Así se tiene: $P (X > Xo / t)$

El riesgo entonces se incrementa con el factor de vulnerabilidad, considerando que el peligro es un fenómeno natural que no puede ser eliminado o reducido. La determinación del riesgo se realiza sobre la base de las proyecciones de las clases de daños para los diferentes tipos de áreas geográficas, edificaciones, infraestructuras, etc.

Usualmente se clasifica el riesgo como:

Riesgo Alto: Probabilidad de grandes daños.

Riesgo Medio: Probabilidad de daños moderados.

Riesgo Bajo: Probabilidad de daños leves ó de no sufrir daños.

El proceso del conocimiento de la vulnerabilidad a las amenazas es de gran importancia para determinar la capacidad de las redes e infraestructura de telecomunicaciones para resistir sus impactos y para encaminar las acciones a la mitigación, restablecimiento y/o mejoramiento de las condiciones que se tenían antes del evento crítico. Las estrategias preventivas y de anticipación son muy útiles a la hora de reducir la vulnerabilidad de las comunidades y de los sectores económicos y productivos nacionales.

Igualmente, en los procesos de recuperación y reconstrucción se debe profundizar en los escenarios de daños y en la cuantificación de los impactos sobre las redes e infraestructura y sus efectos sobre la zona afectada, para lograr la pronta recuperación del servicio a los usuarios, de acuerdo con un plan de prioridades y posibilidades técnicas. El proceso del conocimiento de las amenazas, la vulnerabilidad y el riesgo ayudará a prever otros aspectos administrativos eventualmente necesarios para la recuperación y reconstrucción. Entre éstos se encuentran procesos de indemnización, cobro de seguros, importación, nacionalización de equipos y sistemas y, otros factores financieros y económicos.

A criterio de los expertos, lo primero que se debe hacer para prevenir y reducir la vulnerabilidad ante estos desastres naturales es evaluar los elementos de amenaza o peligrosidad, la vulnerabilidad y el riesgo ante estos eventos. Para ello, es necesario crear comisiones multidisciplinarias para compilar datos y clasificarlos, ordenarlos y modelar las probabilidades de ocurrencia versus el tiempo. Así, se podrá determinar la peligrosidad de zonas vulnerables expuestas a eventos naturales desastrosos.

Con la determinación de la peligrosidad de los eventos, los expertos podrán clasificar la vulnerabilidad de las diferentes zonas, construcciones e infraestructura que en ellas se encuentran. Igualmente, se podrán cuantificar

los riesgos. Con ellos, se podrá estudiar la manera de reducirlos a través de acciones concretas a corto, mediano y largo plazo. Las acciones de corto plazo tienen que ver con la urgente implementación de medidas de prevención, mitigación y atenuación del riesgo por las entidades, empresas, operadores y proveedores de redes y servicios de telecomunicaciones, a través de planes, acciones y con recursos y presupuestos específicos para disminuir las vulnerabilidades. Las acciones a mediano plazo pueden hacer relación a la creación de normas nacionales y locales de obligatorio cumplimiento, y las acciones a largo plazo a los programas de investigación y desarrollo de nuevas técnicas para reducir los riesgos y las vulnerabilidades.

2.3 NORMAS, PLANES Y DOCUMENTOS SOBRE TELECOMUNICACIONES EN EMERGENCIAS[6]

El papel importante que desempeñan las telecomunicaciones de emergencia ha sido reconocido en numerosos documentos internacionales, declaraciones, convenios, resoluciones y tratados que comprometen a los Estados al aporte y desarrollo de las Telecomunicaciones en situaciones de socorro, emergencias, catástrofes y desastres producto de conferencias internacionales y de la labor realizada en reuniones especializadas de la Unión Internacional de Telecomunicaciones UIT y de la Comisión Interamericana de Telecomunicaciones CITEL. Entre estos documentos se citan: el convenio de Tampere (Irlanda 1998), la III cumbre de jefes de estado de las Américas (Quebec, Canadá, 2001); el plan de acción de Yokohama (1994): las Resoluciones 44/236 y 51/194 de la ONU; las Resoluciones 7 y 36 de las conferencias mundiales de la UIT, y la recomendación REC. 24/CCP. III/ (VI-96) de la CITEL.

De manera general, estos documentos recomiendan, entre otros, que cada uno de los países desarrolle un Plan Nacional para proveer comunicación de emergencia y que los recursos de los Servicios Móviles Terrestres se refuercen para asistir en comunicaciones de alivio de desastre. Igualmente, que los países garanticen una aportación rápida y fiable de recursos de telecomunicaciones para atenuar los efectos de las catástrofes y realizar operaciones de socorro en caso de emergencia, así como la creación de un sistema mundial de información para la difusión de información fiable y oportuna sobre emergencias y catástrofes naturales.

---

[6] Documento de Alcance - Atención de desastres del Ministerio de Tecnologías de la Información y las Comunicaciones elaborado en 2010.

A continuación, se presentan los documentos a nivel nacional que se relacionan con el tema de estudio.

2.3.1 La Ley 46 De 1988

En el entorno nacional, el congreso de Colombia expidió en el año de 1988 la Ley 46 “por la cual se crea y organiza el Sistema Nacional para la Prevención y Atención de Desastres SNPAD” y a su vez ordena la elaboración de un Plan Nacional para la Prevención y Atención de Desastres.

2.3.2 El Decreto Ley 919 de 1989

En 1989 el Gobierno nacional expide el Decreto Ley 919 “por el cual se organiza el Sistema Nacional para la Prevención y Atención de Desastres. El Decreto Ley 919 establece, entre otros:

“…La utilización de los sistemas y medios de comunicación en caso de desastres y calamidades se regirá por las reglamentaciones que para efecto dicte el Ministerio de Tecnologías de la Información y las Comunicaciones.” (Art. 15, inc. 2º.)

“La Oficina Nacional para la Atención de Desastres promoverá la organización y funcionamiento de la red nacional de comunicaciones en situaciones de desastre o calamidad, de la red sísmica y vulcanológica Nacional, de la red de alertas hidrometeorológicas, de la red nacional de centros de reserva, de la red nacional de información y de las demás redes que técnicamente se consideren necesarias” (art.65).

“Las entidades y organismos de la administración central y sus entidades descentralizadas podrán confiar recursos en administración fiduciaria para los efectos de la prevención y atención de desastres y calamidades, y para las actividades de las fases de rehabilitación, reconstrucción o desarrollo,

previa autorización de la Oficina Nacional para la Atención de Desastres, que podrá estar subordinada a la inclusión en el contrato respectivo de la facultad de intervención de esa misma Oficina en orden a asegurar la estricta destinación de los recursos…"(art.66).

"Todos los organismos y dependencias de la administración central y todas las entidades descentralizadas del orden nacional incluirán en sus presupuestos, apropiaciones especiales para prevención y atención de desastres…" (art.67).

2.3.3 El Decreto 93 de 1998

Para 1998 el Gobierno Nacional expide el Decreto 93 de 1998 por el cual se adopta el Plan Nacional para la Prevención y Atención de Desastres PNPAD, y la Directiva Presidencial No. 05 de 2001 que dicta "las Guías o Protocolos de Actuación del Alto Gobierno para los casos de emergencias y desastres". El Decreto 93 determina las orientaciones, acciones, programas y proyectos, tanto de carácter sectorial como de orden nacional, regional y local, en las fases de prevención, atención inmediata y reconstrucción, y los temas de orden técnico, científico, jurídico, comunitario, económico, financiero, y de coordinación interinstitucional e intersectorial que deben ser tratados en desarrollo del Plan Nacional para la Prevención y Atención de Desastres.

El artículo 3º del Decreto 93 de 1998 determina los objetivos del Plan Nacional para la Prevención y Atención de Desastres, así:

- La reducción de riesgos y prevención de desastres.
- La respuesta efectiva en caso de desastre.
- La recuperación rápida de zonas afectadas.

El artículo 5º del Decreto 93 de 1998 determina los PRINCIPIOS generales que orientan las acciones de las entidades nacionales y territoriales en relación con el Plan Nacional para la Prevención y Atención de Desastres, y el artículo determina las estrategias generales del Plan Nacional para la Prevención y Atención de Desastres.

Por su parte, el artículo 7º del Decreto 93 de 1998 describe los principales programas que el Sistema Nacional para la Prevención y Atención de Desastres SNPAD debe ejecutar; así:

- Programas para el conocimiento sobre riesgos de origen natural y antrópico.
- Programas para la incorporación de la prevención y reducción de riesgos en la planificación.
- Programas de fortalecimiento del Desarrollo Institucional.
- Fortalecimiento de las entidades nacionales del sistema.
- Fortalecimiento de los comités regionales y locales de prevención y atención de desastres, CREPAD y CLOPAD.
- Fortalecimiento de las entidades operativas (en especial, Sistema Nacional de Cuerpos de Bomberos, Defensa Civil Colombiana, Cruz Roja Colombiana.).
- Fortalecimiento de la infraestructura y protección de redes de servicios públicos y líneas vitales.
- Desarrollo y actualización de planes de emergencia y contingencia.
- Previsiones para la ejecución de proyectos de reconstrucción en caso de desastre, y de rehabilitación de líneas vitales e infraestructura afectada.
- Diseño y mantenimiento de un Sistema Integrado de Información SII, para la prevención y atención de desastres,

que contenga la información acerca de las acciones y la gestión de las entidades nacionales, regionales y locales del Sistema Nacional.

El Decreto 93 de 1998, tanto en su Objetivos (artículo 3º) como en sus programas, especialmente en el numeral 3 del artículo 7º, promueve:

- El mejoramiento de las redes y sistemas de comunicaciones para fortalecer la capacidad de operación y respuesta de la red de urgencias en caso de desastre.
- El fortalecimiento de las entidades nacionales del sistema.
- El fortalecimiento de las entidades operativas, en particular los cuerpos de bomberos, la Defensa Civil y la Cruz Roja.
- El fortalecimiento de los comités regionales y locales de prevención y atención de desastres, CREPAD y CLOPAD.
- El mantener una reserva permanente de recursos financieros a fin de soportar una respuesta inmediata a la emergencia, y brindar apoyo alimentario, de vivienda, de combustibles, transporte y telecomunicaciones, entre otros.

Bajo el ordenamiento del Decreto 93 de 1998, el “Plan Nacional para la Prevención y Atención de Desastres”, crea 10 Áreas o Grupos Sectoriales, entre estos, el Grupo Sectorial # 2 para la “Coordinación de Telecomunicaciones” siendo la entidad responsable de la coordinación el Ministerio de Tecnologías de la Información y las Comunicaciones.

2.3.4 EL CONPES 3146 DE 2001

El documento CONPES 3146 de 2001: “Estrategia para consolidar la ejecución del plan nacional para la prevención y atención de desastres – PNPAD - en el corto y mediano plazo”, en su diagnóstico sobre los Aspectos Relativos al Desarrollo Institucional del Sistema Nacional para la Prevención

y Atención de Desastres –SNPAD - (II. Sección B, Página 8 y ss.,) manifiesta que: "…un balance general de su desarrollo institucional permite señalar algunos puntos que requieren ser fortalecidos:

- El SNPAD no cuenta con un sistema integrado de comunicaciones para facilitar la interacción y coordinación entre sus miembros y la comunicación con la comunidad.
- Aunque el SNPAD presenta positivos avances en cuanto a la interrelación y coordinación entre los ámbitos local, regional y nacional, aún subsisten deficiencias en este sentido.
- Si bien existen acciones de fortalecimiento hacia los departamentos y municipios, se requiere de una estrategia nacional permanente para incorporar el tema en la planificación territorial y sectorial, en las inversiones, en la coordinación interinstitucional y en la participación comunitaria (Pág. 19).
- Existen importantes avances en tecnologías de información y comunicación TIC, además de una política nacional en la materia, sin embargo, son insuficientes para generar programas permanentes de uso de estas tecnologías y servicios en la divulgación del conocimiento para capacitación, toma de decisiones y concientización ciudadana.
- La Dirección de Prevención y Atención de Desastres y el Ministerio de Tecnologías de la Información y las Comunicaciones continuarán con el diseño y puesta en marcha del sistema de comunicación e información pública para el SNPAD, que conecte a todas las entidades miembros de este, entre ellas y con la comunidad (Pág. 19).
- La Dirección de Prevención y Atención de Desastres, a partir de la información generada por las redes de monitoreo y alertas del sistema, continuará coordinando la comunicación de información de alertas a través de los Comités Regionales y Locales del SNPAD. Esta actividad se verá fortalecida una vez la Dirección cuente con el sistema de comunicación e

información pública. Para alertas de carácter nacional, la Dirección de Prevención y Atención de Desastres, a través del Comité Técnico Nacional contará con el apoyo de los ministerios (Pág. 21).

Respecto al fortalecimiento de las líneas programáticas del Plan Nacional (II. Sección A, Página 22 y ss.,) el CONPES manifiesta en el aparte Concientización Ciudadana, que:

- La Dirección de Prevención y Atención de Desastres y el Ministerio de Tecnologías de la Información y las Comunicaciones formularán y desarrollarán una estrategia nacional de comunicación e información pública masiva y permanente, a través de canales adecuados, orientada a elevar el nivel de conciencia ciudadana en temas relacionados con el manejo integral de riesgos.
- La Dirección de Prevención y Atención de Desastres, la Defensa Civil, la Cruz Roja Colombiana y los Cuerpos de Bomberos, con el apoyo del Ministerio de Tecnologías de la Información y las Comunicaciones, fortalecerán el apoyo que ofrecen a los Comités Regionales y Locales del SNPAD en las acciones de socialización de los Planes de Contingencia.

En relación con los aspectos financieros del SNPAD el Anexo 3 del CONPES 3146 de 2001: Requerimientos Iniciales de Inversión - Estrategia para Consolidar la Ejecución del Plan Nacional para la Prevención y Atención de Desastres - Trienio 2002 -2004 (Pág. 30), expresa que el Ministerio de Tecnologías de la Información y las Comunicaciones debe elaborar una estrategia tendiente a planificar el Sistema Nacional de Comunicaciones (de emergencias), para lo cual deberá disponer de Requerimientos Iníciales de Inversión para una demanda aproximada de 2.000 Millones de pesos.

Finalmente, el CONPES 3146 recomienda, entre otros:

- Solicitar a cada uno de los Ministerios y demás entidades del sistema, diseñar el plan de los compromisos que surgen de este documento, y gestionar los recursos para financiar las acciones priorizadas bajo su competencia, y las encargadas en cabeza del Comité Técnico Nacional y de las Comisiones Asesoras del Sistema.

2.3.5 La Ley 1341 de 2009

El artículo 8º de la Ley 1341 de 2009, establece que “en casos de atención de emergencia, conmoción interna y externa, desastres, o calamidad pública, los proveedores de redes y servicios de telecomunicaciones deberán poner a disposición de las autoridades de manera gratuita y oportuna, las redes y servicios y darán prelación a dichas autoridades en la transmisión de las comunicaciones que aquellas requieran. En cualquier caso se dará prelación absoluta a las transmisiones relacionadas con la protección de la vida humana. Igualmente darán prelación a las autoridades en la transmisión de comunicaciones gratuitas y oportunas para efectos de prevención de desastres, cuando aquellas se consideren indispensables. Los proveedores de redes y servicios de telecomunicaciones deberán suministrar a las autoridades competentes, sin costo alguno, la información disponible de identificación y de localización del usuario que la entidad solicitante considere útil y relevante para garantizar la atención eficiente en los eventos descritos en el presente artículo”.

2.4 ASPECTOS SOBRE LA IMPORTANCIA DEL ESTUDIO

Desde sus primeros días, las telecomunicaciones han desempeñado una importante función en el socorro aportado a situaciones de emergencia y desastre. Quizás el acontecimiento más conocido sea el de los hechos que rodearon el hundimiento del Titanic en 1912. La tecnología de la radiocomunicación telegráfica sirvió para solicitar ayuda a barcos cercanos que pudieron contribuir al salvamento de más de 700 personas en altamar. La repercusión del desastre del Titanic en las comunicaciones marítimas fue enorme. Aquel mismo año, se adoptó el primer Convenio internacional para la seguridad de la vida humana en el mar y, más adelante, se modificó el Reglamento de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones UIT para incluir requisitos operativos obligatorios y disposiciones sobre comunicaciones para socorro marítimo. La importancia de las telecomunicaciones en la seguridad de la vida humana no ha disminuido y por el contrario en la actualidad desempeñan una función vital en las operaciones de socorro en caso de emergencia.

En reflejo de su importancia, el mercado de las telecomunicaciones ocupa uno de los primeros renglones de la economía mundial. Los servicios aportan toda clase de comunicaciones de voz, datos, imágenes y video, en tierra, mar y aire; donde las redes de telecomunicaciones se convierten en el sistema nervioso de la sociedad y se configuran en una infraestructura crítica y esencial para un país. En tal sentido, las telecomunicaciones conforman una de las más importantes infraestructuras, que soporta, no solo las comunicaciones públicas para todos los habitantes del territorio nacional y de éste con el exterior, así como las comunicaciones de las entidades del Estado y del Gobierno Nacional, sino las comunicaciones de las entidades y organismos de socorro en casos de emergencia o desastre.

Sin embargo y paradójicamente, las redes públicas de telecomunicaciones casi siempre quedan colapsadas, interrumpidas o inutilizadas en los instantes cruciales que siguen a las catástrofes naturales. Esta pérdida de comunicación genera de por sí otra emergencia adicional a la misma catástrofe natural, ya que las zonas afectadas suelen quedar aisladas muy rápidamente del contexto regional, nacional e internacional.

Las redes públicas de telecomunicaciones son el único medio de comunicación que tiene la población para pedir ayuda a los organismos de socorro en casos de emergencia, normalmente a través del número único de emergencias, así como para informar a familiares acerca del estado de sus vidas y sus bienes. Las redes públicas sirven al gobierno y a las autoridades para transmitir alertas e instrucciones a la población y a los organismos de socorro para el establecimiento de sus comunicaciones corporativas y para con las autoridades, dentro y fuera de la zona de emergencia.

No se puede prestar una asistencia humanitaria adecuada y eficaz si no funcionan las telecomunicaciones en la zona de emergencia, y esto resulta aún más importante cuando son numerosos los organismos de socorro que operan en el terreno antes, durante y después de una catástrofe. La deficiencia y daños en las redes de telecomunicaciones genera una mayor dificultad cuando se presentan emergencias de gran magnitud impidiéndose prestar adecuadamente servicios de asistencia humanitaria y operaciones de búsqueda, salvamento y rescate. Así mismo se dificultan enormemente las operaciones de coordinación, información y gestión de la emergencia por parte de las autoridades, quienes posiblemente tampoco cuentan con las comunicaciones apropiadas en la zona de emergencia y para la comunicación de ésta con el exterior.

Es indiscutible que las telecomunicaciones son parte fundamental de la eficiencia en la respuesta y la atención que se pueda dar ante una emergencia o desastre y más aun si éste es del orden nacional. Varios son los fenómenos naturales que por diversas causas pueden llegar a generar eventos catastróficos.

3 MODELO DE VULNERABILIDAD Y RIESGOS

En este capítulo se presenta el modelo desarrollado, incluyendo los aspectos generales, las definiciones de niveles de adversidad al riesgo, de umbrales de tolerancia y del universo de riesgos, así como la identificación de los riesgos, la calificación de amenazas por vulnerabilidades y su priorización, la identificación de escenarios hipotéticos, la presentación de las tablas de riesgos, la definición de criterios de impacto vs. relevancia de impacto y la descripción del modelo y sus guías de uso.

3.1 DEFINICIÓN Y ASPECTOS GENERALES DEL MODELO SELECCIONADO

Existen diferentes tipos de enfoques para la aproximación a la formulación de un modelo de vulnerabilidad y riesgo. Estos modelos pueden dividirse en aquellos que intentan simular matemáticamente la amenaza natural, la vulnerabilidad física de los elementos asociada a los materiales y los parámetros constructivos como normas, buenas prácticas y procesos de calidad; y aquellos modelos que se enfocan en una gestión integrada del riesgo.

Dentro de los modelos matemáticos se pueden nombrar entre muchos otros el modelo IRAM que realiza análisis de riesgos específicos para la infraestructura, donde la vulnerabilidad es modelada matemáticamente en función del acceso y la exposición según el NSTAC7, centrado especialmente en la seguridad. Existe otro modelo de evaluación de la vulnerabilidad de la infraestructura llamado (I-VAM) que usa una aproximación matemática basada en valores de multi atributos de la infraestructura, usando un sistema de calificación del riesgo.

Adicionalmente, existen otras aproximaciones enfocadas netamente al estudio y modelación de la resistencia de los materiales y su configuración constructiva contra los diferentes tipos de amenaza; estos estudios deben realizar pruebas en laboratorio con modelos a escala de los elementos a ser sometidos a prueba.

[7] ***National Security Telecommunications Advisory Committee de Estados Unidos**

Por otro lado, en concordancia con los principales objetivos del estudio, que son:

- Identificar en las cuatro zonas identificadas la infraestructura vital de telecomunicaciones.
- Identificar y cuantificar para las cuatro zonas identificadas las amenazas sobre la infraestructura vital.
- Identificar y cuantificar para las cuatro zonas identificadas la vulnerabilidad de la infraestructura.
- Determinar un modelo general del análisis y evaluación del riesgo para las redes e infraestructura de telecomunicaciones para las cuatro zonas identificadas.
- Aplicar el modelo general de evaluación del Riesgo para la infraestructura vital en las cuatro zonas identificadas de amenaza.
- Generar conclusiones y recomendaciones para la protección de la infraestructura vital en las cuatro zonas identificadas de amenaza.
- Generar conclusiones y recomendaciones generales para la protección de la infraestructura, como orientación al sector de telecomunicaciones en las cuatro zonas identificadas.

Se determinó que el tipo de modelo que mejor se ajusta a las necesidades del Ministerio de Tecnologías de la Información y las Telecomunicaciones es aquel que incluya una gestión integrada del riesgo en términos de aplicar buenas prácticas en los procesos corporativos tanto de las instituciones

gubernamentales como de los operadores de la infraestructura de Telecomunicaciones en el país.

Con base en lo anterior, se seleccionó un modelo que determina los pasos necesarios que se deben llevar a cabo para realizar una gestión integrada del riesgo así:

1. Definición de niveles de adversidad al riesgo
2. Definición de umbrales de tolerancia
3. Definición del universo de riesgos
4. Identificación de riesgos
5. Determinación de probabilidades de ocurrencia
6. Determinación de impactos
7. Calificación de riesgos de acuerdo a probabilidad e impacto
8. Priorización de riesgos modelo
9. Aproximación a las acciones de mitigación
10. Generación de un mapa de riesgos
11. Ejecución de actividades de monitoreo y control de riesgos

Para desarrollar cada uno de estos pasos, se hace necesario entender los conceptos fundamentales de la gestión del riesgo, los cuales son aplicados y adaptados para la identificación, análisis, planeación, monitoreo y control de los riesgos a los que está sometida la infraestructura de telecomunicaciones en las zonas de estudio.

A continuación se presentan algunas definiciones asociadas al proceso de la gestión del riesgo.

Amenaza

Una amenaza natural se puede definir como aquel evento o fenómeno natural que impacta de manera negativa los intereses socio-económicos de una población determinada. Para el estudio en cuestión se definen como amenazas aquellos eventos naturales que pueden impactar la correcta operación de la infraestructura de telecomunicaciones.

Vulnerabilidad

La vulnerabilidad se puede definir como la capacidad que tiene un elemento de resistir los efectos y consecuencias de un fenómeno natural ante la materialización de un riesgo y que impide la normal operación de un servicio de comunicaciones.

Riesgo

Es el resultado de la función de todos los factores que generan la amenaza por todos los factores que definen la vulnerabilidad de los elementos.

Impacto

Se puede determinar como los daños generados a los elementos de una red vital de telecomunicaciones que impactan en un nivel determinado la prestación del servicio analizado. Los niveles pueden estar determinados por valores cualitativos, estimados por juicios de expertos o por valores cuantitativos que pueden estar expresados en función del número de personas afectadas por la interrupción o degradación de los niveles acostumbrados del servicio analizado.

En términos generales para calcular el riesgo se tiene que:

Riesgo= Amenaza x Vulnerabilidad

Donde la amenaza está definida por cada uno de los eventos naturales, cuyos valores están definidos y detallados en el capítulo de diagnóstico de las Amenazas Naturales, así como por su probabilidad de ocurrencia y la fase en la que se encuentre.

La vulnerabilidad está dividida en vulnerabilidad física de los elementos y vulnerabilidad funcional, las cuales están definidas y detalladas en el capítulo de diagnóstico de la vulnerabilidad de las redes básicas de telecomunicaciones, enfocados en su resistencia y redundancia.

Se define que los riesgos se pueden mantener en estado latente hasta que se genera un evento que impide la normal operación de un servicio de comunicaciones.

El proceso de análisis y evaluación de los riesgos del modelo a usar, describe las actividades que se deben realizar iterativamente, en la medida de lo posible alineadas con las estrategias corporativas de las entidades gubernamentales y/o con las de los operadores de telecomunicaciones. Estas actividades se agrupan en las etapas de planeación, identificación, análisis, mitigación, contingencia y monitoreo y control de la gestión del riesgo, según se definen a continuación.

- ***Planeación*** – Etapa necesaria para la determinación de un enfoque para administrar los riesgos, alineada a las estrategias corporativas y sus intereses. Esta planeación debe incluir cuáles son los sistemas que se usarán para la identificación y análisis, cómo se establecen los presupuestos para las

acciones de mitigación y tratamiento del riesgo, así como los mecanismos de reporte a la alta dirección y las entidades de gobierno.

- ***Identificación de riesgos*** – Proceso en el cual se realiza la identificación de los elementos de la infraestructura que están sometidos a algún tipo de amenaza natural en función su vulnerabilidad física y funcional.

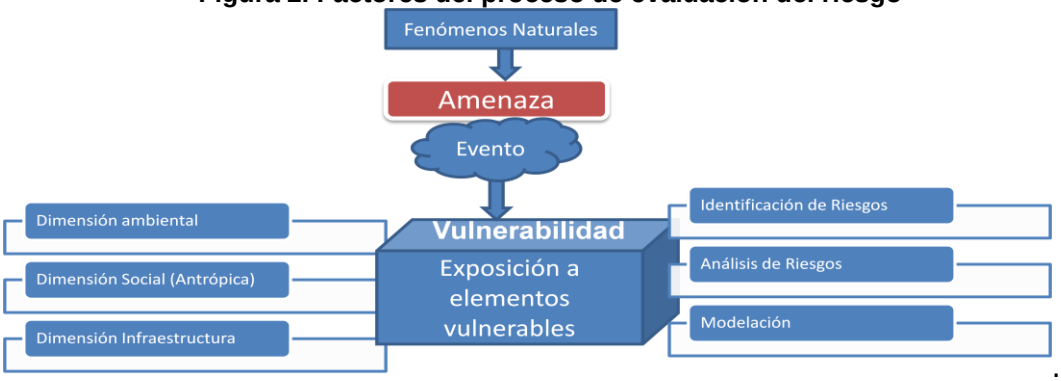
- ***Análisis de riesgos*** – Proceso de diagnóstico de la probabilidad que un riesgo identificado ocurra y su posible impacto en el servicio. Dicho análisis deber ser llevado a cabo por juicio de expertos en grupos interdisciplinarios.

- ***Mitigación del riesgo*** – Proceso que involucra el desarrollo de estrategias y acciones para administrar o mitigar el riesgo. Estas acciones deben ser estructuradas basándose en la temporalidad del evento de la amenaza, es decir, medidas de mitigación de prevención de desastres, medidas de contingencia post desastres, así como medidas que permitan operar durante la ocurrencia de un evento.

- ***Monitoreo, reporte y control de riesgos*** – Proceso metodológico iterativo para el seguimiento de los riesgos, la identificación de nuevos riesgos y su reporte, el cual propende por la ejecución de planes de acción macro sobre riesgos y la evaluación de su efectividad en la reducción de riesgo.

Esquemáticamente, en el proceso de la evaluación del riesgo se deben tener en cuenta varios factores que influyen en la calificación del mismo con el siguiente enfoque:

Figura 2. Factores del proceso de evaluación del riesgo



Fuente. CINTEL

3.2 DEFINICIÓN DE NIVELES DE ADVERSIDAD AL RIESGO

La adversidad al riesgo se puede definir como el grado de tolerancia o rechazo a convivir con un riesgo.

Para el presente estudio, la gradualidad se define por:

1. Tipo de servicio prestado

2. Porcentaje de la población afectada

3. Tiempo de recuperación de la prestación del servicio

La adversidad al riesgo adicionalmente está enmarcada en la determinación de las redes y servicios vitales de telecomunicaciones y se presenta en el capítulo 5.1 del presente estudio, donde se establece que la población colombiana necesita servicios constantes y continuos de los servicios portador, telefonía celular, TPBCL, Internet, TV, radiodifusión sonora AM y FM, servicios móviles aeronáuticos y marítimos así como las comunicaciones de emergencia.

Con base en lo anterior y bajo el entendimiento de que la sociedad actual depende en gran mediad de los servicios de telecomunicaciones, así como que estos servicios son vitales para el soporte en la prevención y atención de desastres y para otras etapas de reparación, construcción y redesarrollo de las zonas impactadas por un fenómeno natural, se determina dentro del estudio un enfoque con un alto grado de adversidad a que alguno de estos servicios falle, dado que es altamente importante el continuo funcionamiento de los servicios que soporten las redes de emergencia del país.

En conclusión y con fines modelar escenarios de análisis pesimistas, se establece que el análisis de riesgo se concentrará en que ningún elemento

de las redes vitales de telecomunicaciones a evaluar debe estar sometido a grandes amenazas naturales o caracterizarse por presentar vulnerabilidades físicas y/o funcionales altas, ***definiendo así que el estudio será explícitamente adverso a tolerar cualquier riesgo y para esto calificarán escenarios hipotéticos de ocurrencia o materialización de la amenaza natural en cada caso*.**

3.3 DEFINICIÓN DE UMBRALES DE TOLERANCIA

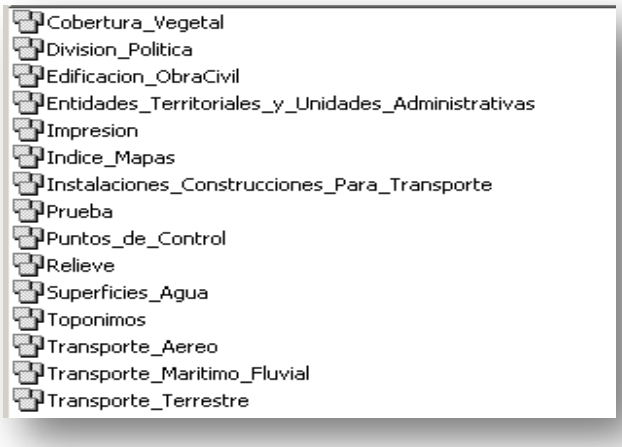
Los umbrales de tolerancia se definen para cada una de las amenazas, en el capítulo 4 Diagnóstico de Amenazas Naturales con la siguiente metodología.

- Estandarización del Sistema de Coordenadas:
    - A cada una de las capas de información recibida se le realiza un proceso de ajuste para estandarizar el sistema de proyección al sistema WGS84, mediante los procesos de conversión a MAGNA establecidos por el IGAC.
    - En el caso de no contar con información digital, se procede con la digitalización de la información y su proyección al sistema MAGNA.
    - Se define cuáles elementos de la red se representarán como punto y cuáles como polígono. Los elementos representados en áreas corresponden a aquellos tipos de servicio cuyo principal atributo es una cobertura espacial definida.
- Delimitación de la zona de estudio.
    - Se detallan las zonas específicas que presentan un grado de amenaza significativo a modelar.
    - Se establece el perímetro de influencia de la zona a analizar en diferentes escalas; se crean capas de polígonos con los valores de amenaza que servirán para los análisis espaciales de sobre posición, asignación de atributos espaciales, intersección y corte.

- Selección capas de análisis.

    - Para la información de cartografía básica se usa el modelo de datos del IGAC definido de la siguiente forma:

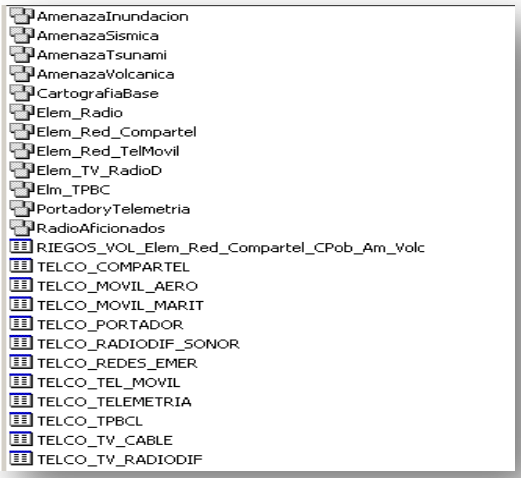
Figura 3. Modelo de datos Cartografía 1:500.000



Fuente: IGAC

    - Para la información de cartografía temática se usa el modelo de datos sugerido por CINTEL de la siguiente forma:

Figura 4. Modelo de datos CINTEL



Fuente: CINTEL

- Diagnóstico de las amenazas naturales:

    - **Amenaza Sísmica:** En función a la intensidad del sismo, la NSR-98, el mapa de intensidades y daños de INGEOMINAS/FOREC, el Plan de Ordenamiento.

    - **Volcánica:** En función del tipo de evento generado por el volcán y la clasificación de INGEOMINAS.

    - **Inundación:** En función del nivel máximo de tolerancia de soporte estimado como mayor a 20 cm, con base en zonas de inundación, rondas de los ríos y depresiones del terreno.

    - **Tsunami:** Por el nivel estimado de alarma generada y su correspondiente impacto mediante escalas de Tsunami y estado del océano.

- Diagnóstico de las vulnerabilidades:
    - Los umbrales de tolerancia se definen para cada una de las vulnerabilidades a las que están sometidas los siguientes elementos:
        - Edificaciones
        - Armarios / Gabinetes
        - Torres / Antenas
        - Redes Aéreas Fibra Óptica
        - Redes Aéreas de Cobre
        - Redes Subterráneas (Canalización /Ductos) de Cobre
        - Redes Subterráneas (Canalización /Ductos) de Fibra Óptica

Finalmente el resultado del factor Riesgo = Amenaza X Vulnerabilidad se categoriza manera específica para cada tipo de servicio, donde el máximo valor de Alto corresponde al mayor valor encontrado en la simulación del modelo de acuerdo con nivel de adversidad definido previamente en el numeral 3.2 del presente documento.

Alto	**Daños generados sobre los elementos físicos y funcionales de cada red**
Medio	**Daños menores indirectos a algunos elementos de la red**
Bajo	**Sin daños o que no afectan la correcta funcionalidad del elemento de cada red**

3.4 DEFINICIÓN DEL UNIVERSO DE RIESGOS

Para definir el universo de riesgos se establece y se detalla con precisión las áreas por el tipo de amenaza natural identificada por las autoridades para la zona de estudio, así como la recopilación de todos los elementos de la red ubicados en dichas zonas.

Este proceso se realiza mediante el diagnóstico de la recopilación, depuración y montaje de un sistema georreferenciado de consulta de la información sobre cada una de las amenazas naturales en Colombia con la información recibida por las instituciones encargadas.

Posteriormente, el modelo contempla la ejecución de una sobre posición de todas las capas de información recibidas sobe la temática de amenaza natural para cada fenómeno estudiado, sobre las capas de todos los elementos de la red de cada servicio de telecomunicaciones identificado y entregado por cada una de las entidades para este estudio.

Dicha sobre posición determina y selecciona cuáles elementos de la red analizada están realmente amenazados por fenómeno natural. Dicho proceso debe ser realizado de la siguiente manera:

- Establecimiento de los elementos de red que tienen una cobertura de afectación claramente definida, como la cobertura de los elementos de telefonía móvil en cada una de las tecnologías.
- Realización de la unión de capas que delimitan cada fenómeno natural, con el fin de tener una cobertura general que agrupe las amenazas específicas.

  - Amenaza sísmica. Se realizó una unión espacial de las capas de daños e intensidades extraídas de los mapas de amenaza sísmica proporcionados por INGEOMINAS, obteniendo una cobertura que

determina claramente las zonas que presentan una gradualidad de alta a baja de amenaza sísmica específica para la ciudad de Armenia.

- Amenaza Volcánica. Se realizó una unión espacial de todos los tipos de amenaza volcánica por lahares, piroclastos, cenizas y proyectiles extraídas de los mapas de este tipo proporcionados por INGEOMINAS, obteniendo una cobertura única que identifica claramente el tipo de amenaza al cual estaría expuesto cada elemento de la red de telecomunicaciones.
- Amenaza por Tsunami. Se realizó una unión espacial de todos los tipos de amenaza por Tsunami estimada para la cuidad de Tumaco con foco en fenómenos como licuación, golpe de ola e inundación salobre, extraídas de los mapas proporcionados por el OSSO la Alcaldía de Tumaco y otras entidades de prevención y atención de desastres.
- Amenaza por Inundación. Con base en la información reciente de las inundaciones ocurridas en Colombia en el 2010, se procedió a elaborar un mapa de inundación propia con los siguientes parámetros:

    i. Establecimiento de rondas de ríos de un kilómetro a lado y lado de la línea que representa este tipo de elemento hidrográfico en la cartografía del IGAC escala 1:500.000, las cuales fueron clasificadas como zonas de amenaza por inundación alta.

    ii. Establecimiento de rondas de lagos y lagunas de un kilómetro a lado y lado del polígono que representa este tipo de elemento hidrográfico en la cartografía del IGAC escala 1:500.000, las cuales fueron clasificadas como zonas de amenaza por inundación alta.

iii. Establecimiento de una cota media para la Mojana Sucreña de 25 metros sobre el nivel del mar de todos los cuerpos de agua identificados en la cartografía del IGAC escala 1:500.000. El modelo digital del terreno usado es el SRTM[8] de 90 metros de la Nasa.

iv. Análisis de zonas por debajo de la cota media de elevación de los ríos establecida mediante cálculos algebraicos de extracción y clasificación de los pixeles del SRTM de la siguiente forma:

1. Menores que 0 metros y hasta 15 metros sobre el nivel del mar, clasificados como amenaza por inundación alta.

2. Mayores que 16 metros y hasta 25 metros sobre el nivel del mar, definidos como amenaza por inundación media.

3. Mayores que 25 metros sobre el nivel del mar, definidos como amenaza por inundación baja o nula.

[8] Shuttle Radar Topography Mission (SRTM). Farr, T. G., et al. (2007), The Shuttle Radar Topography Mission, Rev. Geophys., 45, RG2004, doi:10.1029/2005RG000183. http://www2.jpl.nasa.gov/srtm/srtmBibliography.html

v. Con base en los datos obtenidos por los ítems i al iv se realizó la unión de todas las capas obteniendo una única capa de información que contiene el estimado de las áreas de amenaza por inundación para la zona de la Mojana Sucreña.

- Identificación de todos los elementos físicos y funcionales que hacen parte de la de la red de telecomunicaciones que por servicio se va a modelar. Se debe realizar una estandarización de los campos a utilizar.
- Georreferenciación de todos los elementos físicos de la red de telecomunicaciones que por servicio se va a modelar en el sistema MAGNA-SIRGAS (WGS-84) definido por el IGAC para Colombia.
- Extracción de todos los elementos de red que pueden estar afectados por cada una de las amenazas naturales mediante procesos de análisis espacial propios de un SIG.
- Asignación espacial de los atributos de amenaza, contenidos en las coberturas que se unieron previamente por cada tipo de fenómeno natural, a cada uno de los elementos de la red de telecomunicaciones que por servicio se va a modelar.
- Recopilación de todos los elementos de red que están sometidos a un determinado tipo de amenaza e identificación de aquellos que no están sometidos a ningún tipo de amenaza.

Por último, las capas de información establecidas por cada uno de los servicios de telecomunicaciones estudiados, TPBC, Telefonía Móvil, Radioaficionados, Compartel, Telemetría, Portador etc. que se encuentran en las zonas de amenaza del estudio conforman en su totalidad el universo de riesgos que se merecen una análisis en términos

de impacto al servicio prestado en función de su vulnerabilidad física y funcional determinada en el capítulo *5. Diagnóstico de vulnerabilidad de redes básicas de telecomunicaciones.*

3.5 IDENTIFICACIÓN DE RIESGOS MODELO

Este proceso surge de la sobre posición espacial de la información de amenaza y vulnerabilidad arrojando un listado sin priorizar con todos los riesgos detectados. Dicha lista puede surgir del proceso de selección del universo de riesgos descrito en el numeral 3.4 del presente documento. Sin embargo y, dado que el modelo define realizar una serie de etapas predeterminadas para garantizar una correcta Gestión del Riesgo, los pasos para realizar la identificación de los riesgos se pueden determinar de la siguiente manera:

1. Selección de los servicios y la infraestructura vital de telecomunicaciones.
2. Identificación de todos los elementos de red para cada uno de los servicios e infraestructura seleccionada.
3. Definición de los operadores y estandarización de la información a solicitar.
4. Diagnóstico detallado de las zonas de amenaza del estudio.
5. Diagnóstico detallado de la vulnerabilidad de los elementos de la red.
6. Recopilación de la información, homogenización, depuración y estructuración de una base de datos espacial.
7. Estructuración de las capas de información para análisis espacial.
8. Georreferenciación de las amenazas naturales y otra información asociada.

9. Análisis espacial y extracción de los elementos de red sometidos a cada amenaza.

10. Identificación de la exposición de cada elemento a determinado tipo de amenaza.

11. Identificación y consolidación de los elementos expuestos a amenazas.

12. Identificación de la vulnerabilidad de todos los elementos de cada uno de los servicios y asignación de su probabilidad de daño con base en el peor escenario.

En esta etapa, el resultado obtenido es una lista completa de todos los elementos que están sometidos a un tipo de amenaza con su respectiva vulnerabilidad a la misma. Este listado debe tener toda la información del tipo de amenaza, la población afectada, el municipio en el cual se encuentra el elemento, las coordenadas y toda la información específica de cada elemento de red incluidos los sistemas de soporte y respaldo, entre otros.

3.6 CALIFICACIÓN DE AMENAZAS POR VULNERABILIDADES Y SU PRIORIZACIÓN

Los riesgos son calificados en función de la probabilidad de ocurrencia de la amenaza natural descrita en detalle en el capítulo 4 del presente documento y el impacto que dicha amenaza puede ocasionarle al elemento. Estos valores son multiplicados por la vulnerabilidad de cada elemento ante cada tipo de amenaza descritos en detalle en el capítulo 5 del presente documento.

Esta etapa define el valor absoluto del riesgo arrojando como resultado cuáles elementos de red están realmente expuestos, representados como riesgos bajos, medios y altos.

El valor resultante de la calificación de las amenazas por las vulnerabilidades determina las razones por las cuales un elemento se encuentra en riesgo, donde se puede concluir que los riesgos se pueden priorizar con base en los siguientes escenarios y todas sus otras posibles combinaciones:

a. Un riesgo puede tener una **alta amenaza** pero contar con una **baja vulnerabilidad**, lo que puede determinar que **el riesgo es bajo.**

b. Un riesgo puede tener una **alta amenaza** pero contar con una **mediana vulnerabilidad**, lo que puede determinar que el **riesgo es medio.**

c. Un riesgo puede tener una **alta amenaza** y contar con una **alta vulnerabilidad**, lo que puede determinar que el **riesgo es alto.**

d. Un riesgo puede tener una **baja amenaza** y contar con una **alta vulnerabilidad**, lo que puede determinar que el **riesgo es alto.**

e. Un riesgo puede tener una **baja amenaza** pero contar con una **mediana vulnerabilidad**, lo que puede determinar que el **riesgo es medio.**

f. Un riesgo puede tener una **baja amenaza** pero contar con una **alta vulnerabilidad**, lo que puede determinar que el **riesgo es alto.**

Para efectos del cálculo del modelo se toma el peor escenario, es decir una afectación del 100% del elemento por la amenaza, en otras palabras la materialización u ocurrencia de un evento natural (amenaza altas) sobre un elemento de la red.

Los riesgos son priorizados de altos a bajos de manera que se establece cuáles son los elementos de la red por tipo de servicio que pueden presentar mayor impacto sobre la prestación del servicio en una zona determinada.

3.7 ESCENARIOS BASADOS EN ESCENARIOS HIPOTÉTICOS

Con el fin de establecer políticas y procedimientos enfocados a una adecuada gestión del riesgo ante amenazas naturales, es necesario que se incluya en el proceso escenarios hipotéticos de ocurrencia del evento con el fin de establecer políticas de prevención adecuadas antes y después de la ocurrencia de un desastre.

Estos escenarios hipotéticos son determinados por las características de la amenaza natural de la siguiente manera:

Amenaza Volcánica - Determinada por las fases eruptivas del Volcán.

Amenaza Sísmica - Determinada por probabilidades estimadas de ocurrencia de un sismo dada una eventual magnitud.

Amenaza por Tsunami - Determinada por las escalas SIEBERG de intensidades de Tsunamis y/o DOUGLAS que describe los de estados del Océano.

Amenaza por Inundación - Determinada por el aumento de la media anual por mes de la pluviosidad en la zona de estudio.

El presente modelo incluye la variable por fase de la amenaza que se puede modificar para obtener diferentes resultados, sin embargo, para efectos del cálculo del modelo se toma el peor escenario, es decir una afectación del 100% del elemento por la amenaza, en otras palabras la materialización o ocurrencia de un evento natural sobre un elemento de la red.

3.8 TABLAS DE RIESGO

Como resultado de las interacciones se obtienen tablas de resultados agregadas por cada uno de los servicios de telecomunicaciones y por el tipo de amenaza natural de la siguiente manera.

Amenaza Sísmica

- Tablas de Amenaza Sísmica para la Red Compartel
- Tablas de Amenaza Sísmica Red TPBC
- Tablas de Amenaza Sísmica Red Telefonía Móvil
- Tablas de Amenaza Sísmica Red Televisión Radio Difundida
- Tablas de Amenaza Sísmica Red de Radiodifusión Sonora
- Tablas de Amenaza Sísmica Portador
- Tablas de Amenaza Sísmica Telemetría
- Tablas de Amenaza Sísmica Red Radioaficionados

Amenaza Volcánica

- Tablas de Amenaza Volcánica para la Red Compartel
- Tablas de Amenaza Volcánica Red TPBC
- Tablas de Amenaza Volcánica Red Telefonía Móvil
- Tablas de Amenaza Volcánica Red Televisión Radio Difundida
- Tablas de Amenaza Volcánica Red de Radiodifusión Sonora

- Tablas de Amenaza Volcánica Portador
- Tablas de Amenaza Volcánica Telemetría
- Tablas de Amenaza Volcánica Red Radioaficionados

Amenaza Tsunami

- Tablas de Amenaza Tsunami para la Red Compartel
- Tablas de Amenaza Tsunami Red TPBC
- Tablas de Amenaza Tsunami Red Telefonía Móvil
- Tablas de Amenaza Tsunami Red Televisión Radio Difundida
- Tablas de Amenaza Tsunami Red de Radiodifusión Sonora
- Tablas de Amenaza Tsunami Portador
- Tablas de Amenaza Tsunami Telemetría

Amenaza Inundación

- Tablas de Amenaza Inundación para la Red Compartel
- Tablas de Amenaza Inundación Red TPBC
- Tablas de Amenaza Inundación Red Telefonía Móvil
- Tablas de Amenaza Inundación Red Televisión Radio Difundida
- Tablas de Amenaza Inundación Red de Radiodifusión Sonora
- Tablas de Amenaza Inundación Portador

- Tablas de Amenaza Inundación Telemetría
- Tablas de Amenaza Inundación Red Radioaficionados

Los resultados de estas tablas se presentan detallados en el capítulo de 7 Aplicación del modelo en las zonas y para las amenazas definidas.

3.9 DEFINICIÓN DE LOS CRITERIOS DE IMPACTO VS RELEVANCIA DE IMPACTO

En este paso se definen los criterios de impacto observados y se evalúa la relevancia del impacto sobre los niveles de servicio prestados en la zona con el fin de establecer las medidas de mitigación y contingencia, guardando el justo balance del costo beneficio de ejecutarlos.

Se debe prestar especial atención a los costos asociados a la ejecución de los planes de mitigación contra los beneficios cuantitativos y cualitativos de la prestación del servicio.

3.10 DESCRIPCIÓN DEL MODELO AJUSTADO

El modelo se ha plasmado en una base de datos geográfica que contiene toda la información recopilada de las entidades gubernamentales así como de los operadores de la infraestructura de telecomunicaciones para la zona de estudio.

Para la ejecución de las actividades descritas en el modelo se realizaron varios pasos de análisis espacial, mediante el uso de herramientas SIG, sobreponiendo las amenazas, las vulnerabilidades y la infraestructura, validando la exposición de ésta con el siguiente enfoque:

Toda la información obtenida es georreferenciada y convertida al sistema MAGNA definido por el IGAC.

3.11 DESCRIPCIÓN DE LA USABILIDAD DEL MODELO Y GUÍAS DE USO

Para ejecutar el modelo por una entidad gubernamental o un operador de la infraestructura de telecomunicaciones, se deben seguir los pasos descritos en este capítulo.

- **Definición de niveles de adversidad al riesgo:** Se definen cuáles son los mínimos y máximos tolerables del valor del riesgo de la prestación del servicio en una zona determinada.
- **Definición de umbrales de tolerancia:** Se definen y establecen los umbrales de amenaza natural con los cuales es posible convivir, así como los de la vulnerabilidad de la infraestructura, en el sentido de lo que ésta pueda soportar ante impactos por eventos naturales.

  Se hace necesario detallar los niveles de la vulnerabilidad física y funcional para cada elemento de acuerdo con lo descrito en el capítulo correspondiente de este documento.
- **Definición del universo de riesgos:** Se determina el conjunto de los riesgos que están sometidos a amenaza natural y que tienen un grado de vulnerabilidad tal que se puedan ver afectados.
- **Identificación de riesgos:** Se prepara la información cartográfica mediante la representación de las amenazas naturales, la hidrografía, vías de acceso, los centros poblados y sus habitantes, el modelo digital del terreno, entre otros en un sistema de información que permita el análisis espacial.

  Posteriormente se verifica que el sistema de coordenadas de todos los elementos se encuentren en el mismo sistema de coordenadas, se

recomienda usar el procedimiento de conversión al sistema MAGNA sugerido por el IGAC.

Una vez realizados los ajustes anteriores, se extraen todos los elementos de la red que están sometidos a cada una de las amenazas mediante procesos de unión espacial, intersección y extracción.

- **Determinación de probabilidades de ocurrencia:** Se determinan las probabilidades de ocurrencia del evento ocasionado por una amenaza natural con base en los históricos generados por las entidades gubernamentales del sector y se establecen estimados de ocurrencia. En las etapas de planeación de la respuesta a los riesgos, se recomienda que el operador determine probabilidades de ocurrencia cercanas al 100% para evaluar los posibles efectos sobre la infraestructura y tomar medidas preventivas.

  Por otro lado, se determinan las probabilidades de ocurrencia de daños si el evento de la amenaza natural se materializa. Es decir, se evalúa el valor de la vulnerabilidad física y funcional de los elementos tomando el peor escenario de impacto directo sobre cada elemento en particular.

- **Determinación de impactos:** Se establece claramente cuál es el impacto que puede generar que un elemento determinado deje de prestar el servicio en una zona definida. Se debe tener en cuenta todos los costos asociados al impacto y los planes de mitigación y contingencia que se deben ejecutar para minimizar el impacto. Es importante determinar adicionalmente el impacto que puede generar la prestación o no del servicio durante y después de la ocurrencia de un desastre natural, así como la capacidad de recuperación ante el

mismo. Es importante realizar la simulación del valor del riesgo al que está sometida la infraestructura con énfasis en la prevención, es decir desde la planeación de la red que presta un servicio específico.

- **Calificación de riesgos de acuerdo con la probabilidad e impacto:** Una vez realizados los cálculos de probabilidad y de impactos se procede a realizar los estimados de la función Riesgo = Amenaza X Vulnerabilidad, que establece el valor del riesgo en alto, medio y bajo definido por los máximos y los mínimos por cada servicio
- **Priorización de riesgos del modelo:** La lista de riesgos en la tabla de los mismos es priorizada y catalogada de acuerdo con su nivel alto, medio y bajo con el fin de establecer cuales riesgos deben ser atendidos con mayor celeridad, ya sea para acciones preventivas o de contingencia.
- **Aproximación a las acciones de mitigación:** Sobre los riesgos de más alta calificación se establecen planes concretos de mitigación y contingencia, de acuerdo con las políticas de cada operador y/o entidad gubernamental con el fin de acoplarlos a los programas de la organización.
- **Generación de un mapa de riesgos:** Con los planes de mitigación y contingencia sobre los riesgos priorizados se establecen mapas de riesgo sobre los cuales se debe concentrar la gestión. Las organizaciones deben velar porque este mapa de riesgos sea de carácter público así como que la mayoría de ellos se encuentren en niveles bajos o medios.
- **Ejecución de actividades de monitoreo y control de riesgos:** Las organizaciones deben involucrar en sus políticas, sistemas de gestión integral del riesgo y las buenas prácticas a implementar cada año,

recopilando las lecciones aprendidas de la ejecución de los períodos anteriores. Se recomienda establecer grupos interdisciplinarios que ejecuten seguimientos sistemáticos y programados en conjunto con las entidades del estado correspondientes, sobre la ejecución de los planes de gestión del riesgo sobre la amenaza natural a la que está sometida la infraestructura de telecomunicaciones en Colombia.

4 DIAGNÓSTICO DE AMENAZAS NATURALES

En este capítulo se presentan las generalidades del diagnóstico realizado de las amenazas naturales definidas para el estudio, empezando por la definición de los conceptos a utilizar, la delimitación de las zonas de análisis y el diagnóstico de cada tipo de amenaza natural en la zona de estudio definida para la misma.

El diagnóstico de cada tipo de amenaza comprende la caracterización de la zona de estudio, sus generalidades socio económicas y políticas, la valoración de la amenaza y la priorización y zonificación de la amenaza.

4.1 GENERALIDADES

La amenaza natural se puede subdividir o clasificar dependiendo del fenómeno que la crea. Desde el aspecto atmosférico, se pueden generar tipos de amenaza por tornados, incendios, tormentas, rayos, granizo entre otros; desde el aspecto hidrológico se pueden generar tipos de amenaza por inundaciones, erosión, derrumbes y sequías entre otros y, desde el aspecto geológico se pueden generar tipos de amenaza por sismos, que a su vez pueden generar otros fenómenos como la licuefacción, los derrumbes y los tsunamis. El aspecto geológico también genera otros tipos de amenaza por eventos volcánicos que a su vez, pueden generar otros fenómenos como cenizas, proyectiles, gases tóxicos, flujos de lava, lodo y piroclastos.

Los anteriores elementos, que conforman en su conjunto una amenaza natural, pueden estar interrelacionados y normalmente la ocurrencia de uno puede generar otro o potencializar la ocurrencia de varios fenómenos en una zona.

Los niveles de amenaza natural a los que está expuesta una zona particular, suelen ser diferentes a los rangos de medida que se usan para determinar la intensidad o impacto de los mismos. A manera de ejemplo, se observa que en el caso de amenaza sísmica la escala más usada es la escala de Richter que indica la magnitud del evento. Sin embargo, ésta no hace referencia a la amenaza a la que puede estar expuesta una población por la ocurrencia de un sismo.

4.1.1 DEFINICIONES DE AMENAZA NATURAL

Con base en lo descrito anteriormente, a continuación de se detallará la definición de las amenazas por sismos, volcanes, tsunami e inundación.

4.1.1.1 Amenaza Sísmica

La ocurrencia de un sismo se puede dar por múltiples razones y a la fecha no se puede determinar con precisión cómo y cuándo ocurrirá. La sismología es la rama de la geología que estudia las causas y consecuencias de la ocurrencia los sismos en el planeta.

Los sismos ocurren todo el tiempo y se pueden originar por:

- Movimientos de placas continentales
- Movimientos generados por fallas geológicas
- Procesos volcánicos
- Causas atribuibles al hombre como construcción de represas y explosiones

Las consecuencias que pueden traer los sismos para la infraestructura de telecomunicaciones se pueden clasificar en:

- Licuefacción, hundimiento de la infraestructura de soporte de telecomunicaciones
- Deslizamientos que ocasionen caída de torres en cerros
- Colapsos de edificaciones
- Taponamiento de vías de acceso
- Derrumbe de puentes

Sin embargo, las consecuencias de los riesgos no siempre son catastróficas y dependen de los lugares de ocurrencia.

La amenaza sísmica difiere del riesgo sísmico en varios aspectos. De acuerdo con el ITC[9], la amenaza sísmica se describe como el potencial de daño que pueden ocasionar fenómenos naturales, como los movimientos telúricos, las fisuras del suelo o la licuefacción, sobre los intereses de la sociedad desde la destrucción de la infraestructura hasta la pérdida de vidas.

Igualmente, el ITC[10] describe que el riesgo sísmico es la probabilidad de ocurrencia de las consecuencias adversas generadas por la amenaza.

4.1.1.2 Amenaza Volcánica

La amenaza que genera un volcán ubicado en una zona específica depende del tipo de volcán, de las condiciones geomorfológicas del terreno, de la población asentada en la zona de influencia, de la rosa de los vientos, así como de la historia registrada del volcán.

Existen diversos tipos de volcán, los cuales pueden generar diferentes tipos de amenaza. Según el USGS[11], aunque un volcán no esté en proceso eruptivo, las clases de peligro pueden ser:

- Columnas y nubes eruptivas (gases, proyectiles, cenizas)
- Gases volcánicos (lluvia ácida, gases tóxicos)
- Flujos y domos de lava (difieren en velocidad de movimiento)

---

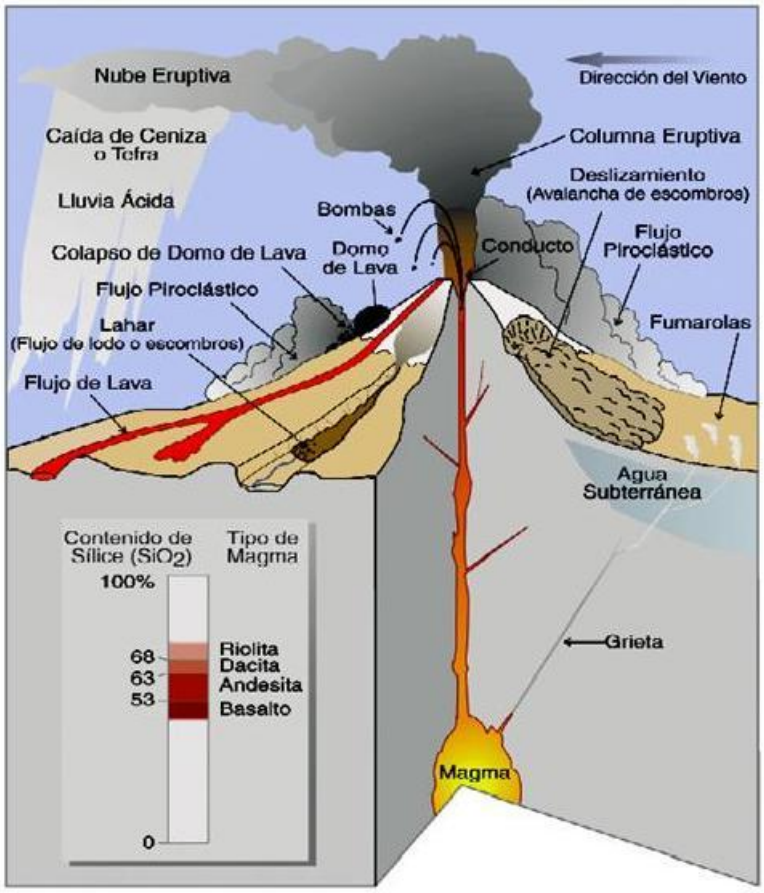
[9] ITC (International Institute for Aerospace Survey and Earth Sciences). Earthquake Hazard Analysis. 1996. Pag 1

[10] Idem.

[11] USGS Fact Sheet 144–00, octubre 2000. (http://pubs.usgs.gov/fs/fs144-00/fs144-00.pdf)

- Flujos piroclásticos (flujos calientes de ceniza a alta velocidad)
- Deslizamientos (avalanchas de escombros)
- Lahares (flujos de lodo y escombros)

Figura 5. Tipos de volcanes



Fuente (USGS, 2000)

Independientemente del tipo de volcán, éstos pueden generar diferentes amenazas para la infraestructura de telecomunicaciones, dependiendo del tipo de elemento que arroje el volcán hacia las edificaciones. El tipo de amenaza que puede generar un volcán para esta infraestructura puede ser:

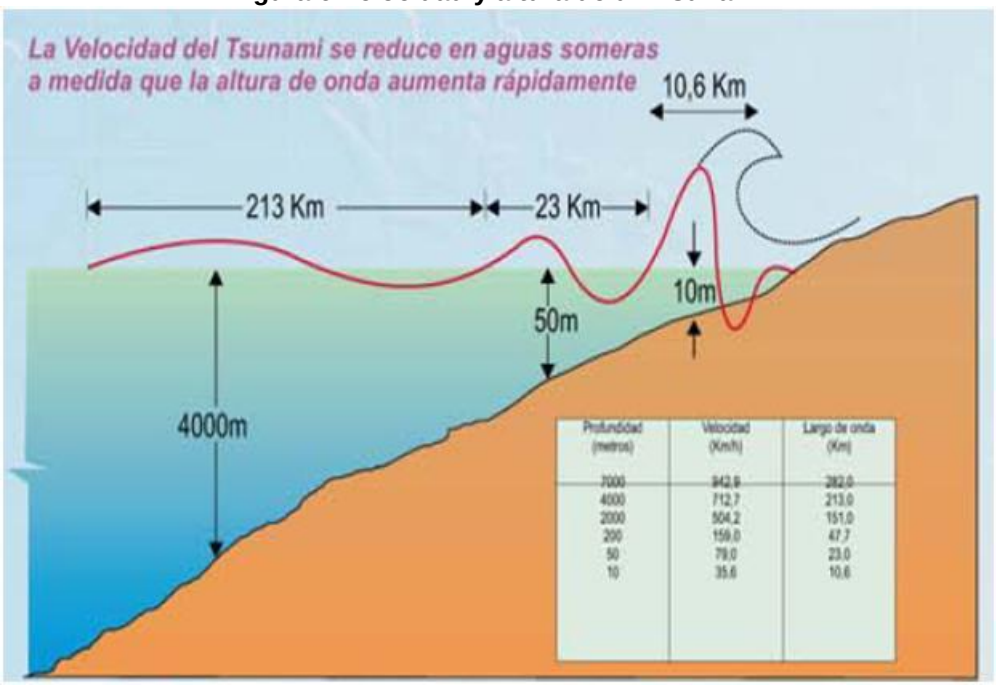
- Flujo de cenizas, taponamiento de ventilación, colapso de cubiertas por peso, material granulado que impide la propagación.
- Flujo de piroclastos, proyectiles que impacten directamente la infraestructura, incendios o destrucción total.
- Flujo de lodos y avalanchas que destruyan la infraestructura y deslizamientos de masa que afecten la ubicación de las torres.
- Flujo de lava, derretimiento de cimientos de torres y otra infraestructura.
- Sismos que provoquen desalineamiento de la infraestructura de telecomunicaciones.
- Vapores tóxicos que impidan el acceso para mantenimiento.

4.1.1.3 Amenaza por tsunami

Los tsunamis o maremotos son olas de gran tamaño que impactan con gran fuerza las costas de los continentes y las islas. Estas olas son creadas generalmente por la ocurrencia de sismos de gran magnitud como resultado de la confluencia de dos placas tectónicas. Sin embargo, los maremotos pueden ser ocasionados por otros fenómenos por impactos directos en el mar como meteoritos, o como consecuencia de eventos volcánicos como proyectiles de gran tamaño, sismos o grandes desprendimientos de masa. Los rompimientos del hielo polar pueden ocasionar maremotos de menor intensidad. La velocidad de un tsunami depende directamente de la profundidad del océano y la altura de la ola es inversamente proporcional a la profundidad.

La Real Academia de la Lengua define tsunami como *"Ola gigantesca producida por un sismo o una erupción volcánica en el fondo del mar".*

Figura 6 Velocidad y altura de un Tsunami



Fuente UNESCO

Existen diversos tipos de amenaza que pueden generar un tsunami, las cuales se pueden resumir en:

- Impacto por ola rompiente y destrucción de la infraestructura de telecomunicaciones.
- Inundaciones y daños en equipos ubicados en plantas bajas.
- Desestabilización de estructuras por erosión.

El riesgo por tsunami al que está expuesta la infraestructura de telecomunicaciones en una zona determinada, es determinado por el factor de la amenaza de tsunami identificado por diferentes modelos globales, por la vulnerabilidad ante impactos de objetos, inundaciones y bloqueo de vías de acceso.

Figura 7 Modelo de propagación de un tsunami en el Pacífico sudeste, nueve horas después de su generación

Fuente: Antofagasta, Chile (30 de julio de 1995). Cortesía de LDG, Francia."[12]

4.1.1.4 Amenaza por Inundación

Las causas y consecuencias de las inundaciones se determinan normalmente por la zona de estudio y normalmente se asocian a condiciones hidrológicas extremas como lluvia excesiva, tsunamis, saturación del suelo o fallas de la infraestructura como diques o represas. Cuando una zona determinada que permanece seca durante la mayor parte del año se cubre de agua, se considera que está inundada.

Normalmente, los tipos de inundación se pueden dar por:

- Desbordamientos de ríos y quebradas
- Deshielos

12 UNESCO-IOC.Tsunami Glossary.IOC Information document No. 1221. Paris, UNESCO, 2006.

- Tsunamis

El tipo de amenaza que puede generar una inundación para la infraestructura de telecomunicaciones es:

- Daños por corto circuito en los componentes electrónicos
- Daños en el sistema de accesos viales y puentes
- Filtraciones de agua en los cimientos

4.1.2 Definiciones de amenaza, riesgo, vulnerabilidad y exposición

4.1.2.1 Amenaza

Una amenaza natural se puede definir como aquellos eventos o fenómenos naturales que impactan de manera negativa los intereses socio-económicos de una población determinada. Para el estudio en cuestión se define como amenaza aquellos eventos naturales que pueden impactar la correcta operación de la infraestructura de telecomunicaciones.

4.1.2.2 Riesgo

Enmarcado en el presente estudio, un riesgo se puede definir como una circunstancia incierta ocasionada por una amenaza natural que puede afectar la correcta operación de la infraestructura de telecomunicaciones. Los riesgos se pueden mantener en estado latente hasta que se genera un evento que impide la normal operación de un servicio de comunicaciones.

4.1.2.3 Vulnerabilidad

La vulnerabilidad se puede definir como la capacidad que tiene un elemento de resistir los efectos y consecuencias de un fenómeno natural ante la

materialización de un riesgo y que impide la normal operación de un servicio de comunicaciones.

4.1.2.4 Exposición

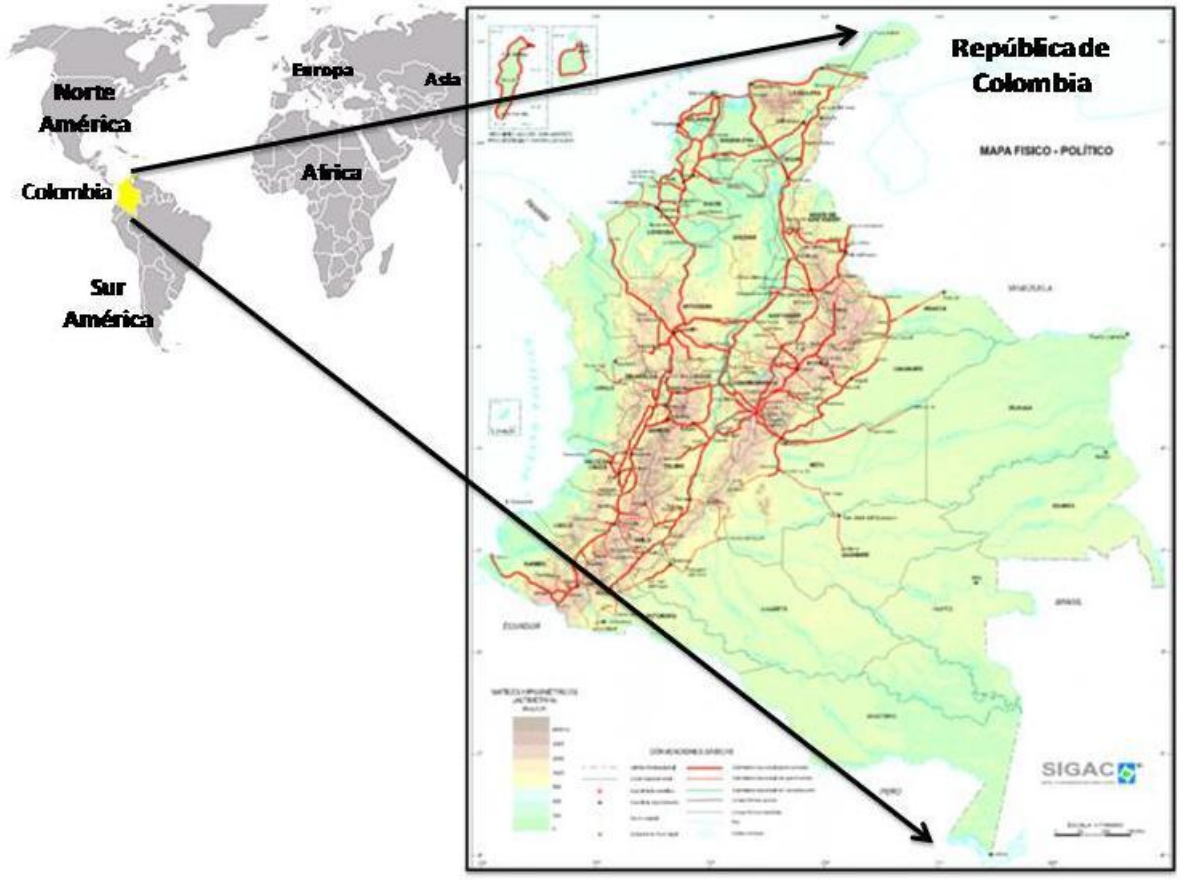
La exposición se puede definir como el factor de la vulnerabilidad por la amenaza. Adicionalmente, la exposición puede estar determinada por la probabilidad de ocurrencia de la amenaza en el tiempo. Puede ser usada para ajustar el grado o nivel del riesgo al que de un elemento de la infraestructura de telecomunicaciones puede estar expuesto.

4.1.3 Delimitación general de la zona de estudio

4.1.3.1 Contexto general de la República de Colombia

La República de Colombia se encuentra ubicada al nororiente del continente Sur Americano; limita al norte con Panamá, Costa Rica, Nicaragua, Honduras, Jamaica, Haití, República Dominicana, al oriente con Venezuela y Brasil, al sur con Perú y Ecuador.

Figura 8 Mapa Físico de Colombia



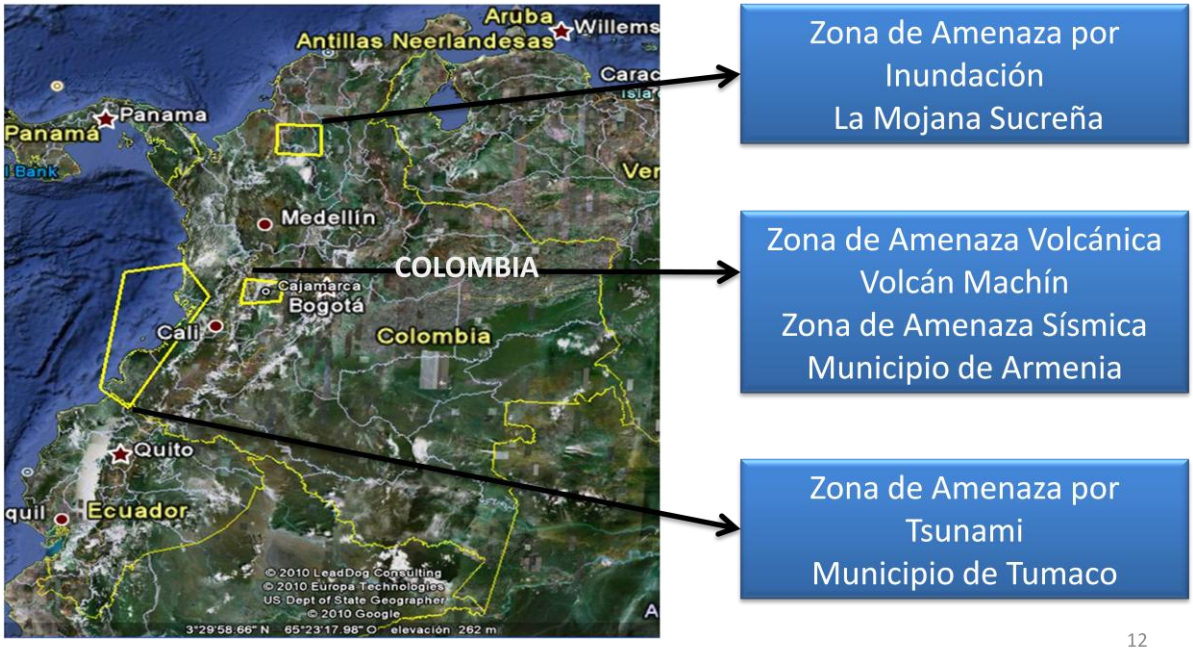
Fuente: IGAC

Desde el punto de vista geológico, Colombia se encuentra ubicada en una zona de confluencia de placas tectónicas como lo son la suramericana, la del Caribe y la de Nazca, confluencia que en parte ha formado la cadena montañosa andina dividida en Colombia por tres cordilleras: Occidental, Central y Oriental; entre estas cordilleras existen dos valles importantes que son el del Río Cauca y el del Río Magdalena. Con respecto a la zona de estudio por amenaza por inundación, ésta se encuentra ubicada cerca del Río Cauca, sobre la terminación de la cordillera central, al sur del departamento de Sucre.

Las principales ciudades de Colombia se encuentran dentro de estas cordilleras a excepción de Barranquilla que se encuentra en la Costa Caribe; Armenia, una de las ciudades objeto del estudio por amenaza sísmica, se encuentra en las laderas occidentales de la Cordillera Central la cual a su vez contiene la cadena más importante de volcanes de Colombia como el Nevado del Ruiz, del Huila, Tolima y el Volcán Machín.

4.1.3.2 Ubicación de las zonas de estudio en Colombia

Figura 9 Ubicación general de las zonas de estudio



Fuente: Google Earth, CINTEL

4.2 DIAGNÓSTICO DE AMENAZA SÍSMICA: QUINDÍO, ARMENIA

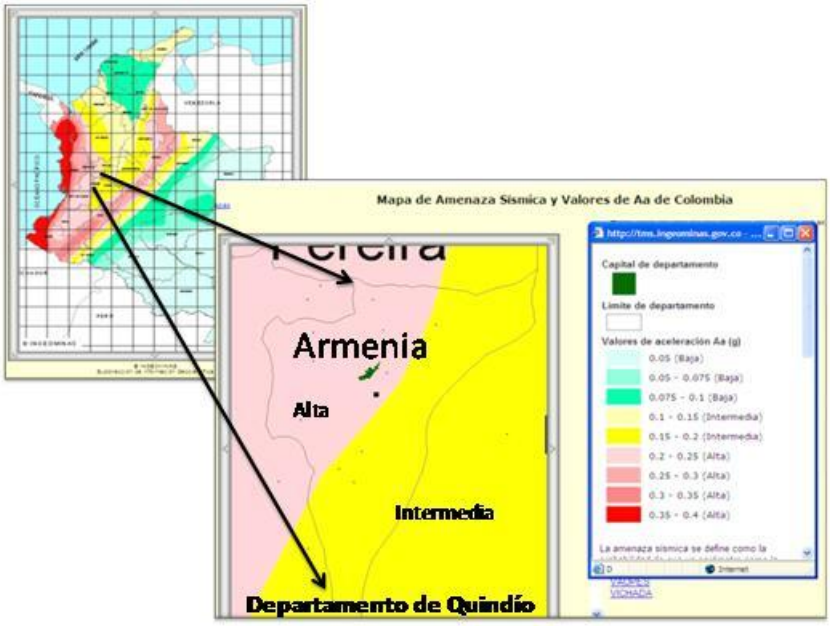
4.2.1 Delimitación de la zona de estudio

Con el efecto de tener un área de cubrimiento general de toda la infraestructura de telecomunicaciones, se estableció un área mayor que el perímetro urbano de la ciudad de Armenia. Sin embargo, el estudio detallado se realizará sobre la ciudad.

De otro lado, cabe detallar que la zona de estudio por amenaza sísmica está contenida dentro de la zona de estudio por amenaza volcánica originada por caída de cenizas y, eventualmente por actividad sísmica que pueda afectar la infraestructura de telecomunicaciones para la ciudad de Armenia, desencadenada por la actividad volcánica.

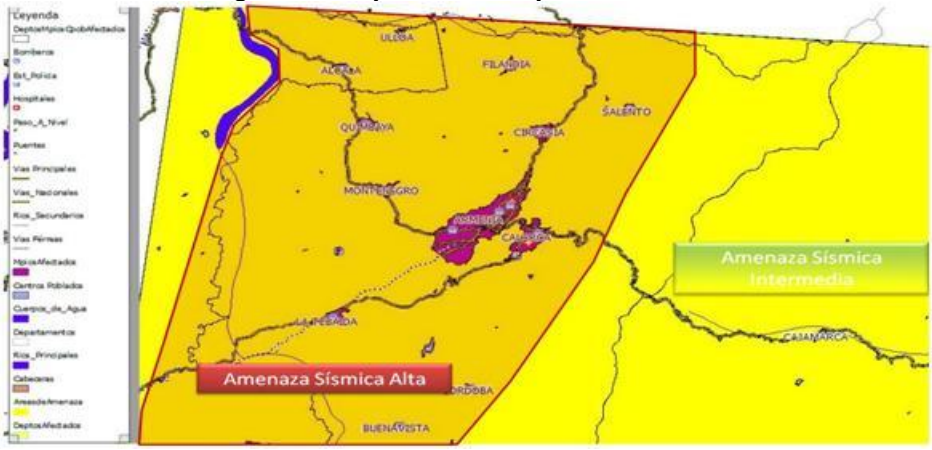
El mapa de amenaza sísmica general para el departamento de Quindío abarca varios municipios a los que se les define con el tipo de amenaza alta. En el estudio se utiliza la microzonificación sísmica de la ciudad de Armenia, entregada por INGEOMINAS, el cual recopila información del FOREC sobre el sismo de 1999. Estos estudios se encuentran plasmados en mapas georreferenciados sobre los cuales se identifica detalladamente la amenaza sísmica, la cual es sobre puesta contra la información de la vulnerabilidad de la infraestructura de telecomunicaciones estimada por CINTEL con la información recibida por los diferentes operadores. Dicha sobre posición fue realizada mediante el uso de herramientas de sistemas de información geográfica.

Figura 10 Mapa General de Amenaza Sísmica Departamento de Quindío.



Fuente: INGEOMINAS

Figura 11 Mapa de municipios afectados

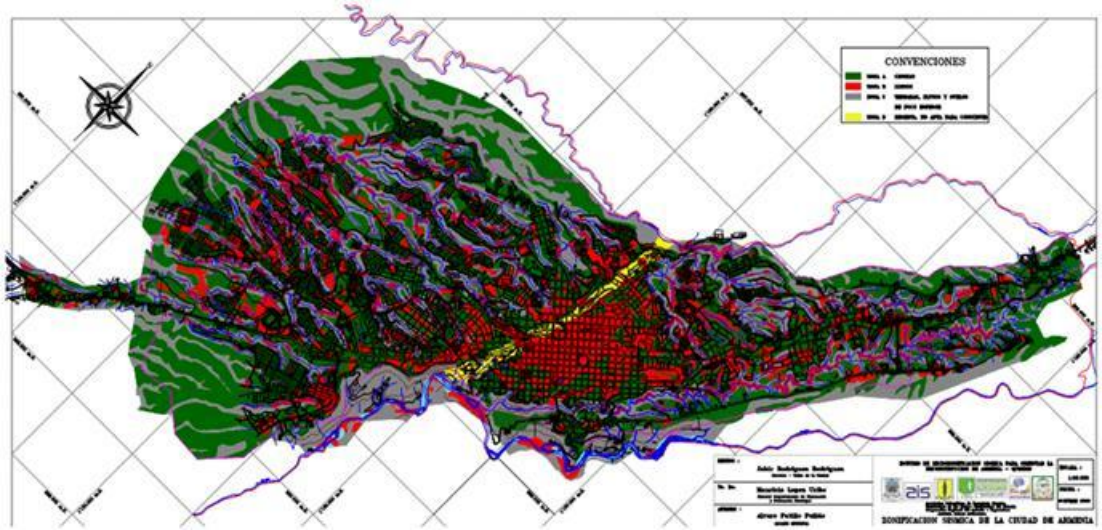


Fuente: CINTEL

Con respecto al plano de Microzonificación Sísmica del Municipio de Armenia, la alcaldía de este municipio ha informado que dicho plano fue

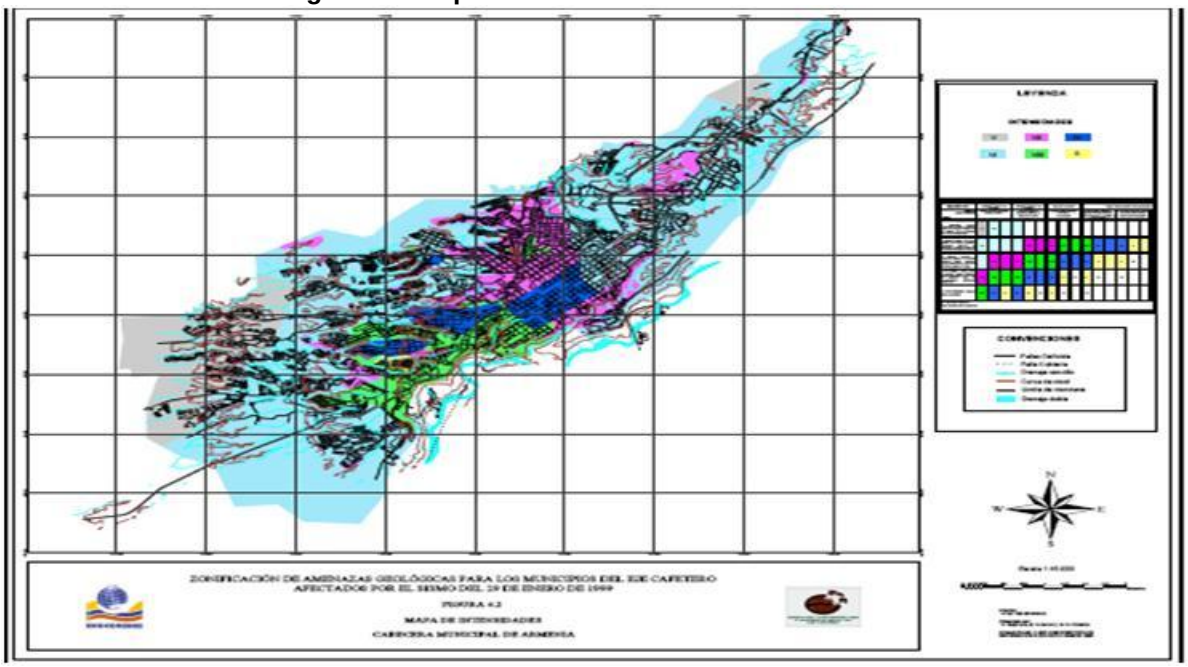
aprobado por el Acuerdo 079 de 2000 y que hasta la fecha de este estudio sigue vigente.

Figura 12. Microzonificación Sísmica de Armenia



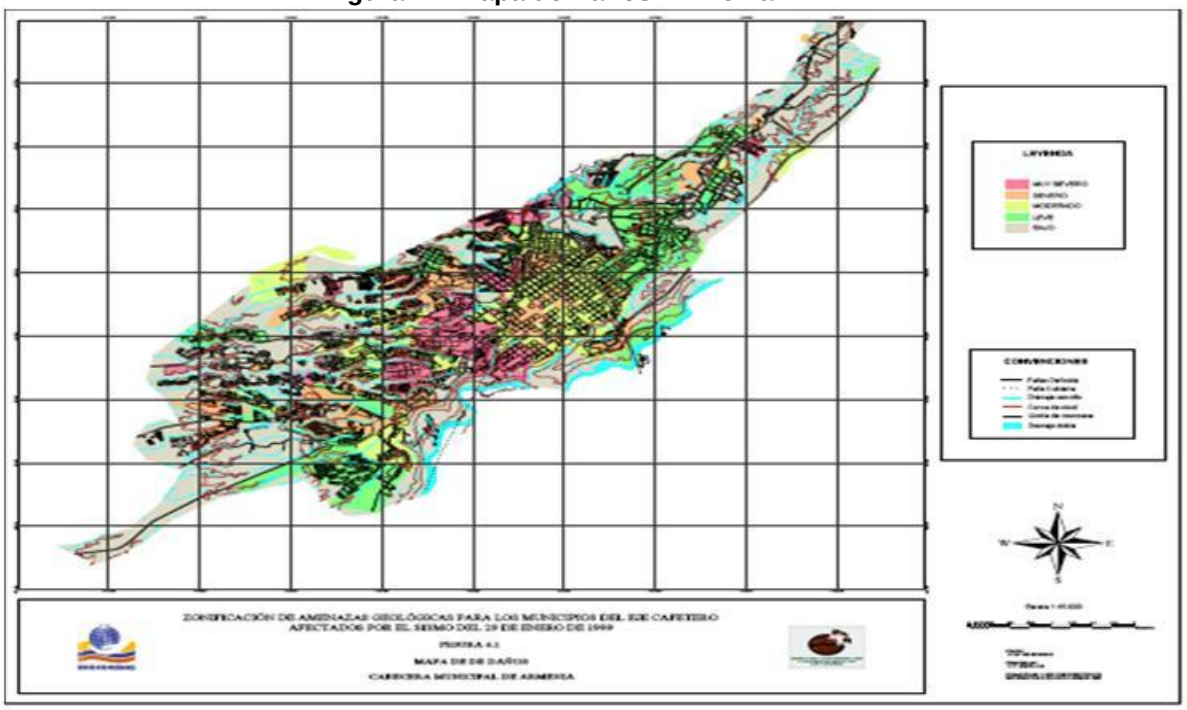
Fuente: Asociación Colombiana de Ingeniería Sísmica. Universidad de los Andes, Quindío, CRQ, INGEOMINAS

Figura 13. Mapa de Intensidades. Armenia



Fuente: INGEOMINAS / FOREC

Figura 14. Mapa de Daños. Armenia



Fuente: INGEOMINAS / FOREC

4.2.2 Caracterización de la zona de estudio por amenaza sísmica

La ciudad de Armenia en el departamento del Quindío, se caracteriza por ser una zona clasificada como de alto riesgo sísmico, la cual está ubicada cerca de la ladera occidental de la corrillera central. Desde las épocas de la colonia, los asentamientos humanos en la zona se caracterizaron por ubicarse en sitios cercanos a quebradas, zonas altas y laderas; en lo que ahora se conoce como zonas de fallas geológicas. La mayor parte del Departamento del Quindío se encuentra en zonas de piedemonte conformadas por colinas formadas por depósitos de ceniza provenientes en gran parte del Volcán Machín. Se presenta en general un comportamiento relacionado a fallas activas como las fallas Montenegro, Armenia y Quebrada Nueva.

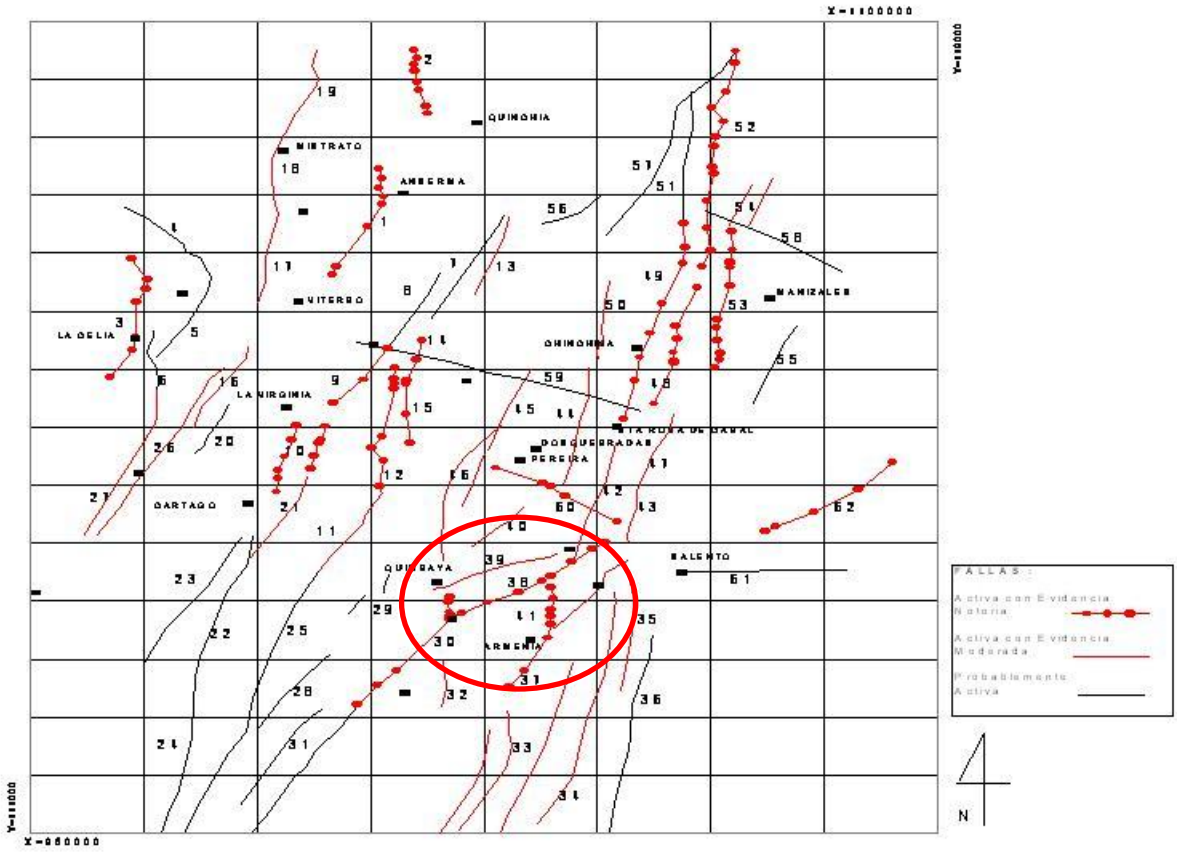
"Los deslizamientos inducidos, por efecto de sismos, pueden ocurrir principalmente en áreas montañosas, y sectorialmente en piedemontes y colinas. Su ocurrencia depende de la pendiente, tipo de suelo, cobertura vegetal y nivel de saturación del suelo durante la vibración sísmica. En las ciudades los rellenos de vertiente se destacan porque allí se concentran la mayor parte de deslizamientos inducidos por sismo, tal como ocurrió para el sismo del 25 de enero de 1999 en las ciudades de Armenia y Pereira. Así mismo, y relacionado al desarrollo vial allí también se concentran los deslizamientos relacionados a cortes de taludes"[13]

"La mayoría de las fallas activas en la región cruzan la zona de sur a norte, tales como el megafallamiento de Romeral, caracterizado por las fallas satélites de Córdoba, Navarco, Silvia-Pijao, Buenavista, el Salado, Cauca-Almaguer, Armenia, Salento, Montenegro y las fallas Palestina y Cauca-Patía, las cuales se destacan entre las principales, con magnitudes probables de 6.1< Mw < 6.9 (Guzmán et al,1998). Existe un menor número de fallamientos en dirección NW-SE"[14]

[13] **Ecorregión del Eje cafetero Capítulo de Amenazas**

[14] **Idem**

Figura 15 Ecoregión del Eje Cafetero. Mapa sintético de fallas activas y probablemente activas



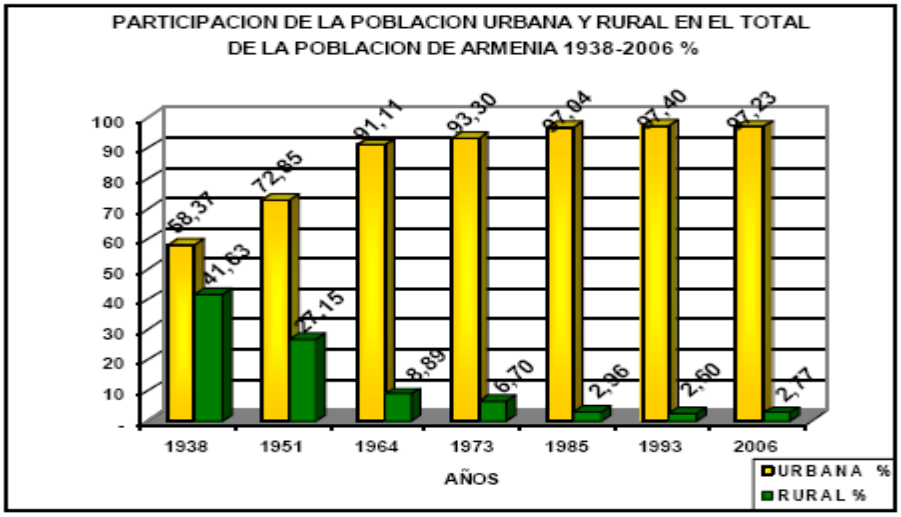
Fuente: Guzmán et al, 1998

4.2.3 Generalidades de las condiciones socio económicas y políticas

El Departamento del Quindío, aunque es el departamento más pequeño del país, ha aportado históricamente grandes contribuciones al PIB nacional, enmarcado principalmente por su actividad agropecuaria asociada al café. Con el paso de los años, la población rural ha disminuido incrementándose las actividades asociadas al entorno urbano así como a actividades de ecoturismo.

Lo anterior conlleva a concluir que la demanda de los servicios asociados al sector de las telecomunicaciones se puede estar incrementando, creando así la necesidad de tener mayor disponibilidad de los servicios asociados a este sector.

Figura 16 Participación de la población urbana y rural en Armenia 1938-2005[15]



Fuente: DANE - Censos de Poblaciones. Cálculos POT.

Con respecto al entorno político asociado a la amenaza sísmica, Armenia se caracteriza por haber tenido uno de los primeros planes de ordenamiento territorial del país y ha sido objeto de varias inversiones en estudios de amenaza sísmica. Sin embargo, en la revisión del POT "Armenia, una ciudad para la vida 2009-2023" se establece que es necesario revisar las políticas asociadas a la mitigación de la amenaza sísmica, así como detallar los estudios de microzonificación.

[15] **Plan de Ordenamiento Territorial de la Ciudad de Armenia. Volumen 3. Diagnóstico Municipal**

El municipio ha establecido diferentes estudios de análisis de las amenazas donde con respecto a la amenaza geológica, se estableció a grandes rasgos que:

Tabla 1. Análisis de la Amenaza[16]

FACTOR	CONDICIÓN
Movimientos en masa y asentamientos diferenciales	
1. Unidad geológica	1.1 Presencia de tefras. 1.2 Presencia de depósitos antrópicos
2. Pendiente	2.1 Mayores a 30° o 57%
3. Uso del suelo	3.1 Areas sin vegetación o con árboles muy pesados. 3.2 Cortes y/o taludes verticales
Inundaciones	
4. Pendiente	4.1 Menores a 5° u 8%
Sismos	
5. Fallas geológicas	5.1 Deformación tectónica en un corredor de 200 m. a partir de la traza principal de las fallas de Armenia, Montenegro y La Tebaida. 5.2 Presencia de depósitos antrópicos.

Fuente: POT Armenia "Duque y Rosenbaum. Research report for period october to december 1997. Imperial College of Science Technology and Medicine. Londres, 16 de diciembre de 1997."

Como una recomendación del estudio del plan de ordenamiento territorial, se estableció que se debe *"REVISAR EN PROFUNDIDAD EL TEMA DE RIESGO. El POT nunca involucró el estudio de microzonificación sísmica, el estudio de vulnerabilidad física para el centro de Armenia y el estudio de estabilidad de taludes y otros insumos en la planificación de la gestión del riesgo"*.

[16] **Idem**

4.2.4 Valoración de la amenaza sísmica

Con base en los eventos ocurridos en la zona con respecto a eventos sísmicos, se estableció en detalle la valoración de la amenaza sísmica mediante la especialización de las consecuencias de un evento sísmico hacia la infraestructura de telecomunicaciones, en una tabla de valoración determinada por una probabilidad estimada de ocurrencia de un sismo dependiendo de su magnitud contra una correlación entre la valoración de las intensidades detectadas para la ciudad de Armenia.

El resultado de la tabla de valoración de la amenaza sísmica se detalla a continuación.

Tabla 2. Determinación de los Valores de Amenaza.

Intensidad / Daños sobre el componente	Vulnerabilidad Física ante la amenaza					Correlación con la Magnitud			
	LEVE	BAJO	MODERADO	SEVERO	MUY SEVERO	Magnitud	Probabilidad de ocurrencia	Probabilidades de ocurrencia estimadas en la zona de estudio	Los valores de Magnitud se cambian en el modelo con el fin de realizar un análisis de la probabilidad de daños que se puedan originar
	0.05	0.1	0.2	0.4	0.8				
XI-XII	Agrietamientos, desalineación, abnegación	Sin daño estructural, pero con algún daño en elementos complementarios	Sin daño estructural, pero posiblemente con algún daño a los elementos no estructurales	Agrietamiento, desplazamiento de cimientos, destrucción estructuras portantes, colapso de columnas, paredes y cubiertas:	Destrucción Total / Colapso			Ocurren Remotamente	
8	0.02	0.04	0.08	0.16	0.32	8	5.00%	5%	
X	Agrietamientos, desalineación, abnegación	Sin daño estructural, pero con algún daño en elementos complementarios	Sin daño estructural, pero posiblemente con algún daño a los elementos no estructurales	Agrietamiento, desplazamiento de cimientos, destrucción estructuras portantes, colapso de columnas, paredes y cubiertas:	Destrucción Total / Colapso			Ocurren esporádicamente (1999)	
7	0.035	0.07	0.14	0.28	0.56	7	10.00%	10%	
VIII-IX	Sin daño	Agrietamientos, desalineación, abnegación	Sin daño estructural, pero con algún daño en elementos complementarios	Sin daño estructural, pero posiblemente con algún daño a los elementos no estructurales	Daños a elementos estructurales y no estructurales pero sin colapso.			Ocurren eventualmente	
6	0.15	0.3	0.6	1.2	2.4	6	50.00%	50%	
VI-VII	Sin daño	Sin daño	Agrietamientos, desalineación, abnegación	Sin daño estructural, pero con algún daño en elementos complementarios	Sin daño estructural, pero posiblemente con algún daño a los elementos no estructurales			Suceden frecuentemente	

Intensidad / Daños sobre	Vulnerabilidad Física ante la amenaza					Correlación con la Magnitud			
	LEVE	BAJO	MODERADO	SEVERO	MUY SEVERO	[illegible]	Probabilida	Probabilidades	rea liza r un
4.5	0.18	0.36	0.72	1.44	2.88	4.5	80.00%	80%	
III-V	Sin daño	Sin daño	Sin daño	Sin daño	Sin daño pero con algún daño en elementos complementarios			Suceden casi todo el tiempo	
3.5	0.1575	0.315	0.63	1.26	2.52	3.5	90.00%	90%	
I-II	Sin daño	Sin daño	Sin daño	Sin daño	Sin daño pero con algún daño en elementos complementarios			Suceden casi todo el tiempo	
2.5	0.11875	0.2375	0.475	0.95	1.9	2.5	95.00%	95%	

Fuente: CINTEL

La tabla anterior es el resultado de sobreponer la información proveniente del mapa de intensidades sobre la ciudad de Armenia, usando la correlación de la escala de intensidades de Mercalli con la escala de Magnitud de Richter y una asignación de la probabilidad de ocurrencia basada en estimativos generales cualitativos de los sismos ocurridos en la ciudad.

En la siguiente tabla se describe por INGEOMINAS los tipos probables de daños que se pueden presentar en la ciudad por diferentes intensidades.

Tabla 3. Valores intensidades en Armenia

VULNERABILIDAD		A			B			C			D			E			F		
DESCRIPCION		Construcciones en materiales diversos sin mortero			Construcciones en materiales diversos con mortero			Estructuras en concreto reforzado sin DSR			Construcciones con estructura en concreto reforzado y varios niveles diseños sismoresistentes (DSR)								
TIPOS DE CONSTRUCCION		Adobe, bahareque, tapia pisada y otros			Mamposteria no reforzada, piedras en bloques y cantos			Mamposteria reforzada con losas de concreto			Manposteria confinada, CR con mínimo nivel de DSR estructuras metálicas y de maderas			Concreto reforzado (CR) con moderado nivel de diseño sismoresistente			Concreto reforzado (CR) con elevado nivel de diseño sismoresistente		
DAÑOS	PORCENTAJE %	0-20	10-60	50-100	0-20	10-60	50-100	0-20	10-60	50-100	0-20	10-60	50-100	0-20	10-60	50-100	0-20	10-60	50-100
1. LIGEROS: Fisuras pequeñas en pocas paredes.		V	VI																
2. MODERADOS: Pequeñas grietas en muchas		VI				VII		VII	VIII		VIII	IX		IX	X		X	XI	
3. GRAVE: Anchas y extensas grietas en muchas			VII		VII	VIII		VIII	IX		IX	X		X	XI		XI		
4. SEVEROS: Serios daños en paredes, daño		VII	VIII		VIII	IX		IX	X	XI	X	XI		XI					
5. DESTRUCCION: Colapso total o casi total.		VIII	IX	X	IX	X	XI	X	XI		XI								
CR - Concreto reforzado																			
DSR - Diseño sismo resistente																			
NOTA ACLARATORIA: Cada intensidad y su color represntativo resultan de la combinación entre el porcentaje de daños y la vulnerabilidad por barrio																			

Fuente: CINTEL.

Por otro lado se puede establecer claramente una relación ente la Escala de Intensidad de Mercalli y la Escala de Magnitud Richter de la siguiente manera:

Tabla 4. Comparación de las Escalas de Mercalli y Richter

Escala de Mercalli		Magnitud Richter	
I. II.	Casi nadie lo siente. Sentido por unas cuantas personas.	2.5	No es sentido en general, pero es registrado por sismómetros.
III. IV.	Notado por muchos, pero sin la seguridad de que se trate de un temblor. Sentido por muchos en el interior de las casas. Se siente	3.5	Sentido por mucha gente.

Escala de Mercalli		Magnitud Richter	
	como si un vehículo pesado golpeara la casa.		
V.	Sentido por casi todos; mucha gente despierta; los árboles y los postes de alumbrado se balancean.		
VI.	Sentido por todos; mucha gente sale corriendo de sus casas; los muebles se desplazan y daños menores se observan.	4.5	Puede causar daños menores en la localidad.
VII.	Todos salen corriendo al exterior; se observan daños considerables en estructuras de pobre construcción. Daños menores en edificios bien construidos.		
VIII.	Daños ligeros en estructuras de buen diseño; otro tipo de estructuras se colapsan.	6	Sismo destructivo.
IX.	Todos los edificios resultan con daños severos; muchas edificaciones son desplazadas de su cimentación; grietas notorias en el suelo.		
X.	Muchas estructuras son destruidas. El suelo resulta considerablemente fracturado.	7	Un terremoto o sismo mayor.
XI.	Casi todas las estructuras caen. Puentes destruidos. Grandes grietas en el suelo.	8.0 ó Mayor	Grandes terremotos.
XII.	Destrucción total. Las ondas sísmicas se observan en el suelo. Los objetos son derribados y lanzados al aire.		

Fuente: RED SISMICA DEL NORESTE DE MEXICO

Por otro lado y con fines de modelar posibles escenarios ocurrencia de sismos en la zona, se establece hipotéticamente la probabilidad de ocurrencia de sismos en la zona de la siguiente manera:

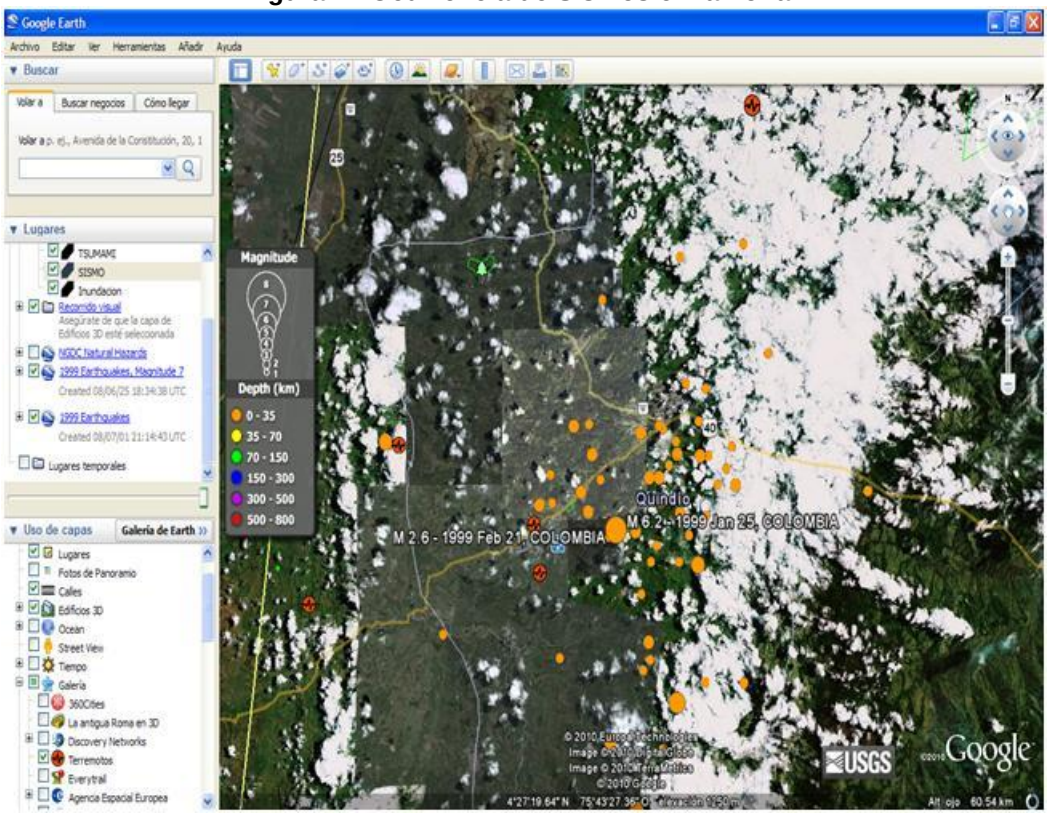
Tabla 5. Tabla de valores hipotéticos de probabilidad de ocurrencia de un sismo en la zona de estudio.

INTENSIDAD	PROBABILIDAD
I	0.95
II	0.95
III	0.9
IV	0.9
V	0.9
VI	0.8
VII	0.8
VIII	0.5
IX	0.5
X	0.1
XI	0.05

Fuente: CINTEL.

Nota: Estos valores son generados con el fin de establecer un mecanismo de probabilidad de ocurrencia estimado y por lo tanto solo deben ser usados para efectos de simular los posibles escenarios de riesgos que surgen al calificar la exposición de la vulnerabilidad física de los elementos de la red de telecomunicaciones antes esta amenaza. El presente estudio arroja resultados de los riesgos a los que está sometida la infraestructura de telecomunicaciones ante la ocurrencia de un sismo de una intensidad mayor a VI.

Figura 17 Ocurrencia de Sismos en la Zona:



Fuente USGS y GoogleEarth

4.2.5 Priorización de la amenaza sísmica

En consecuencia del diagnóstico anterior, y para efectos del presente estudio, se tratará la totalidad del municipio de Armenia como una zona de amenaza sísmica alta. Sin embargo, la priorización de la amenaza se da al categorizar los resultados obtenidos de multiplicar el valor de los daños estimados contra el valor de la intensidad / magnitud del evento sísmico esperado. A manera de ejemplo, se describe la calificación de la amenaza para los estudios AM en la zona:

Tabla 6. Tabla de resultados ejemplo de la calificación de la amenaza sísmica para un servicio específico

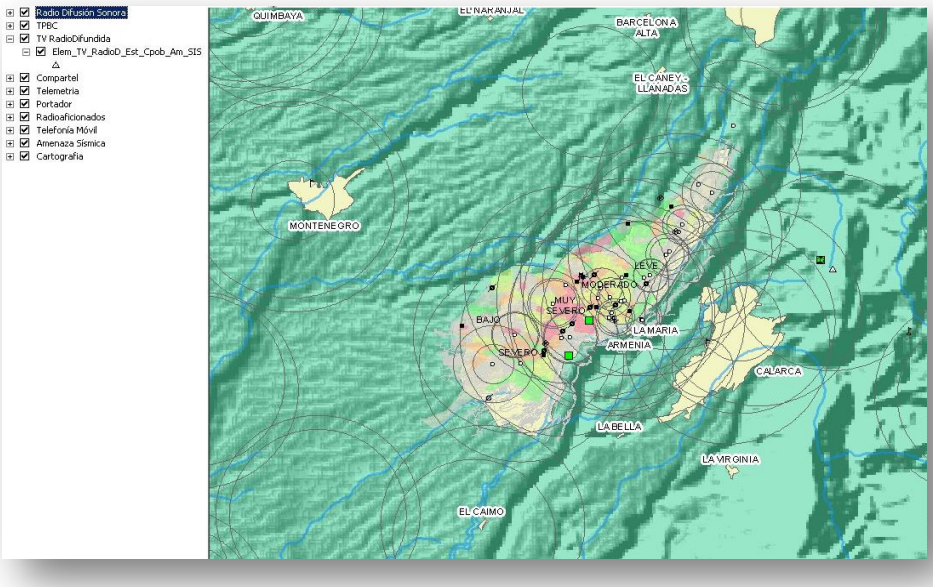
MUNICIPIO	INFRAESTRUCTURA	Calificación Daños	Valor Daños	Intensidad	Valor Intensidad / Magnitud	Impacto Estimado	Probabilidad Estimada
ARMENIA	ESTUDIO	MODERADO	0.2	VI	4.5	0.72	80%
ARMENIA	ESTUDIO	BAJO	0.1	VI	4.5	0.36	80%
ARMENIA	ESTUDIO	BAJO	0.1	VII	4.5	0.36	80%
ARMENIA	ESTUDIO	BAJO	0.1	VII	4.5	0.36	80%
ARMENIA	ESTUDIO	BAJO	0.1	VII	4.5	0.36	80%
ARMENIA	ESTUDIO	BAJO	0.1	VII	4.5	0.36	80%
ARMENIA	ESTUDIO	BAJO	0.1	VII	4.5	0.36	80%

Fuente: CINTEL

Por lo tanto, dicha priorización establece el valor final del riesgo al multiplicar el valor de este impacto y probabilidad contra la vulnerabilidad física y funcional del elemento.

Como resultado del proceso se tiene la siguiente información:

Figura 18 Mapa de Amenaza Sísmica sobre la Infraestructura



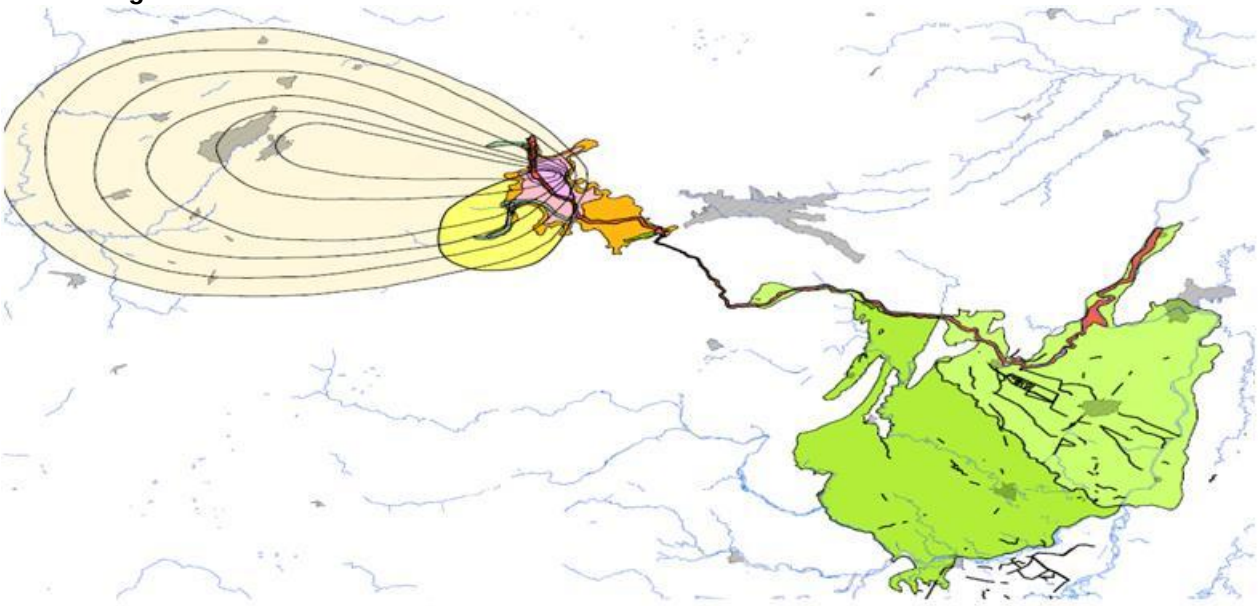
Fuente: CINTEL

4.3 DIAGNÓSTICO DE AMENAZA VOLCÁNICA: TOLIMA, CAJAMARCA

4.3.1 Delimitación de la zona de estudio

Para el efecto de tener un área de cubrimiento general de toda la infraestructura de telecomunicaciones, se estableció la descrita por INGEOMINAS.

Figura 19 Área de cubrimiento total de la influencia del Volcán Machín



Fuente: Ingeominas - Zona de Amenaza Volcánica del Machín

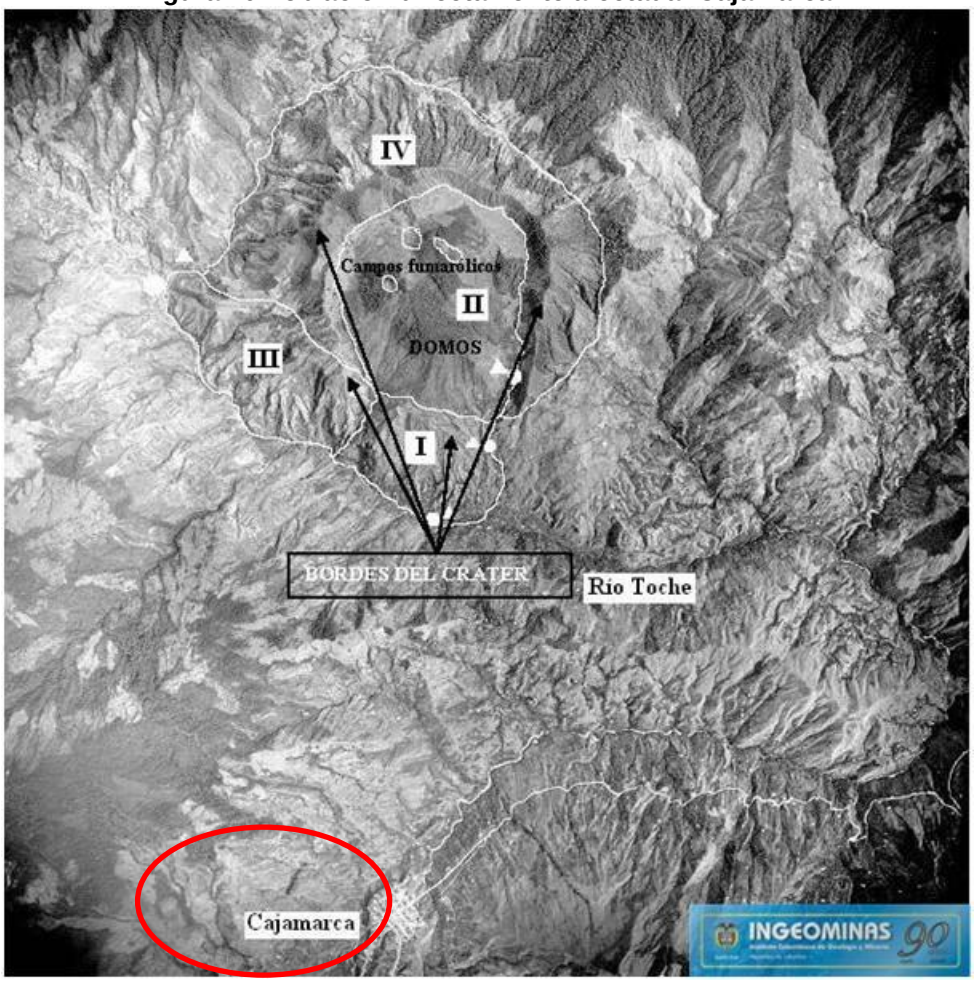
De otro lado, cabe detallar que esta zona de estudio contiene la zona de estudio de la amenaza sísmica de Armenia. Por otro lado, eventualmente la actividad sísmica que genere la actividad volcánica puede afectar la infraestructura de telecomunicaciones que presta el servicio a la ciudad de Armenia.

El mapa de amenaza volcánica puede abarcar algunas zonas de los departamentos de Quindío, Tolima, Risaralda y Valle del Cauca, sin

embargo, el estudio se enfocará en el estudio de la amenaza volcánica para la infraestructura de telecomunicaciones que le presta el servicio a los centros poblados de Anaime, Armenia, Cajamarca, Calarcá, Coello, Espinal, Flandes, Girardot, Guamo, Tapias y Toche. Estos centros poblados serán tomados como puntos, es decir el servicio prestado a la población se tomará como un todo y no desagregado.

Como se puede observar a continuación, la población directamente afectada es la de Cajamarca.

Figura 20 Población directamente afectada: Cajamarca



Fuente: Ingeominas - Zona de Amenaza Volcánica del Machín

Figura 21 Población directamente afectada 3d: Cajamarca

Fuente. Google Earth

4.3.2 Caracterización de la zona por amenaza volcánica

Existen diversos estudios sobre la amenaza volcánica del Machín y sus impactos, como lo son los centros de investigación vulcanológica, las corporaciones autónomas y entidades gubernamentales. Sin embargo, el presente estudio utilizará la información recopilada y publicada por INGEOMINAS. De acuerdo con estudios regionales se ha descrito que:

> *"El Volcán Machín, es un volcán activo en estado de reposo, de carácter muy explosivo, presenta en la actualidad actividad fumarólica en los domos, fuentes termales y actividad sísmica a niveles bajos. Su historia eruptiva se restringe a los últimos 20.000 años, 11 de sus eventos ocurrieron durante los últimos 5000 años, y su último evento ocurrió hace aproximadamente 820 años. Sus productos principales consisten de flujos piroclásticos y caída de piroclastos. Su afectación potencial por caída de piroclastos incluye los municipios de Toche, Tapias, Moralito,*

Cajamarca y Anaime. Por flujos piroclásticos los municipios de Toche, Moralito, Tapias, Cajamarca, Anaime, Coello, El Boquerón y parte de Ibagué. Los flujos de lodo en el cauce del río Coello (inspección de policía de Coello y Nariño a orillas del río Magdalena).[17]

De acuerdo al INGEOMINAS, las amenazas asociadas al Volcán Machín se pueden dar por:

- FLUJOS PIROCLÁSTICOS. "Se pueden originar por colapso de la columna eruptiva o por colapso de domos, generando flujos de ceniza, pómez y oleadas piroclásticas, y flujos de ceniza y bloques, respectivamente. Tomando como base un colapso de columna a 300 metros de altura, se afectarían toda la zona proximal de manera radial y luego seguirían los cauces de las quebradas Santa Marta, San Juan, Azufral, Aguascalientes y Campamento y el río Toche y, sobrepasaría la barrera topográfica de San Lorenzo, para canalizarse por los cauces de los ríos Coello y Bermellón, pudiendo llegar incluso al río Magdalena a la altura de la población de Nariño. Los flujos originados por colapso de domos afectarían áreas relativamente pequeñas (15,3 km2), restringidos a la zona proximal."

- PIROCLÁSTOS DE CAÍDA. "Los piroclástos de caída se distribuirán primordialmente en los primeros 5 Km alrededor del volcán, por proyección balística, y luego por transporte eólico se

[17] **Ecorregión del Eje Cafetero**

desplazarían preferencialmente hacia el flanco occidental, tal y como ha ocurrido en las erupciones anteriores."

- LAHARES. "Al ocurrir flujos piroclásticos en las erupciones del volcán, éstos se enriquecerían en agua ya sea al irlas incorporando paulatinamente o por represamiento de éstas por el alto volumen de material depositado, para luego generar los flujos de lodo que podrían alcanzar hasta el río Magdalena."

- ACTIVIDAD FUMARÓLICA. "El componente volátil es el vapor de agua, más CO2, y en menor proporción H2S, SO2 y CO; algunos de los cuales se pueden acumular en las depresiones cercanas al volcán y convertirse por lo tanto en elementos letales."

- ACTIVIDAD SÍSMICA. "Se han detectado sismos de alta frecuencia, correspondientes a fenómenos de ruptura, algunos sentidos por los habitantes de las zonas proximales."

- PETROGRAFÍA: "Los productos del Machín se han catalogado como fenodacitas constituidas por plagioclasa (oligoclasa), feldespato potásico, cuarzo, anfíbol, biotita y vidrio; los accesorios son el apatito y los metálicos."

4.3.3 Generalidades de las condiciones socio económicas y políticas

La zona se caracteriza por tener condiciones socio económicas diversas, homogeneizadas por las actividades agropecuarias y comerciales. Quizá una de las principales actividades económicas impactadas por un posible evento volcánico será la relacionada con el transporte terrestre; la zona se caracteriza por un alto flujo vehicular de transporte de carga entre el

occidente, el centro y el oriente del país. Por esta vía transita la carga proveniente de Buenaventura con destino a Bogotá D.C.

Según el INGEOMINAS[18]:

- "En el área de influencia directa de la actividad del VCM se localizan centros urbanos importantes, tales como, Ibagué, (340.191), Armenia (216.467), Girardot (81.380), Flandes (19.028), Calarcá (44.047), Cajamarca (7.867), Espinal (43.422), Guamo (14.157), Saldaña (7.259), Nariño (C/marca; 1.227)), Coello (912), San Antonio (4.831), San Luis (3.254), Valle de San Juan (1.562) y Anaime (Figura 1). Esto significa que en toda el área de influencia pueden vivir cerca de un millón de personas, pues no están listados todos los municipios.

- Las principales actividades económicas están ligadas a las industrias agropecuaria, textil y minera; son de destacar en la zona el cultivo de café, arroz, frutas y verduras, y la producción de cemento. Para la actividad económica nacional, además, son importantes la carretera que une a Bogotá con el puerto de Buenaventura (soporta el 50% de las importaciones y de las exportaciones) y con Quito (Ecuador) y las rutas aéreas nacionales que conectan con el suroeste del territorio y con el sur del continente."

18 INGEOMINAS. EVALUACIÓN DE LA AMENAZA VOLCÁNICA POTENCIAL DEL CERRO MACHÍN (DEPARTAMENTO DEL TOLIMA, COLOMBIA). Manizales, septiembre de 2002

4.3.4 Valoración de la amenaza volcánica

A manera preliminar, se ha podido constatar que la amenaza volcánica para la zona de estudio se debe clasificar desde amenaza alta hasta amenaza intermedia, en las cuales las restricciones para el desarrollo de infraestructura de telecomunicaciones deben ser altas, enfocándose en aquellas medidas que impliquen disminuir la vulnerabilidad para la prestación del servicio, dado que se cuenta ya con un desarrollo urbano y de infraestructura vial importante que lo requiere. Esté análisis será desarrollado a profundidad en las siguientes fases del presente estudio.

Dado que a la fecha no existe evidencia reciente de eventos ocurridos en la zona, se establecerá en detalle la valoración de la amenaza volcánica mediante la especialización de las amenazas realizada por INGEOMINAS, contra la información de la infraestructura de telecomunicaciones recibida por los operadores en una tabla de valoración que será detallada durante la siguiente etapa del estudio y que contendrá de manera general, los siguientes campos:

Tabla 7 Tabla de valoración de la vulnerabilidad y el riesgo por volcán

Fase	%	Máximo	Indicador
0	10-20%	20%	Reposo (800 años hasta Fase 1)
1	20-30%	30%	Pre crisis (Meses hasta pocos Años)
2	30-40%	40%	Inicio Crisis (Semanas)
3	40-70%	70%	Erupciones Magmáticas Menores (Días a Semanas)
4	80-90%	90%	Explosiones Ráfaga (Días)
5	90-100%	100%	Erupción Principal (Horas)
6	80-90%	90%	Posclimatica (pocos Meses)
7	40-70%	70%	Final Erupción

Fuente: CINTEL

Las Fases Eruptivas son determinadas por el INGEOMINAS para el Volcán Machín, los valores de probabilidad se ajustan de manera cualitativa de

forma que aumenta la probabilidad estimada de ocurrencia de los eventos asociados al volcán.

El modelo considera que en la medida que las entidades aumenten el nivel de alarma sobre la actividad de un volcán dado, se deberá ajustar la fase en la que se encuentra el proceso y el modelo calculará la probabilidad estimada de ocurrencia del fenómeno en cada una de las zonas de amenaza sobre la infraestructura instalada.

4.3.5 Priorización y zonificación de la amenaza volcánica

La zona de estudio se dividirá en sub zonas de amenaza de la siguiente manera:

- ZONAS DE AMENAZA POR IMPACTO DE FLUJOS PIROCLÁSTICOS
- ZONAS DE AMENAZA POR IMPACTO DE LAHARES
- ZONAS DE AMENAZA POR CAÍDA DE PIROCLÁSTOS
- ZONAS DE AMENAZA POR IMPACTO DE PROYECTILES

Cada una de estas zonas tendrá divisiones internas dependiendo de la ubicación geográfica, las cuales tendrán los niveles sugeridos por las entidades gubernamentales.

Tabla 8. Tabla de resultados ejemplo de la calificación de la amenaza volcánica para un servicio específico

Zonas Amenazadas				
Identificador del Elelemento	Impacto por Ceniza	Impacto por Lahar	Impacto por Piroclasto	Impacto por Proyectiles
31030	1	0	0	0
31040	1	0	0	1

Zonas Amenazadas				
Identificador del Elelemento	Impacto por Ceniza	Impacto por Lahar	Impacto por Piroclasto	Impacto por Proyectiles
31028	1	0	0	0
31039	1	0	0	0
31001	1	0	0	0
31002	1	0	0	0
31021	1	0	0	0
31023	1	0	0	0
31025	1	0	0	0
31024	1	0	0	0
31022	1	0	0	0
31029	1	0	0	0
31026	1	0	0	0
31003	1	0	0	0
31031	1	0	0	0
Grand Total	**1**	**0**	**0**	**1**

Fuente: CINEL

Posteriormente, se establece la probabilidad de ocurrencia del evento de acuerdo a la fase a modelar de tal manera que a medida que aumente la actividad del Volcán en cuestión, reportada por las entidades competentes, se debe modificar en la fase eruptiva a modelar:

Tabla 9 Tabla de resultados ejemplo de la priorización de la amenaza volcánica para un servicio específico

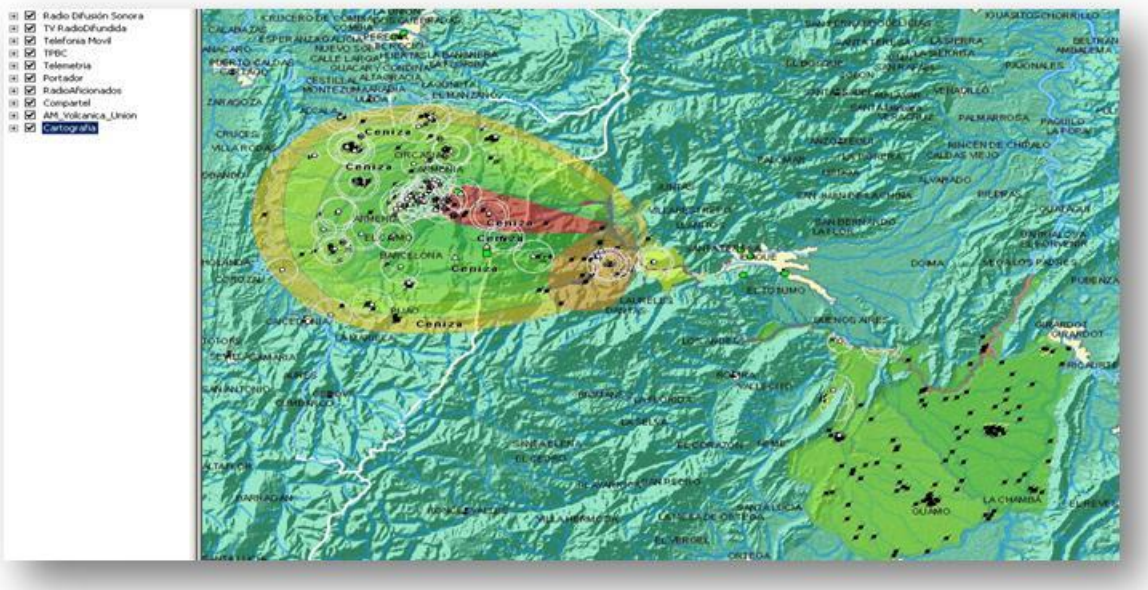
Zonas Amenazadas	Fase Eruptiva a Modelar			1
Identificador del Elemento	% Ceniza	% Lahar	% Piroclasto	% Balístico
31030	0.75%	0.00%	0.00%	0.00%
31040	3.75%	0.00%	0.00%	5.00%
31028	7.50%	0.00%	0.00%	0.00%
31039	22.50%	0.00%	0.00%	0.00%
31001	30.00%	0.00%	0.00%	0.00%
31002	30.00%	0.00%	0.00%	0.00%
31021	30.00%	0.00%	0.00%	0.00%

Zonas Amenazadas	Fase Eruptiva a Modelar			1
Identificador del Elemento	% Ceniza	% Lahar	% Piroclasto	% Balístico
31023	22.50%	0.00%	0.00%	0.00%
31025	22.50%	0.00%	0.00%	0.00%
31024	22.50%	0.00%	0.00%	0.00%
31022	22.50%	0.00%	0.00%	0.00%
31029	7.50%	0.00%	0.00%	0.00%
31026	7.50%	0.00%	0.00%	0.00%
31003	3.75%	0.00%	0.00%	0.00%
31031	3.75%	0.00%	0.00%	0.00%
Grand Total	**30%**	**0%**	**0%**	**5%**

Fuente: CINTEL

Como resultado del proceso, se tiene la siguiente información:

Figura 22 Mapa de Amenaza Volcánica sobre la Infraestructura



Fuente: CINTEL.

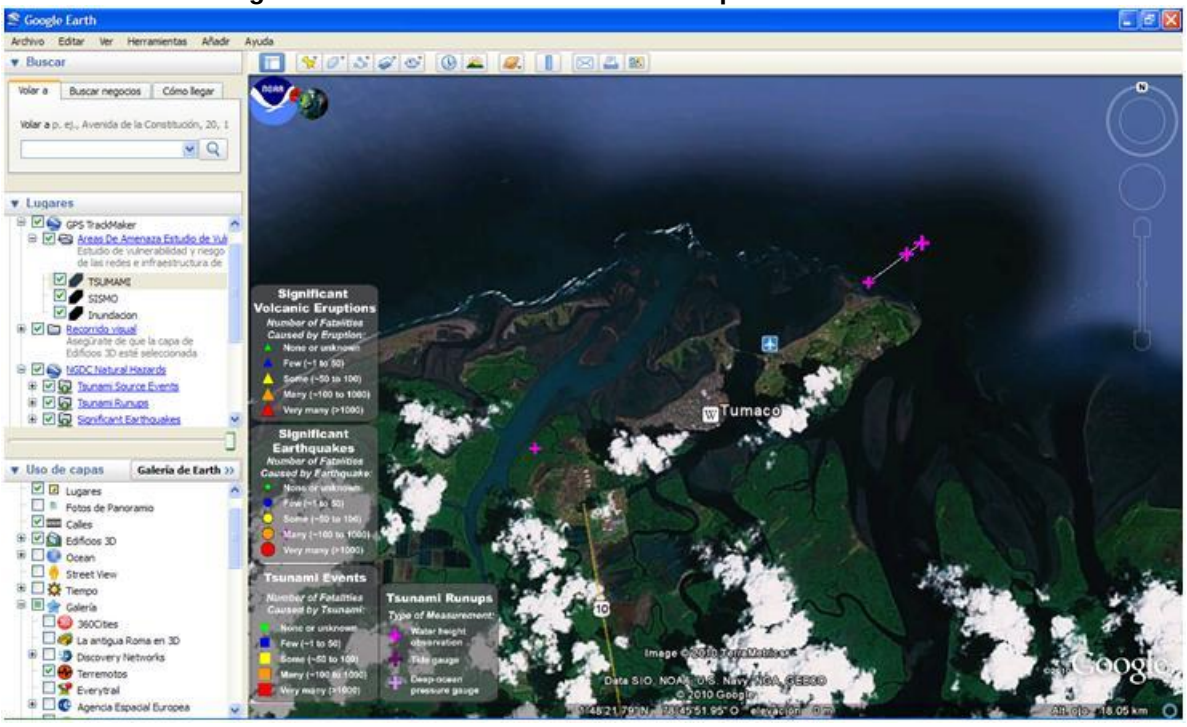
4.4 DIAGNÓSTICO DE AMENAZA POR TSUNAMI: NARIÑO, TUMACO

4.4.1 Delimitación de la zona de estudio

Con el objetivo de tener un área de cubrimiento general de toda la infraestructura de telecomunicaciones, se estableció un área mayor que el perímetro urbano del municipio de Tumaco. Sin embargo, el estudio detallado se realizará sobre el área de influencia cercana de casco urbano.

De otro lado, cabe detallar que en la zona de estudio la amenaza por tsunami depende de los sismos que se puedan dar por la confluencia de la placa tectónica del Pacífico contra la Sur Americana como consecuencia de grandes sismos.

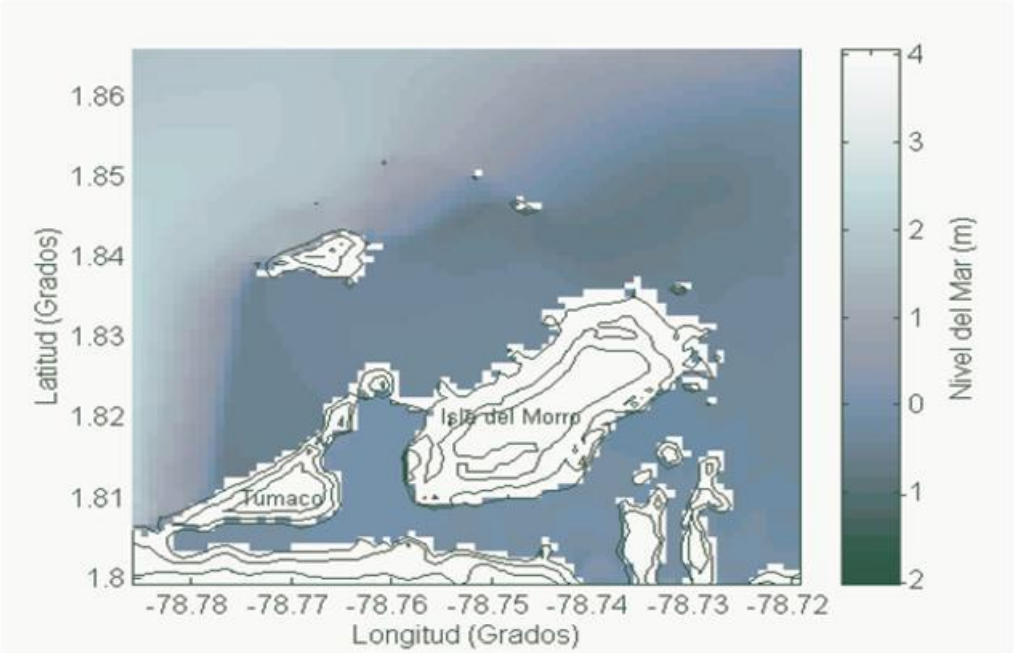
Figura 23. Zona de estudio la amenaza por tsunami



Fuete: NOAA. National Geophysical Datacenter. Eventos Asociados a Tsunami en Tumaco. GoogleEarth

Como se observa en la figura anterior, el municipio de Tumaco se encuentra localizado en una zona propensa a las inundaciones. Adicionalmente, la siguiente gráfica muestra cómo la ciudad se encuentra solo a pocos metros por encima del nivel del océano Pacífico.

Figura 24. Curvas de Nivel del Municipio de Tumaco.[19]



Fuente: DIMAR

Preliminarmente y con el propósito de iniciar el estudio en cuestión, se delimitan de manera general tres zonas de amenaza por tsunami así:

[19] **Simulaciones numéricas de propagación de Tsunami para la costa Pacífica Colombiana. Jhon Henry Caicedo O. , Bruno Martinelli, Hansjürgen Meyer, Julián Augusto Reyna M**

Figura 25 Delimitación preliminar de amenaza por Tsunami

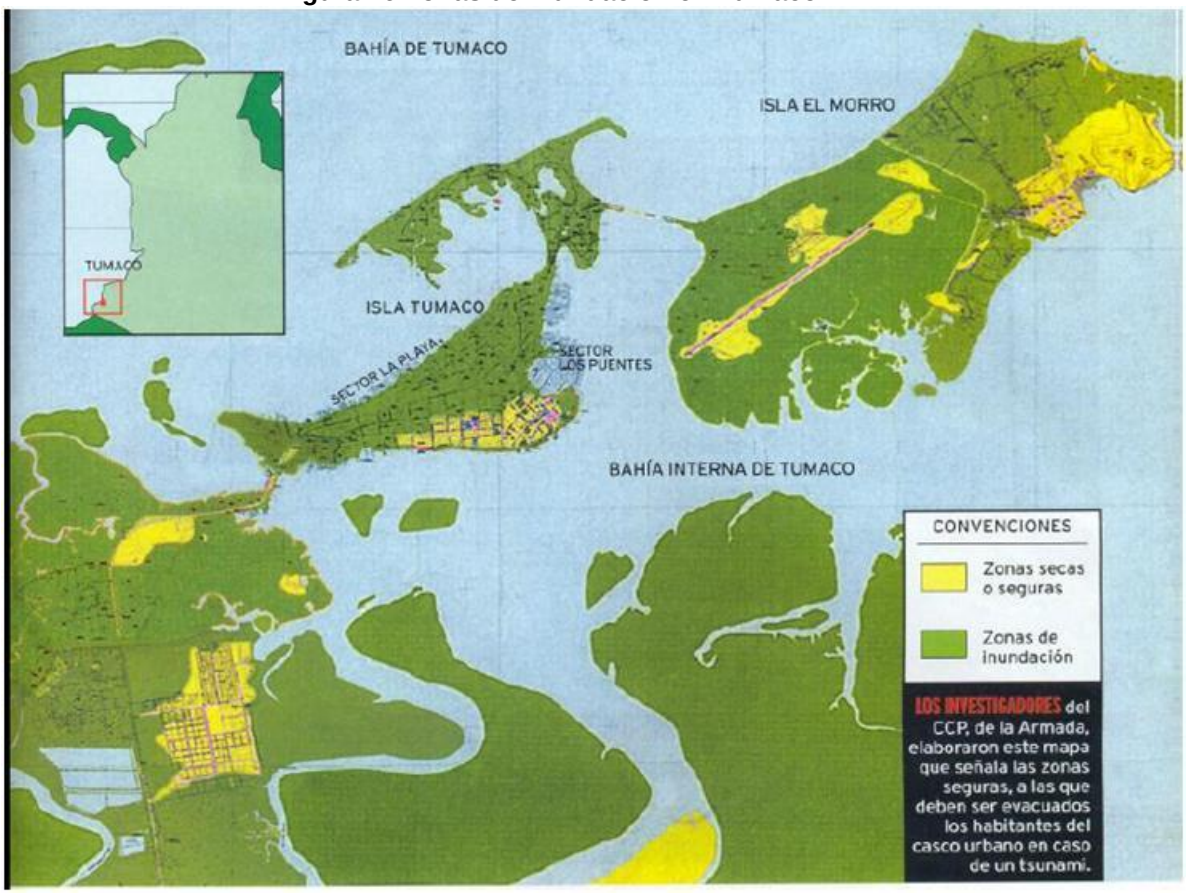
Fuente: CINTEL

4.4.2 Generalidades de las condiciones socio económicas y políticas

La zona se caracteriza por tener un crecimiento desordenado, sus pobladores se dedican mayormente a actividades agropecuarias como la explotación forestal, la pesca y el turismo.

Por estar conformada por tres islas altamente pobladas y estar expuestas a tsunamis, las entidades gubernamentales han dedicado esfuerzos para realizar estudios de amenaza, riesgo y prevención ante estos eventos que han permitido delimitar las zonas expuestas a este fenómeno.

Figura 26 Zonas de Inundación en Tumaco



Fuente: Armada Nacional

4.4.3 Valoración de la amenaza por Tsunami

Para detallar la valoración de la amenaza a la que está expuesta la infraestructura de telecomunicaciones, se sobrepondrá la ubicación de infraestructura según la información suministrada por los proveedores con los mapas de inundación. Para los efectos del impacto de la ola, se simulará para aquellos elementos que prestan el servicio de comunicaciones y que estén expuestos a un impacto directo. Lo anterior teniendo en cuenta que la ubicación de la población se encuentra cerca de las zonas costeras.

Para la zona, se estableció que la valoración de la probabilidad de la ocurrencia del Tsunami se puede dar por las alertas tempranas que emitan las entidades encargadas de acuerdo con los indicadores determinados por dos tipos de escalas, la de SIEBERG de intensidades de Tsunami y la de Douglas del estado del océano. Los valores de probabilidad de ocurrencia para la zona de TUMACO se ajustan de manera cualitativa de manera que aumenta la probabilidad estimada de ocurrencia de los eventos asociados al impacto de la Ola.

El modelo considerará que en la medida que las entidades aumenten el nivel de alarma sobre las alarmas que se generen de TSUNAMI para el Pacífico, se deberá ajustar la fase en la que se encuentra el proceso y el modelo calculará la probabilidad estimada de ocurrencia del fenómeno en cada una de las zonas de amenaza sobre la infraestructura instalada.

Tabla 10 Escala modificada SIEBERG de intensidades de Tsunamis

Escala modificada SIEBERG de intensidades de Tsunamis.			
Fase	**%**	**Máximo**	**Indicador**
1	0%	0%	Muy suave. La ola es tan débil, que solo es perceptible en los registros de las estaciones de marea.
2	1-25%	25%	Suave. La ola es percibida por aquellos que viven a lo largo de la costa y están familiarizados con el mar. Normalmente se percibe en costas muy planas.
3	26-55%	55%	Bastante fuerte. Generalmente es percibido. Inundación de costas de pendientes suaves. Las embarcaciones deportivas pequeñas son arrastradas a la costa. Daños leves a estructuras de material ligero situadas en las cercanías a la costa. En estuarios se invierten los flujos de los ríos hacia arriba.
4	56-75%	75%	Fuerte. Inundación de la costa hasta determinada profundidad. Daños de erosión en rellenos construidos por el hombre. Embancamientos y diques dañados. Las estructuras de material ligero cercanas a la costa son dañadas. Las estructuras costeras sólidas sufren daños menores. Embarcaciones deportivas grandes y pequeños buques son derivados tierra adentro o mar afuera. Las costas se encuentran sucias con desechos flotantes.

Escala modificada SIEBERG de intensidades de Tsunamis.			
Fase	**%**	**Máximo**	**Indicador**
5	76-95%	95%	Muy fuerte. Inundación general de la costa hasta determinada profundidad. Los muros de los embarcaderos y estructuras sólidas cercanas al mar son dañados. Las estructuras de material ligero son destruidas. Severa erosión de tierras cultivadas y la costa se encuentra sucia con desechos flotantes y animales marinos. Todo tipo de embarcaciones, a excepción de los buques grandes, son llevadas tierra adentro o mar afuera. Grandes subidas de agua en ríos estuarinos. Las obras portuarias resultan dañadas. Gente ahogada. La ola va acompañada de un fuerte rugido.
6	96-100%	100%	Desastroso. Destrucción parcial o completa de estructuras hechas por el hombre a determinada distancia de la costa. Grandes inundaciones costeras. Buques grandes severamente dañados. Árboles arrancados de raíz o rotos. Muchas víctimas.

Fuente. .Servicio Hidrográfico y Oceanográfico de Chile. (Modificaciones para efecto del estudio realizadas por CINTEL)

Tabla 11. Escala Modificada DOUGLAS de estado del Océano

Escala Modificada DOUGLAS de estado del Océano				
Fase	**%**	**Máximo**	**Altura en metros / Indicador**	
0	0%	0%	0	Calma o llana
1	1-15%	10%	0 a 0,1	Rizada
2	16-25%	25%	0,1 a 0,5	Marejadilla
3	26-55%	55%	0,5 a 1,25	Marejada
4	56-75%	75%	1,25 a 2,5	Fuerte Marejada
5	76-95%	95%	2,5 a 4	Gruesa
6	95-100%	100%	4 a 6	Muy Gruesa
7	95-100%	100%	6 a 9	Arbolada
8	95-100%	100%	9 a 14	Montañosa
9	95-100%	100%	Más de 14	Enorme

Fuente. Servicio Hidrográfico y Oceanográfico de Chile. Agencia Estatal de Meterología del Gobierno de España
http://www.aemet.es/documentos/es/divulgacion/maritima/escalas_de_viento_y_oleaje.pdf
(Modificaciones para efecto del estudio realizadas por CINTEL)

4.4.4 Priorización y zonificación de la amenaza por tsunami

Con base en los eventos ocurridos en la zona relacionados con tsunami, se establecerá en detalle la valoración de la amenaza por inundación e impacto directo mediante la especialización de las consecuencias de un evento del tsunami hacia la infraestructura de telecomunicaciones.

Cada una de estas zonas tendrá divisiones internas dependiendo de la ubicación geográfica, las cuales podrán variar de acuerdo al nivel de alarma que pueda ser generado por las entidades gubernamentales.

Tabla 12. Tabla de valoración de la vulnerabilidad y el riesgo por tsunami

Zonas Amenazadas				
Identificador del Elemento	ZONA AMENAZA POR TSUNAMI	GOLPE OLA	FUERZAS LATERALES	INUNDACIÓN
33001	0	0	0	0
33002	0	0	0	0
33003	0	0	0	0
33004	0	0	0	0
33005	0	0	0	0
33006	Inundación Salobre	0	1	1

Fuente: CINTEL

Posteriormente, se establece la probabilidad de ocurrencia del evento de tsunami de acuerdo a la fase a modelar de tal manera que a medida que aumente el nivel de alarma, el indicador para tsunami o el estado del océano reportada por las entidades competentes, se debe modificar en la fase del estado del tsunami a modelar:

Tabla 13. Tabla de resultados ejemplo de la priorización de la amenaza por tsunami para un servicio específico

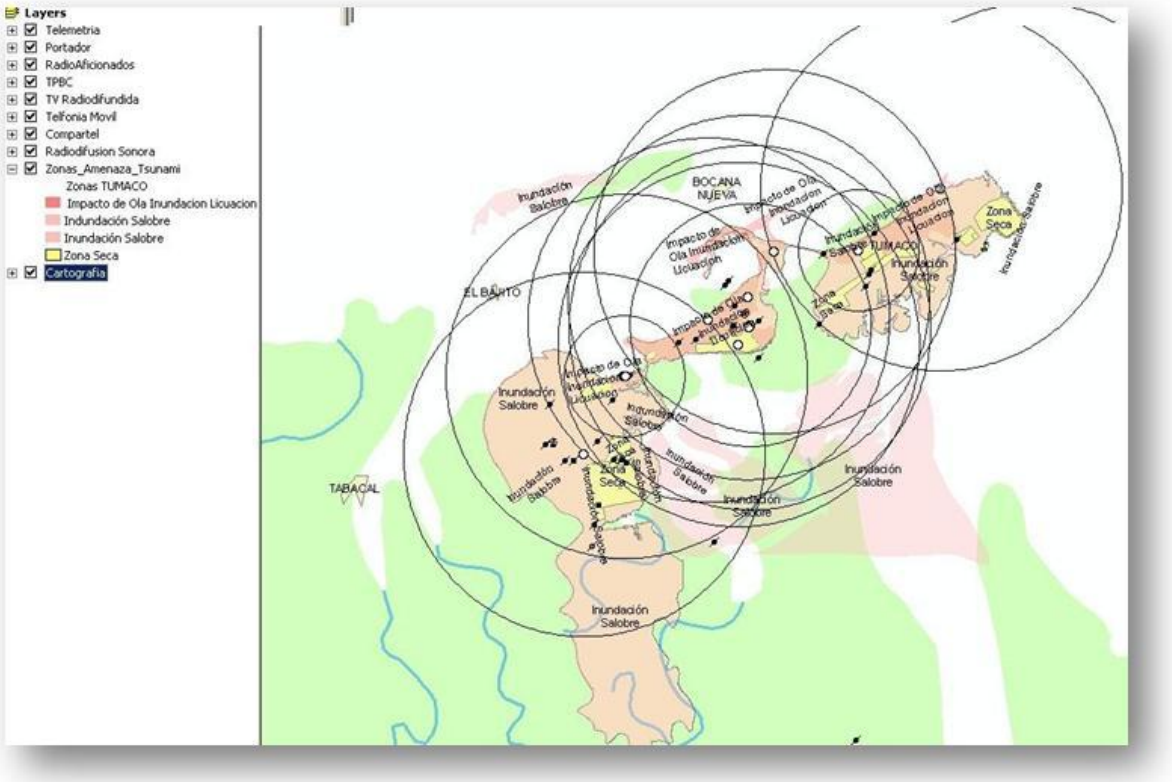
Zonas Amenazadas	Fase TSUNAMI a Modelar			5
Identificador del Elemento	GOLPE DE OLA	FUERZAS LAT	INUNDACIÓN	
33001	0.00%	0.00%	0.00%	
33002	0.00%	0.00%	0.00%	
33003	0.00%	0.00%	0.00%	

Zonas Amenazadas	Fase TSUNAMI a Modelar		5
Identificador del Elemento	GOLPE DE OLA	FUERZAS LAT	INUNDACIÓN
33004	0.00%	0.00%	0.00%
33005	0.00%	0.00%	0.00%
33006	0.00%	95.00%	95.00%

Fuente:CINTEL

Como resultado del proceso se tiene la siguiente información:

Figura 27. Mapa de Amenaza por Tsunami sobre la Infraestructura



Fuente: CINTEL

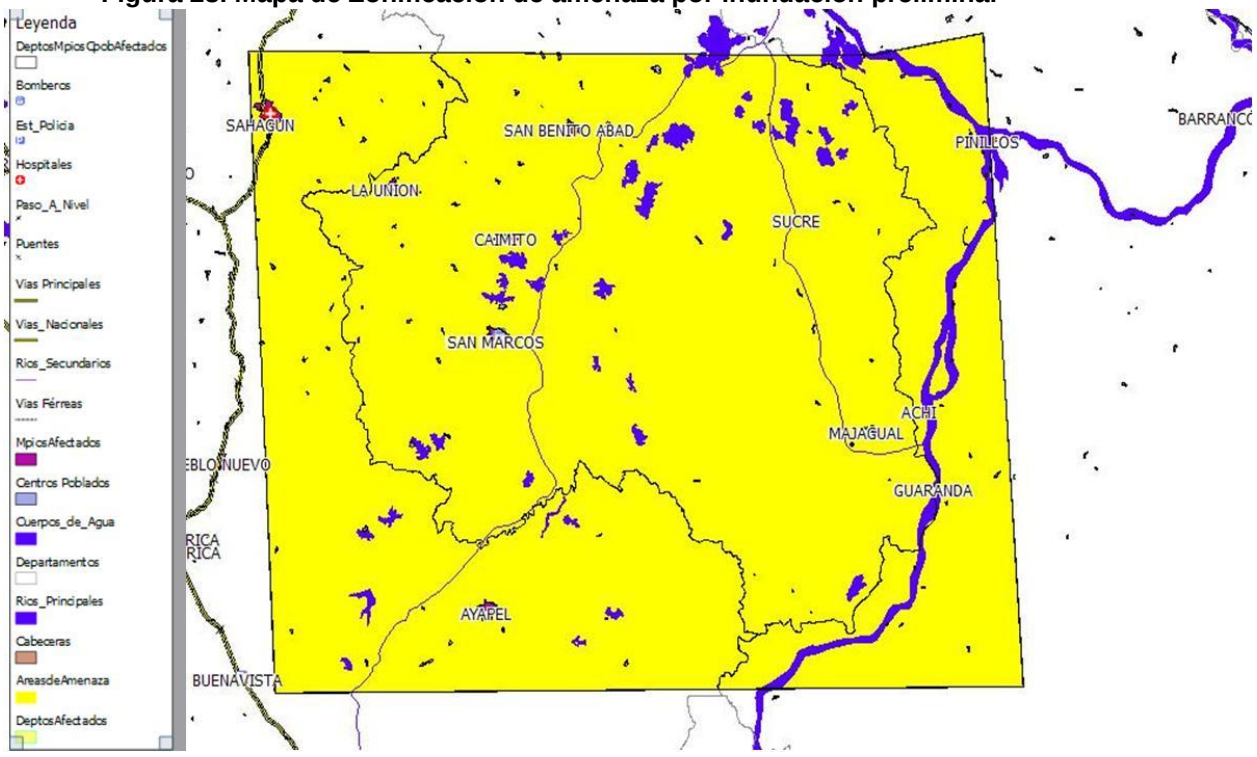
4.5 DIAGNÓSTICO DE AMENAZA POR INUNDACIÓN: SUCRE, LA MOJANA

4.5.1 Delimitación de la zona de estudio

Con el efecto de tener un área de cubrimiento general de toda la infraestructura de telecomunicaciones, se estableció un área que contemplara la Mojana en el sur de Sucre.

Sin embargo, el estudio detallado se realizó sobre el área de influencia cercana que tuviera alguna infraestructura de telecomunicaciones, dado que en la zona no existe una alta penetración de servicios de telecomunicaciones.

Figura 28. Mapa de Zonificación de amenaza por inundación preliminar



Fuente: CINTEL

El estudio se enfocó sobre la afectación de los municipios como Caimito, San Benito, Guaranda, Sucre, Majagual y San Marcos.

La zona está caracterizada por bajos relieves y zonas propensas a inundación natural, en las cuales los asentamientos humanos están normalmente cerca de las fuentes hídricas.

4.5.2 Valoración de la amenaza por inundación

El estudio en la siguiente etapa confrontará la información suministrada por los operadores, contra la información de asentamientos humanos obtenida por el IGAC y el DANE con el fin de establecer la correspondencia entre la amenaza de inundación de la zona contra la infraestructura instalada y la población servida.

Sin embargo y, dada la condición especial de la dura época invernal del último trimestre del año 2010, CINTEL procedió a elaborar un mapa de zonificación por amenaza de inundación tomando los siguientes criterios.

- Establecimiento de rondas de ríos, lagos y lagunas (mapas de hidrografía proporcionados por IGAC) por una extensión de 1 Km a cada lado de dichos elementos, de acuerdo a ajustes realizados tomando dicha distancia como un promedio de los peores escenarios de los municipios afectados en la zona.

- Cálculo de zonas por debajo de la cota de promedio de los ríos (de 20 a 25 msnm) de la zona, usando el Modelo Digital del Terreno, SRTM de 90 metros de la NASA.

La probabilidad de inundación estimada para la Zona de La Mojana se establece mediante la información del índice pluviométrico en un momento determinado (Meses), de tal forma que si supera la media anual se ajusta de

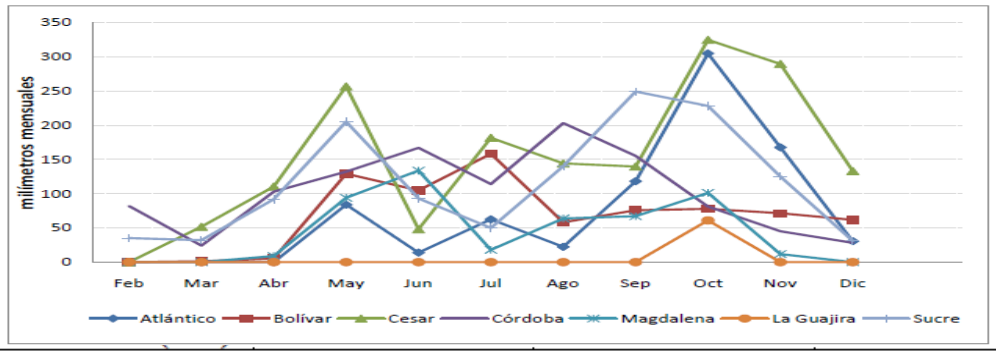
manera cualitativa aumentando la probabilidad estimada de ocurrencia de los eventos asociados a las lluvias y consecuentemente a las inundaciones en la zona.

Tabla 14. Tabla de resultados ejemplo de la calificación de la amenaza por inundación para un servicio específico

Valores Para el Cálculo de la Amenaza por Inundación en La Mojana			
Fase	**%**	**Máximo**	**Indicador**
1	0-25%	0%	Niveles de precipitación (Régimen de Lluvias por debajo del Promedio Anual para el Departamento)
2	26-60%	60%	Niveles de precipitación (Régimen de Lluvias por encima de la Media Anual para el Departamento)
3	61-100%	100%	Niveles de precipitación (Régimen de Lluvias igual o superior al Máximo Anual para el Departamento)

Estimados por CINTEL

Figura 29. Régimen de lluvias en el Caribe Continental



Clasificación	Rango de precipitación en mm	Área (km^2)	%
Árido	< 500 mm	9.236,77	6,98
Muy seco	501 – 1.000 mm	9.151,87	6,92
Seco	1.001 – 2.000 mm	80.509,09	60,88
Húmedo	2.001 – 3.000 mm	26.784,63	20,25
Muy húmedo	3.001 – 7.000 mm	6.561,63	4,96
Total		132.244,00	100,00

Fuente: Documentos de Economía Regional. Geografía económica del Caribe Continental. Luis Armando Galvis. N° 119 Diciembre, 2009. Banco de La República

4.5.3 Priorización y zonificación de la amenaza por inundación

Con base en los eventos ocurridos en la zona con respecto a eventos por inundación, se establece en detalle la valoración de la amenaza por inundación como alto, mediante la especialización de las consecuencias de los mapas de inundación del IDEAM u otras fuentes de información:

Las zonas de inundación para el área de La Mojana, han sido clasificadas como Alta si el elemento se encuentra al menos dentro de la ronda de ríos, lagos y lagunas determinadas por 1 Km, o están por debajo de la cota estimada con los datos de SRTM de la NASA; si esta cota está entre los 11 y los 25 metros se estima como amenaza Baja. Los niveles de pluviosidad que para el modelo determinan la probabilidad de ocurrencia son informados por las entidades gubernamentales relevantes.

Tabla 15. Tabla de valoración de la vulnerabilidad y el riesgo por inundación

DEPARTAMENTO	MUNICIPIO	ID_FUNCION	POB 2010	Zona Inundación	Distancia Ronda Metros	Amenaza Inundación	ZONA SRTM NASA	MSNM	Amenaza por Inundación de Agua Dulce
BOLÍVAR	MOMPOS	30006	42618	Lagos Lagunas	0	Alta	Baja	11 -25	Alta
BOLÍVAR	MONTECRISTO	30007		Rondas Rios	1000	Alta			Alta
BOLÍVAR	TIQUISIO	30008	20194	Rondas Rios	1000	Alta	Baja	11 -25	Alta
CÓRDOBA	AYAPEL	30010	46525	Rondas Rios	1000	Alta			Alta

Fuente: CINTEL

Posteriormente, se establece la probabilidad de ocurrencia del evento de acuerdo a la fase a modelar de tal manera que a medida que aumente el índice de pluviosidad de la región a analizar, reportada por las entidades competentes, se debe modificar en la etapa de inundación a modelar:

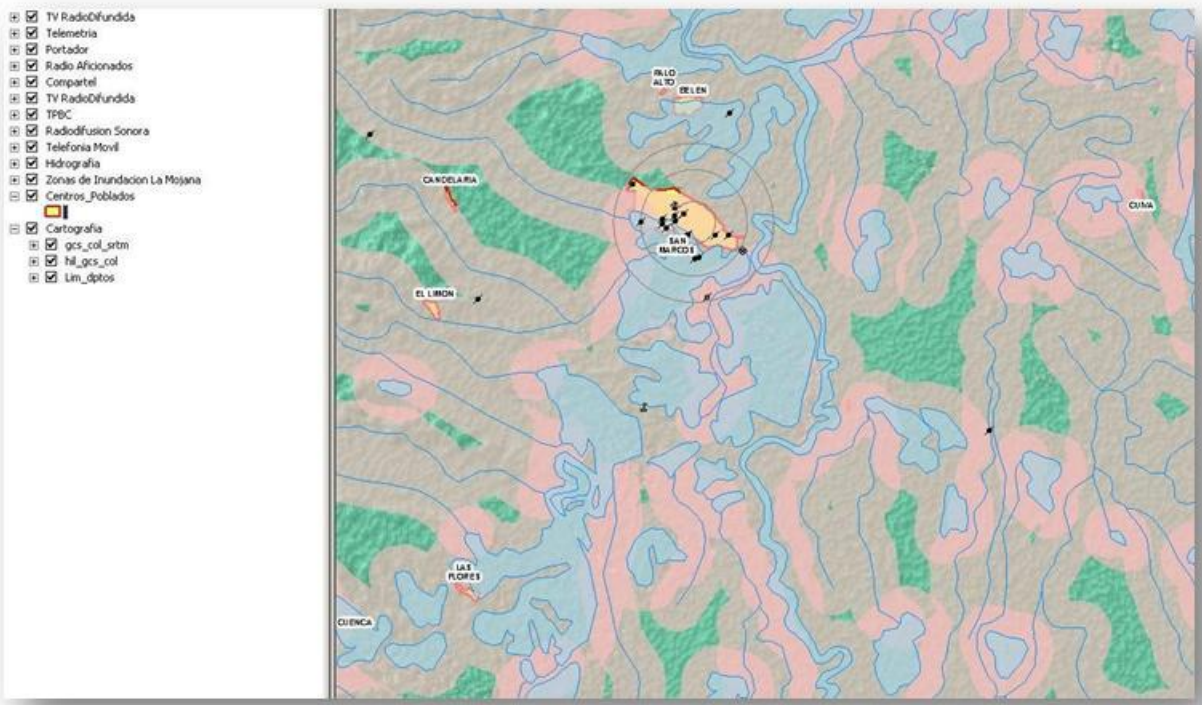
Tabla 16. Tabla de resultados ejemplo de la priorización de la amenaza por inundación para un servicio específico

Zonas Amenazadas	Etapa de Inundación a Modelar		2
Identificador del Elemento	ZONA AMENAZA	Afectación	Probabilidad de Inundación
30005	Alta	1	60.00%
30006	Alta	1	60.00%
30007	Alta	1	60.00%
30008	Alta	1	60.00%
30010	Alta	1	60.00%
30011	0	0	0.00%
30012	0	0	0.00%
30013	0	0	0.00%
30014	0	0	0.00%
30015	0	0	0.00%
30016	0	0	0.00%
30033	Alta	1	60.00%
30034	Alta	1	60.00%
30035	Alta	1	60.00%
30036	Alta	1	60.00%
30037	Alta	1	60.00%
30038	Alta	1	60.00%
Grand Total		**1**	**60%**

Fuente: CINTEL

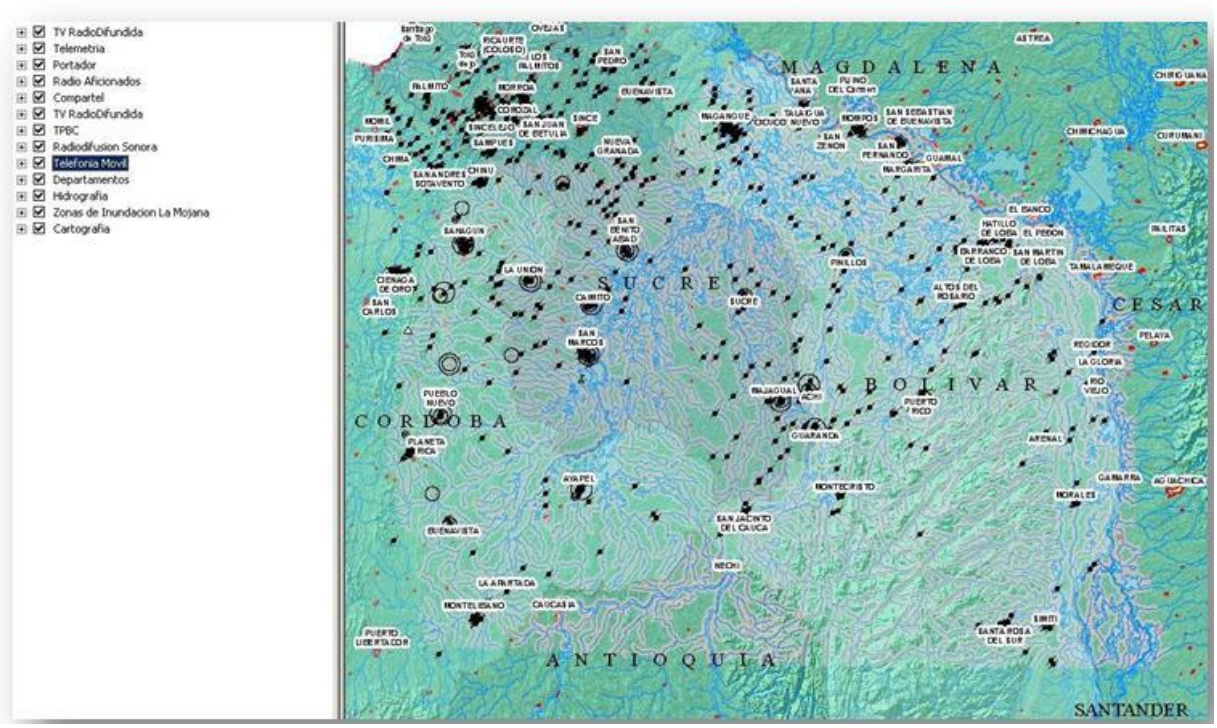
Como resultado del proceso se tiene la siguiente información:

Figura 30. Mapa de Amenaza por Inundación sobre la Infraestructura. Municipio de San Marcos



Fuente: CINTEL

Figura 31. Mapa de Amenaza por Inundación sobre la Infraestructura. La Mojana



Fuente: CINTEL

5 DIAGNÓSTICO DE VULNERABILIDAD DE REDES BÁSICAS DE TELECOMUNICACIONES

En este capítulo se presenta el diagnóstico de vulnerabilidad de las redes de telecomunicaciones definidas como base. Se presenta el análisis que lleva a la determinación de las redes y servicios vitales de telecomunicaciones, se describe la topología general de los servicios vitales de telecomunicaciones y sus elementos básicos, se analiza la vulnerabilidad de las redes vitales de telecomunicaciones, la vulnerabilidad física de los elementos de dichas redes tales como edificaciones, torres/antenas, armarios, gabinetes y shelters, redes de fibra óptica y de cobre, entre otros, y por último se analiza la vulnerabilidad funcional de los servicios de telecomunicaciones vitales definidos.

5.1 REDES Y SERVICIOS VITALES DE TELECOMUNICACIONES

5.1.1 Determinación de las redes y servicios vitales de telecomunicaciones

Se consideran líneas vitales a aquellos servicios y redes que son fundamentales para preservar la continuidad y el bienestar de la sociedad. Dentro de éstos se contemplan las redes de agua potable, eléctricas, de transporte y telecomunicaciones, entre otras.

Las redes vitales de telecomunicaciones a su vez están compuestas por diferentes redes asociadas a la prestación de múltiples servicios de telecomunicaciones, cuya importancia relativa depende de la penetración o uso que de un servicio específico haga una sociedad en sus diferentes sectores sociales y económicos y, del momento histórico en el que se realice su análisis.

Es así, que a finales de los años noventa, en Colombia los servicios de telefonía pública básica conmutada local (TPBCL) y el beeper, se destacaban como los principales servicios de telecomunicaciones "personales" de la población en general y se constituían en servicios vitales de telecomunicaciones "personales".

Actualmente, en Colombia y a nivel internacional, sin lugar a dudas, los servicios de telefonía móvil celular, PCS y trunking y los servicios de acceso a INTERNET se constituyen en servicios vitales para la totalidad de los sectores sociales y económicos del país.

En la Tabla 17 se pueden observar las cifras que soportan esta evolución en la "vitalidad" de los servicios mencionados en función de la penetración[20].

Tabla 17. Evolución de la penetración de TPBCL, celular y acceso a internet

	AÑO 2000	AÑO 2005	AÑO 2009
Lineas de TPBCL en servicio	7.170.777	7.665.067	7.473.867
Habitantes	40.282.217	42.888.592	44.977.758
Penetración TPBCL	17,8%	17,9%	**16,6%**
Líneas Celular	2.256.801	21.849.993	41.154.630
Habitantes	40.282.217	42.888.592	44.977.758
Penetración	5,6%	50,9%	**91,5%**
TOTAL INTERNET FIJO	150.692	687.817	2.266.151
Habitantes	40.282.217	42.888.592	44.977.758
Penetración	0,4%	1,6%	**5,0%**
Accesos Banda Ancha	9698	318.863	2.012.328
Habitantes	40.282.217	42.888.592	44.977.758
Penetración	0,0%	0,7%	4,5%
Accesos xDSL	-	117.548	1.293.532
Habitantes	40.282.217	42.888.592	44.977.758
Penetración	0,0%	0,3%	2,9%
Otros Acceso Banda Ancha	9.698	201.135	718.796
Habitantes	40.282.217	42.888.592	44.977.758
Penetración	0,0%	0,5%	1,6%
Accesos Banda Angosta	150.692	368.954	253.823
Habitantes	40.282.217	42.888.592	44.977.758
Penetración	0,4%	0,9%	0,6%
Accesos Conmutados	150.692	368.954	50.603
Habitantes	40.282.217	42.888.592	44.977.758
Penetración	0,4%	0,9%	0,1%
Otros Accesos banda angosta	-	-	203.220
Habitantes	40.282.217	42.888.592	44.977.758
Penetración	0,0%	0,0%	0,5%
INTERNET MOVIL (suscripción)	ND	ND	915.280
Penetración	ND	ND	**2,0%**

Fuente: CINTEL

[20] **Bajo la categoría de celular se incluye PCS y NO se incluyen usuarios de trunking**

Se observa que la penetración del servicio de telefonía pública básica conmutada local (TPBCL) del año 2000 a 2009, tiene una pérdida de 1,2%, mientras que los servicios de telefonía celular pasan de una penetración de 5,6% a 91,5 %.

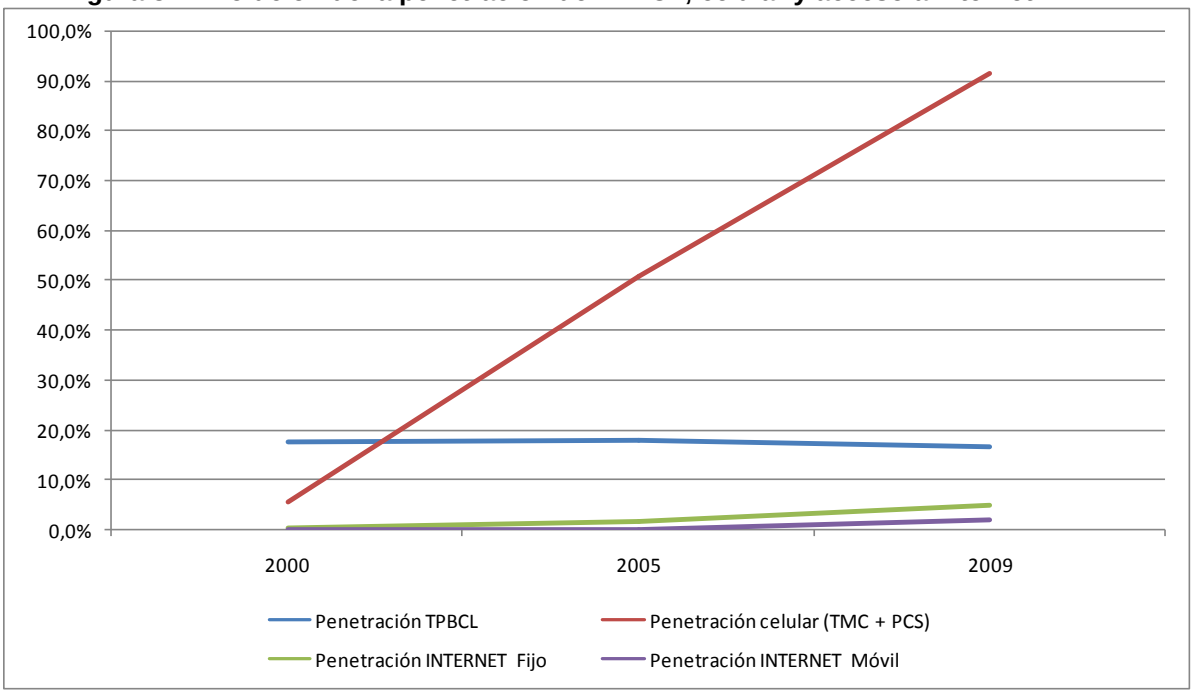
Con relación al acceso fijo a INTERNET, para el mismo período analizado, la penetración se incrementa notoriamente de 0,4% a 5% y el acceso móvil se posiciona con una penetración del 2%.

En este análisis sin embargo, se debe puntualizar que la penetración del servicio de acceso fijo a INTERNET se encuentra explicada en cerca de un 60% por los accesos xDSL (2,9%) y el acceso conmutado (0,1%), accesos soportados por la red de TPBCL, lo cual permite concluir que aunque la TPBCL ha perdido penetración, se constituye en una red vital, tanto por su importancia como red soporte de INTERNET, como por la importancia propia del servicio de TPBCL.

De manera análoga, las redes de servicios de telefonía celular, adicional a la importancia vital en función de la penetración anotada, son soporte a los accesos móviles de INTERNET, que como ya se mencionó han tenido en los últimos años un aumento evidente en su penetración.

La Figura 32, permite observar la penetración de los servicios vitales de comunicaciones móviles (telefonía móvil celular + PCS), telefonía pública básica conmutada local y acceso a INTERNET.

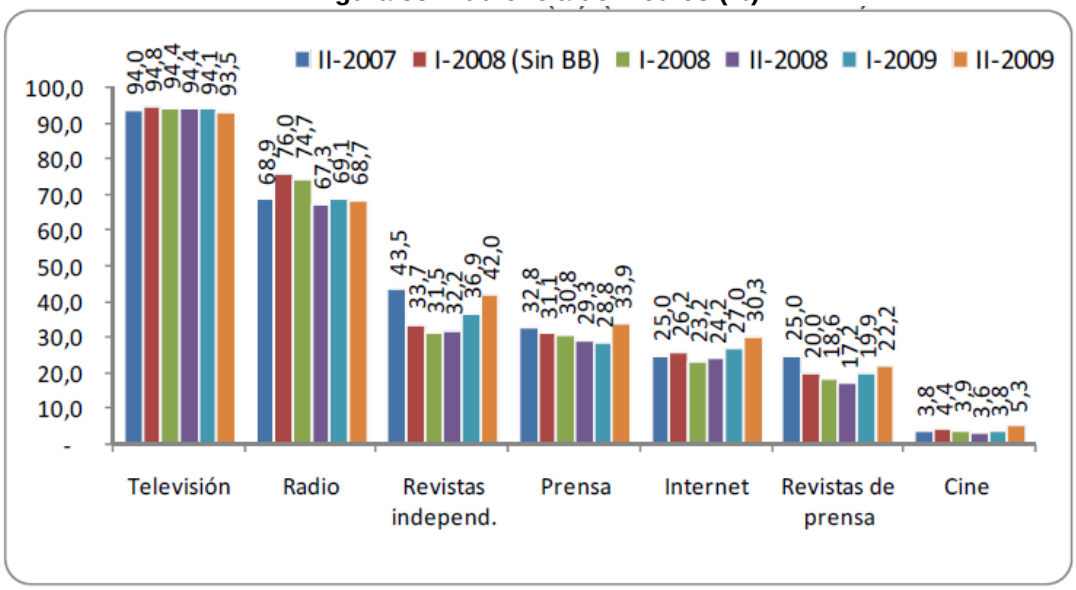
Figura 32. Evolución de la penetración de TPBCL, celular y acceso a internet



Fuente: CINTEL

Por otro lado, deben considerarse como servicios vitales de telecomunicaciones los servicios radiodifundidos de televisión y radio, dado que según su finalidad de formar, informar y entretener, son fundamentales para la continuidad de la sociedad. Según el estudio general de medio correspondiente a 2009 - II, estos servicios contaban con una audiencia del 93,5% y 68,7% respectivamente.

Figura 33. Audiencia de medios (%)



Fuente: ACIM - EGM - CNTV

Ahora bien, considerando la importancia que para la sociedad actual y su bienestar tiene la infraestructura de transporte aéreo y marítimo, para cuya operación son básicos los servicios de móvil aeronáutico y marítimo respectivamente en cuanto a la radionavegación, aproximación y maniobras en tierra, estos servicios se consideran como vitales dentro de la línea vital de las telecomunicaciones.

Otros servicios que en condiciones normales no resaltan como fundamentales, pero que en eventos desastrosos adquieren su real importancia, son los servicios de comunicaciones de emergencias que juegan un papel destacado en las situaciones de desastre. Estos servicios, permiten que la población y la sociedad en general afectada por un evento desastroso, recupere rápidamente los niveles de bienestar estándar existentes al momento antes de su ocurrencia, razón por la cual son vitales para la sociedad.

Finalmente, el servicio portador se destaca como vital, dada su transversalidad a los demás servicios, ya que soporta local, regional, nacional e internacionalmente, la gran mayoría de las redes de los servicios de telecomunicaciones consideradas como vitales.

En conclusión, para el presente estudio se consideran como redes vitales de telecomunicaciones las conexas a los siguientes servicios:

Tabla 18. Redes vitales consideradas para el estudio

1	Portador
2	Telefonía Celular
3	Telefonía Pública Basica Conmutada Local
4	INTERNET
5	Televisión
6	Radiodifusión sonora A.M. & F.M.
7	Móvil Aeronáutico
8	Móvil Marítimo
9	Comunicaciones de Emergencia

Fuente: CINTEL

La Figura 34 ilustra cómo en la sociedad moderna, las Tecnologías de la Información y las Comunicaciones (TIC), dentro de las cuales lógicamente están comprendidas los servicios mencionados, se constituyen en una línea vital básica para mantener y mejorar el bienestar de la sociedad. Las TIC son totalmente transversales a los demás sectores de la sociedad, actualmente no se podría concebir básicamente ninguna actividad del ser humano ajena a la influencia o dependencia de las TIC.

Figura 34. TIC Línea Vital en la Sociedad Moderna

Fuente: CINTEL

Específicamente, en la administración de desastres las TIC juegan un papel fundamental en sus diferentes etapas (Figura 35), así:

- **Prevención y preparación:** en esta etapa, los servicios de comunicación masiva, tales como radiodifusión sonora, televisión e INTERNET, se constituyen en los medios obligados, dada su penetración, para capacitar y preparar en forma masiva y coherente a la población en general y a las entidades y organizaciones en todos los temas relacionados con las cuatro fases de la administración de desastres.

  En esta etapa adicionalmente, las TIC están incorporadas en las redes y sistemas de telemetría y alertas tempranas, tanto a nivel de las redes satelitales, de microondas y transmisión de

datos a través de las redes de telefonía móvil celular y en los sistemas de tratamiento de datos de éstas.

- **Respuesta:** en esta fase de la administración de desastres, las TIC son fundamentales, ya que a través de las redes de radiodifusión sonora, televisión e INTERNET, se mantiene informada a la población y se apoyan las actividades de salvamento, búsqueda y rescate.

  En esta fase, entran a jugar un papel decisivo las comunicaciones de las redes de TPBCL y telefonía móvil celular con relación al acceso de la población a los organismos de emergencia directamente o a través de los números únicos previstos para estos eventos, al igual que como apoyo a las actividades de éstos, permitiendo su intercomunicación. Sin embargo, es de anotar que estas redes históricamente han colapsado por la congestión en su acceso, limitando de esta manera su utilidad en esta fase.

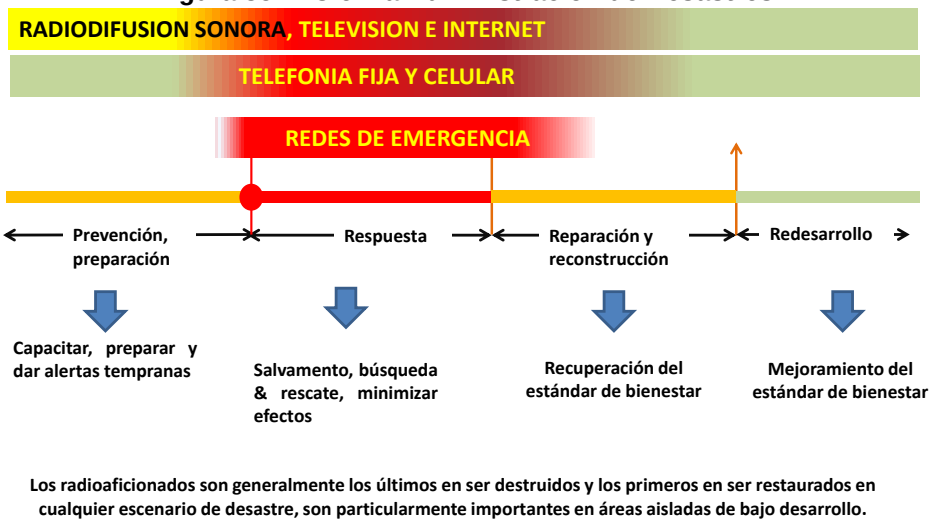
  Finalmente, en las actividades de salvamento, búsqueda y rescate, el papel preponderante lo tienen las redes de emergencia, que permiten coordinar a través de redes de radio normalmente operando en VHF, las actividades de organismos tales como: cruz roja, defensa civil, bomberos, entidades de salud, autoridades municipales, policía y ejército nacional. Los radioaficionados juegan un papel muy importante en el apoyo de estas actividades, debido a que su infraestructura de comunicaciones a nivel de radios, sistema radiante y energía, no representa mayores complejidades para su operación y/o restauración en caso de destrucción.

  En esta fase de respuesta, se deberá priorizar la restauración de los servicios de telecomunicaciones, aún por encima de los de energía eléctrica, ya que mediante éstos y dadas las múltiples relaciones que existen entre las TIC y los demás sectores, se facilitará la restauración de otros servicios vitales

cuya rápida restauración es fundamental en la etapa de respuesta al desastre.

- **Reparación y construcción:** como ya se mencionó, la restauración de las telecomunicaciones es prioritaria y debe comenzar desde la fase de respuesta, ya que está facilitará que las demás líneas vitales sean reparadas y construidas nuevamente, permitiendo que se recupere rápidamente el estándar de bienestar de la sociedad afectada.
- **Redesarrollo:** en esta etapa y ya recobrado el bienestar mínimo aceptable de la sociedad, se realiza el redesarrollo de los diferentes sectores afectados, repensando, rediseñando y construyendo con base en las lecciones aprendidas y creando infraestructura más resistente, menos expuesta y en fin menos vulnerable a los eventos desastrosos, de tal manera que se evite la recurrencia. En el redesarrollo, las TIC son protagonistas, ya que son fundamentales para el análisis, planeación, diseño y construcción de nueva infraestructura, para la modernización y disminución de la vulnerabilidad mediante la incorporación de TIC en los diferentes procesos de todos los sectores de la sociedad.

Figura 35. TIC en la Administración de Desastres



Fuente: CINTEL

Con el fin de ilustrar la definición de servicios vitales, se presenta en líneas generales una metodología utilizada en Holanda para determinar los sectores de infraestructura vitales para su economía y los resultados obtenidos[21].

La metodología utilizó como instrumento clave la elaboración de cuestionarios y encuestas a los diferentes sectores económicos de la sociedad holandesa, con el fin de evidenciar en forma directa la importancia de los diferentes sectores de infraestructura y las relaciones de interdependencia.

---

[21] **Critical (information) Infrastructure Protection in The Netherlands. Eric A.M. Luiijf, Helen H. Burger, Marieke H.A. Klaver TNO Physics and Electronics Laboratory (TNO-FEL)**

Los 11 sectores de infraestructura y los correspondientes productos o servicios sobre los cuales se realiza el análisis de vitalidad, se presentan en la Figura 36.

Figura 36. Sectores, productos y servicios críticos en Holanda

Table 1: The 11 Dutch critical sectors and their 31 critical products and services

No.	Sector	Product or service
1	**Energy**	Electricity
2		Natural gas
3		Oil
4	**Telecommunications**	Fixed telecommunication networks services [3]
5		Mobile telecommunication services
6		Radio communication and navigation
7		Satellite communication and General Positioning System
8		Broadcast services (radio and TV)
9		Internet access
10		Postal and courier services
11	**Drinking water**	Drinking water supply
12	**Food**	Food supply and food safety
13	**Health**	Health care
14	**Financial**	Financial services and financial infrastructure (private)
15		Financial transfer services (government)
16	**Retaining and managing**	Management of water quality
17	**surface water**	Retaining and managing water quantity
18	**Public Order and Safety**	Maintaining public order
19		Maintaining public safety
20	**Legal order**	Administration of justice and detention
21		Law enforcement
22	**Public administration**	Diplomacy
23		Information provision by the government [4]
24		Armed Forces / Defence (emergency support tasks)
25		Public administration
26	**Transport**	Road transport
27		Rail transport
28		Air transport
29		Inland navigation
30		Ocean shipping
31		Pipelines

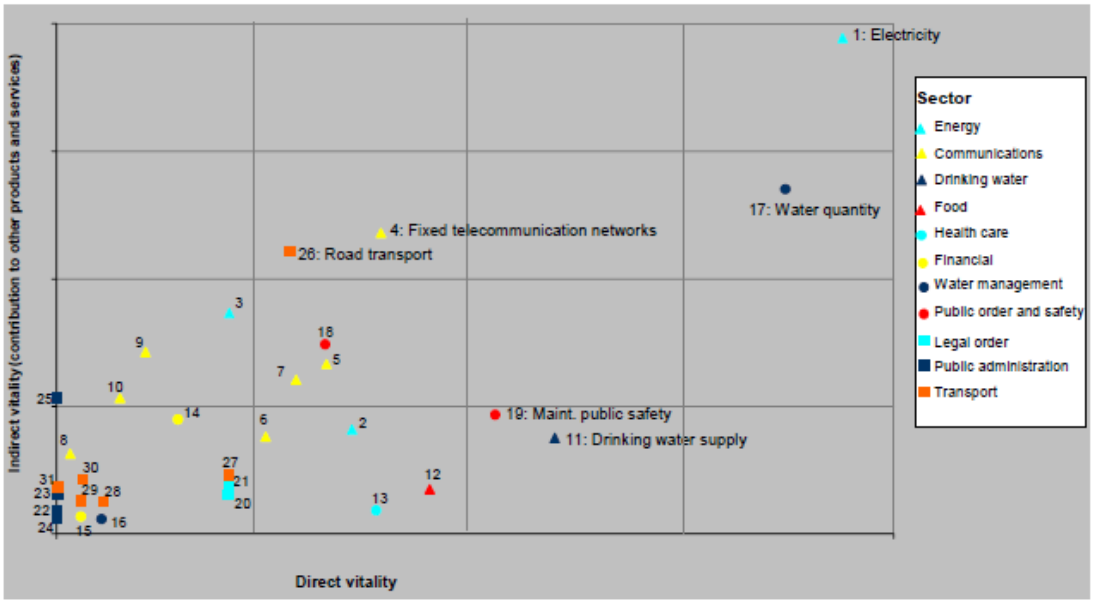
[3] This includes POTS, microwave links, cable and leased lines.
[4] This comprises weather service, citizenship registries and other public information services, etceteras.

Fuente: Critical (information) Infrastructure Protection in The Netherlands. Eric A.M. Luiijf, Helen H. Burger, Marieke H.A. KlaverTNO Physics and Electronics Laboratory (TNO-FEL)

Con relación al sector de las telecomunicaciones, materia del presente estudio, es claro que los servicios considerados bajo el análisis de penetración en Colombia son consistentes con los considerados en el análisis de criticidad en Holanda como reflejo de lo que acontece a nivel internacional, excepto los servicios postales que no están en el alcance del presente estudio.

Partiendo de la definición de vitalidad directa como la contribución que un producto o servicio da a la continuidad y bienestar de la sociedad y, que la vitalidad indirecta se estableció como la cantidad en que otros productos y servicios críticos contribuyen a la dependencia de un producto o servicio crítico, es importante evidenciar (Figura 37), que las redes de telecomunicaciones fijas están en el sexto lugar de vitalidad directa, después de electricidad, cantidad de agua, suministro de agua potable, mantenimiento de la seguridad pública y alimentos y con relación a la vitalidad indirecta es el sector que más contribuye a la sociedad después de electricidad, y cantidad de agua.

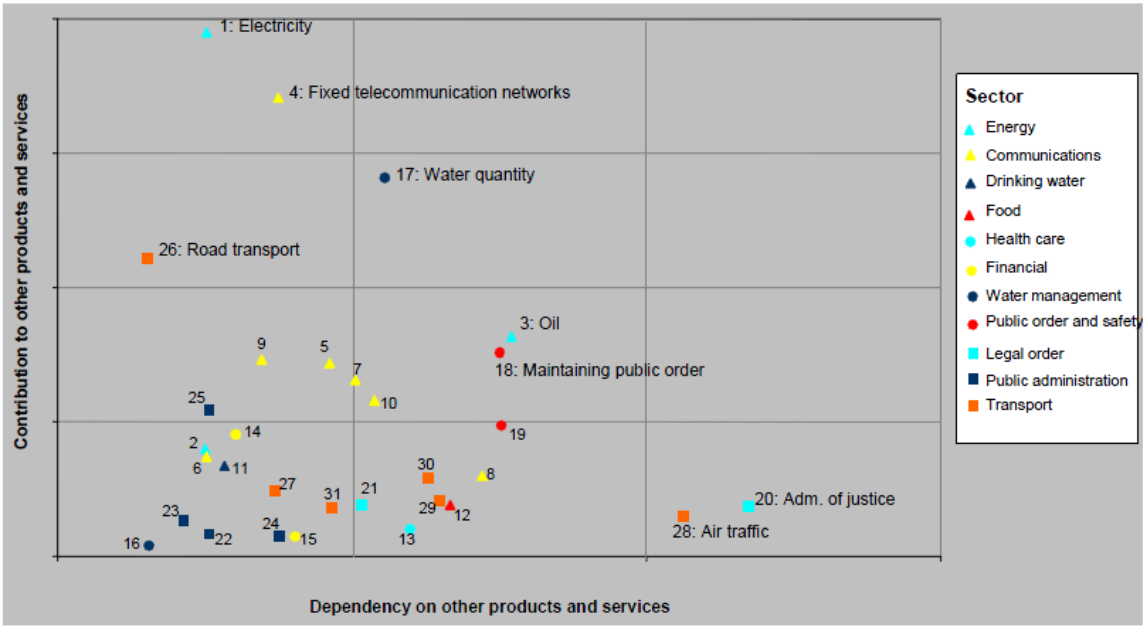
Figura 37. Vitalidad directa e indirecta - Holanda



Fuente: Critical (information) Infrastructure Protection in The Netherlands. Eric A.M. Luiijf, Helen H. Burger, Marieke H.A. KlaverTNO Physics and Electronics Laboratory (TNO-FEL)

Con relación a la dependencia, la Figura 38 permite observar que las redes de telecomunicaciones fijas son las que más contribuyen a otros productos y servicios, después de la electricidad, que es el servicio que más contribuye. Es claro al observar el eje x, que todos los servicios de telecomunicaciones están en la región de baja dependencia, pero por encima de electricidad.

Figura 38. Contribución y dependencia - Holanda



Fuente: Critical (information) Infrastructure Protection in The Netherlands. Eric A.M. Luiijf, Helen H. Burger, Marieke H.A. KlaverTNO Physics and Electronics Laboratory (TNO-FEL)

5.1.2 Descripción, topología general de los servicios vitales de telecomunicaciones y sus elementos básicos

5.1.2.1 Servicio Portador

El servicio portador fue definido por el Decreto 1900 de 1990 como un servicio básico que permite la transmisión de señales entre dos o más puntos definidos en la red de telecomunicaciones a través de redes conmutadas y

no conmutadas, incluyendo servicios tales como el arrendamiento de pares aislados y de circuitos dedicados, entre otros[22].

La transmisión de señales en las redes de portador se realiza básicamente a través de fibra óptica, dada su alta capacidad de transporte, pero adicionalmente se utilizan otros medios como microondas y satélite, según las dificultades geográficas para la instalación de las redes, tamaños de mercado y redundancias requeridas.

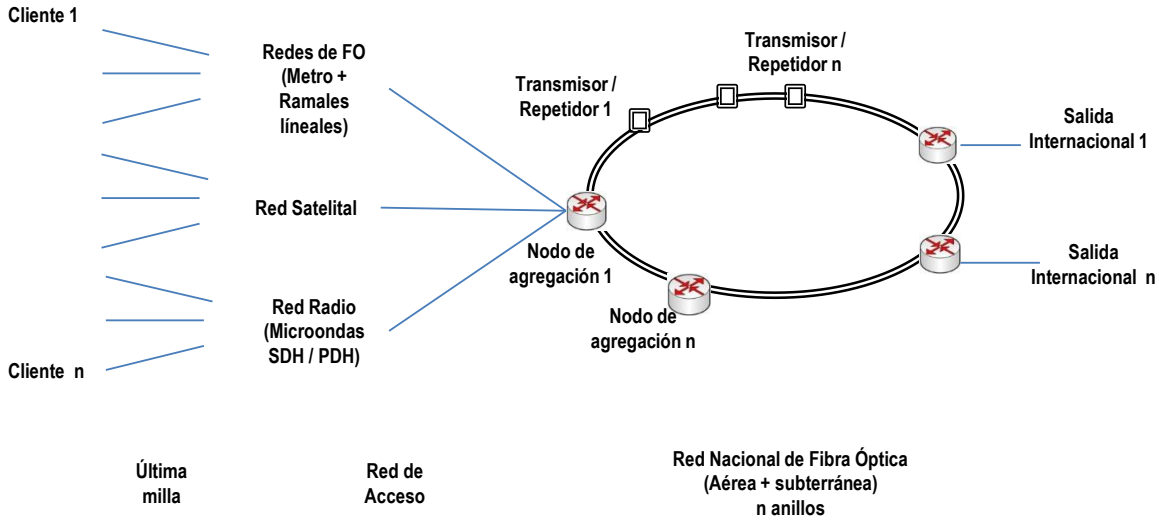
Las redes de portador utilizan diferentes niveles de redundancia en la transmisión de sus señales, en las redes de fibra óptica a nivel de diversidad de ruta, en las de radio mediante la utilización de radios 1+n y de forma combinada para obtener redundancia de medio.

La Figura 39 muestra la topología general de red del servicio portador; el backbone nacional del servicio portador es en fibra óptica (Figura 40), así como la mayoría de sus ramales cuando el tráfico lo justifica. En los otros casos, por razones de ubicación geográfica o de mercado, se utilizan radioenlaces o comunicaciones satelitales, de diferentes capacidades y en diferentes configuraciones. En las grandes ciudades, el servicio portador se presta a través de redes metro.

---

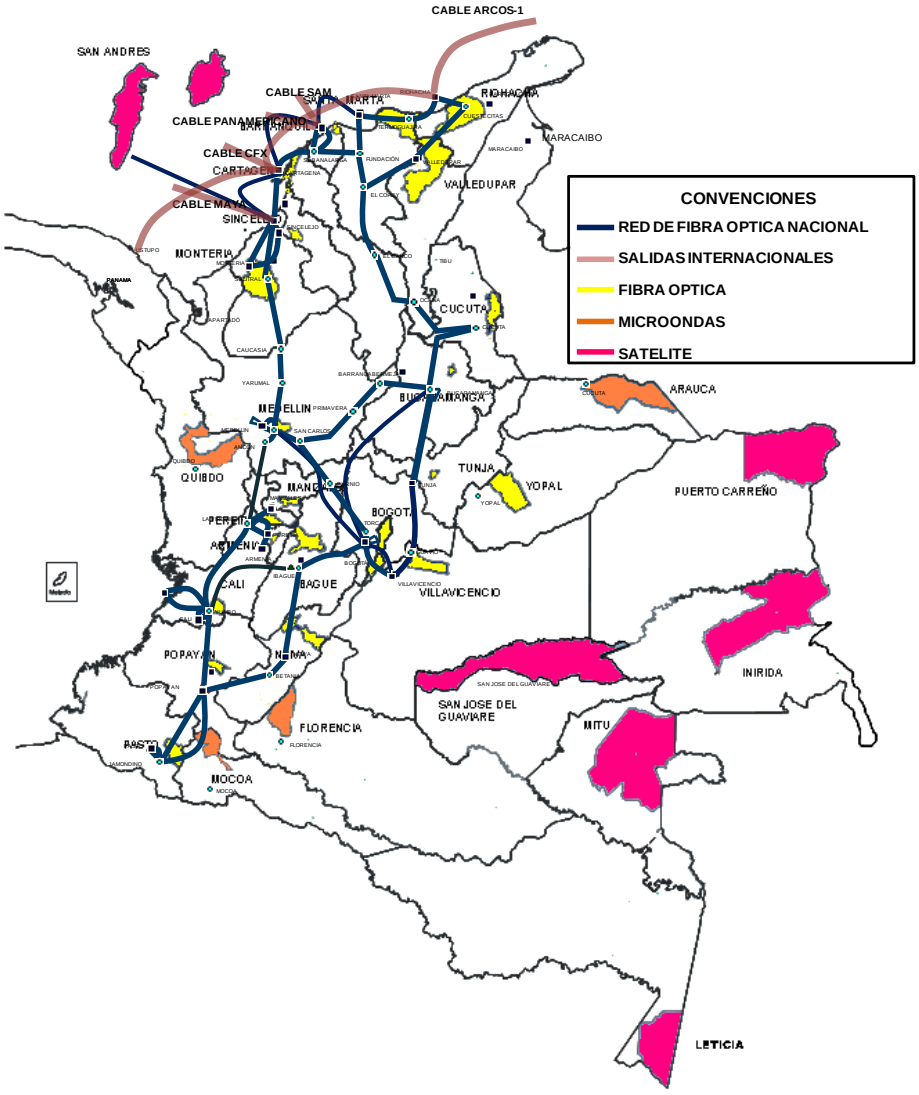
[22] Decreto 1900 de 1990. Artículo 28. Los servicios básicos comprenden los servicios portadores y los teleservicios. Servicios portadores son aquellos que proporcionan la capacidad necesaria para la transmisión de señales entre dos o más puntos definidos de la red de telecomunicaciones. Estos comprenden los servicios que se hacen a través de redes conmutadas de circuitos o de paquetes y los que se hacen a través de redes no conmutadas. Forman parte de éstos, entre otros, los servicios de arrendamiento de pares aislados y de circuitos dedicados.

Figura 39. Topología servicio Portador



Fuente: CINTEL

Figura 40. Redes de servicio Portador en Colombia



Fuente: CINTEL - Operadores

El servicio portador tiene cobertura local (municipios), regional, nacional y permite conectar a Colombia con el mundo a través de las diferentes salidas de cable submarino instaladas.

Las capacidades y rutas del servicio portador varían según operador y como se puede notar en la Figura 40, éstos se concentran en la región Andina, donde habita la mayor cantidad de población y, donde se encuentra instalada la mayor infraestructura de telecomunicaciones, de la cual es soporte el servicio portador y donde se explica un alto porcentaje del PIB nacional.

La fibra óptica utilizada en la red del servicio portador a nivel nacional se instala, bien haciendo uso de la infraestructura eléctrica mediante la utilización de cables OPGW (Optical Fiber Ground Wire) que tienen la funcionalidad de transporte de telecomunicaciones a través de la fibra óptica y la función de aterrizaje eléctrico; mediante cables ADSS (self supporting aerial fiber) que son cables de fibras aéreas autosoportados sobre postería de baja o media tensión; o a través de fibra óptica instalada en ductos y canalizaciones subterráneas y sobre postería especialmente instalada para transporte de telecomunicaciones.

Lo anterior, permite concluir que los principales elementos físicos de la red de portador, expuestos a amenazas naturales son:

- Redes aéreas de fibra óptica
- Redes subterráneas de fibra óptica
- Edificaciones donde se encuentran instalados los equipos de transmisión y repetición y, energía de respaldo.
- Edificaciones donde se encuentran instalados los nodos de servicio locales (nodos de servicio municipal), los nodos de agregación nacional y de conexión internacional y energía de respaldo.
- Torres, antenas y cuartos de equipos de sitios de transmisión de microondas y/o satelital donde se encuentran instalados los

equipos de microondas y/o comunicación satelital y la energía de respaldo.

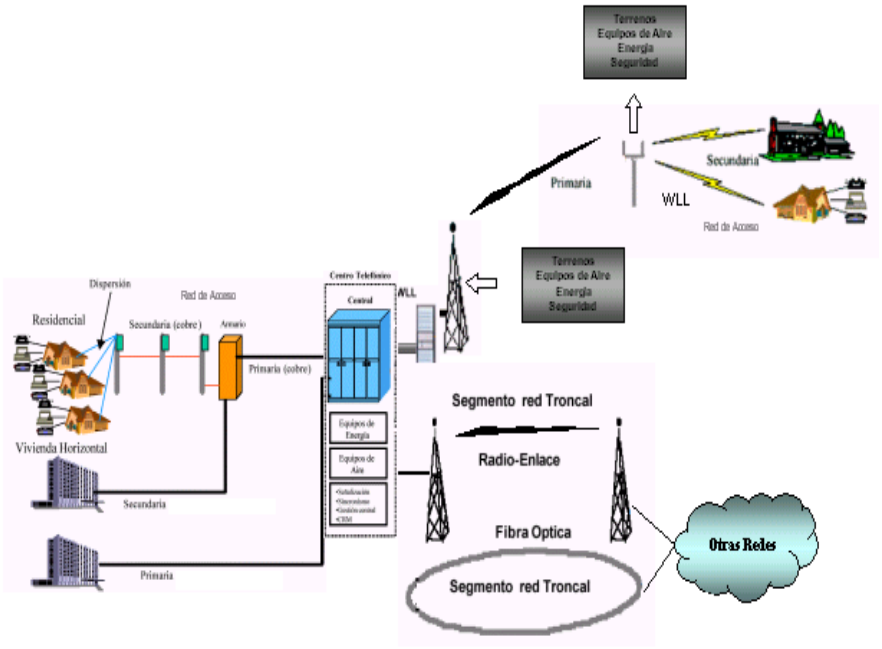
5.1.2.2 Servicio de Telefonía Pública Básica Conmutada Local

El servicio de telefonía pública básica conmutada (TPBC), según lo establece la Resolución No. 87 de la Comisión de Regulación de Telecomunicaciones, es el servicio básico de telecomunicaciones cuyo objeto es la transmisión conmutada de voz a través de la Red Telefónica Pública Conmutada (RTPC)[23], con acceso generalizado al público.

La Figura 41 ilustra los principales elementos de la red de TPBCL.

[23] **RTPC es el conjunto de elementos que hacen posible la transmisión conmutada de voz, con acceso generalizado al público, tanto en Colombia como en el exterior. Incluye las redes de los operadores de TPBCL, TPBCLE, TMR y TPBCLD. Fuente: Resolución 87 - CRC**

Figura 41. Elementos básicos de la red de TPBCL



MODULOS FUNCIONALES	ELEMENTOS DE RED
Centro Telefónico	Etapa de Abonado
	Etapa Troncal
	Sistema de Procesamiento y Control
	Matriz de Conmutación
	Sistema de señalización, sincronismo y gestión
	Equipos de fuerza y aire acondicionado
Red Troncal	Cables de fibra óptica y radioenlaces
	Equipos de microondas, multiplexores, ADM, crossc conectores digitales (DXC), conectores (pigtails, paneles de conexión ópticos (ODF), interfases de red, regeneradores, convertidores, amplificadores, tarjetas de red, entre otros.
	Canalizaciones, ductos y subductos, torres, antenas, mástiles, entre otros
Red Primaria	Cables de cobre y fibra óptica
	Canalizaciones, cámaras, ductos y subductos
	Armarios, concentradores remotos
Red Secundaria	Cables de cobre o fibra óptica
	Canalizaciones, cámaras, ductos, subductos y postes
	Herrajes, cajas de dispersión, conectores, entre otros
Red de Dispersión	Acceso alámbrico: Cable neopren, herrajes y conectores
	Acceso inalámbrico: estación base (subbastidores, tarjetas de energía, de control, de interfaz digital V5.2, distribuidor, racks); antenas, terminales fijas de abonado entre otros

Fuente: CINTEL - Julio 2003

Los centros telefónicos (centrales de conmutación), establecen la conexión física entre dos abonados de la RTPC y están jerarquizados en función de la cercanía al abonado. En general, se distinguen dos jerarquías: las centrales de conmutación urbana que son la de jerarquía más baja en la red y los nodos de jerarquía superior, que permiten la interconexión con otros operadores. Estas centrales se albergan en edificaciones normalmente construidas bajo normas antisísmicas.

Entre una central de conmutación, las otras centrales, otros operadores y los abonados conectantes existe un camino físico, el cual puede ser totalmente alámbrico o inalámbrico, según el diseño de red del operador, el cual está segmentado física y funcionalmente así:

Red Troncal: Es el segmento de red que une las diferentes centrales de una red o la red de TPBCL con otras redes. La red troncal en su generalidad está construida mediante enlaces de fibra óptica. Dependiendo de la topografía y de la disponibilidad de la fibra, se utilizan alternativamente en menor grado, enlaces de microondas y excepcionalmente enlaces satelitales. Esta red troncal puede ser propia o utilizar los servicios de portador parcial o totalmente.

La red troncal a nivel local, normalmente utiliza fibra óptica instalada en ductos y canalizaciones subterráneas, en configuraciones normalmente redundantes (anillos) y dependiendo del operador de servicio portador que establezca la conexión de fibra óptica con otras redes, éstas pueden ir a través de canalizaciones subterráneas, ir a través de postes o a través de la infraestructura eléctrica de alta y media tensión.

La construcción de las canalizaciones y ductería se realiza bajo estrictas normas de entidades como ICONTEC y normas propias desarrolladas por los operadores de TPBCL.

Red primaria: es la porción de la red que conecta el distribuidor principal de la central telefónica con los armarios; esta red normalmente es implementada en cobre, está canalizada y normalmente es de propiedad del operador de TPBCL.

Cuando el operador utiliza acceso fijo inalámbrico (wireless local loop) y dependiendo de la topología de red, este segmento se reemplaza por espectro radioeléctrico en las bandas que el Ministerio de Tecnologías de la Información y las Comunicaciones haya entregado en concesión al operador de TPBCL.

Hacen parte de la Red Primaria, los armarios y concentradores remotos, los cuales dependen de la central matriz urbana para el enrutamiento y la gestión.

Red secundaria: Esta red conecta los armarios con las cajas de dispersión. Normalmente, está construida en cobre y dependiendo de las normas de planeamiento municipal, pueden ir a través de postes o canalizadas y ductadas.

Cuando el operador utiliza acceso fijo inalámbrico (wireless local loop), este segmento se reemplaza por espectro radioeléctrico en las bandas que el Ministerio de Tecnologías de la Información y las Comunicaciones haya entregado en concesión al operador de TPBC.

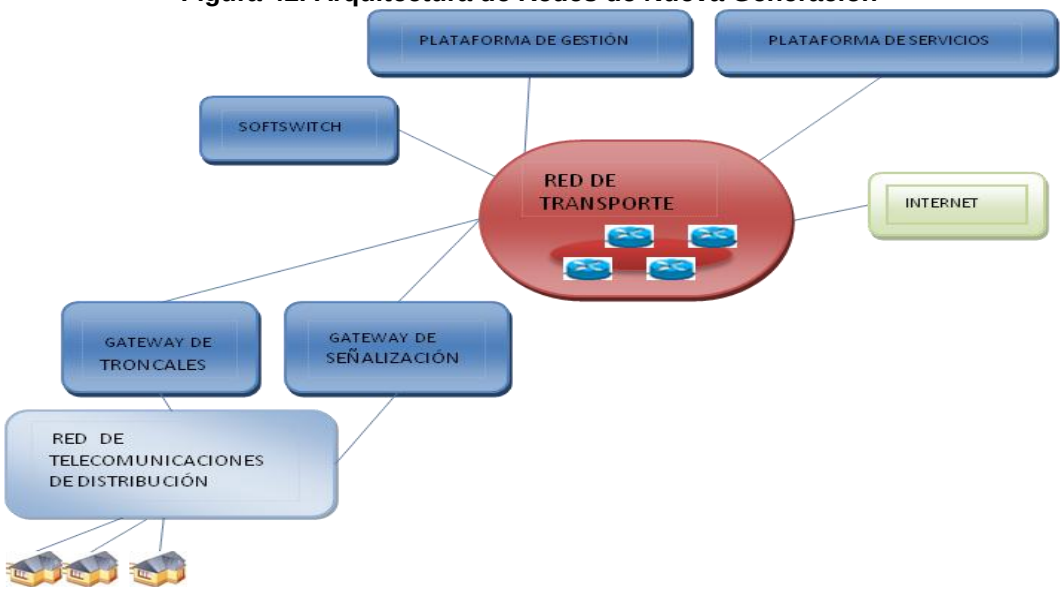
Red de dispersión: Este segmento de red conecta la caja de dispersión y la entrada al edificio, casa o lugar de residencia del abonado.

Cuando el operador utiliza acceso fijo inalámbrico (wireless local loop), este segmento se reemplaza por espectro radioeléctrico en las bandas que el Ministerio de Tecnologías de la Información y las Comunicaciones haya entregado en concesión al operador de TPBC.

Red Interna: Conecta el punto exterior de la residencia del abonado con la toma del aparato telefónico de mesa o pared.

La arquitectura de las redes de nueva generación (Figura 42), se diferencia de la arquitectura anterior en que los elementos de la central son renovados mediante la implementación de elementos de redes de nueva generación como lo son los gateways, encargados de la función de transporte, y los softswitch, encargados de las funciones de señalización. Éstos por su naturaleza, cuentan con elementos de protección y esquemas de respaldo que minimizan el impacto ante fallas. En relación con la red de distribución, sus elementos se asemejan en cuanto a sus características físicas.

Figura 42. Arquitectura de Redes de Nueva Generación



Fuente: CINTEL

Los principales elementos físicos de la red de telefonía pública básica conmutada local, expuestos a amenazas naturales son:

- Redes aéreas de cobre
- Redes subterráneas de fibra óptica y de cobre
- Edificaciones donde se encuentran instaladas las centrales de conmutación o softswitches y energía de respaldo.
- Gabinetes donde se encuentran instalados los concentradores remotos, gateways, estaciones base de telefonía inalámbrica (BS WLL wireless local loop), multiacceso alambrado, PCM, VSAT y nodos WI MAX y energía de respaldo.
- Armarios
- Torres, antenas y cuartos de equipos de sitios de transmisión donde se encuentran instalados los equipos de microondas y/o comunicación satelital y la energía de respaldo, para cuando se utiliza espectro radioeléctrico para los enlaces a nivel troncal o primario y cuando se hace uso de acceso fijo inalámbrico (wireless local loop).

5.1.2.3 Servicio de Telefonía Móvil Celular

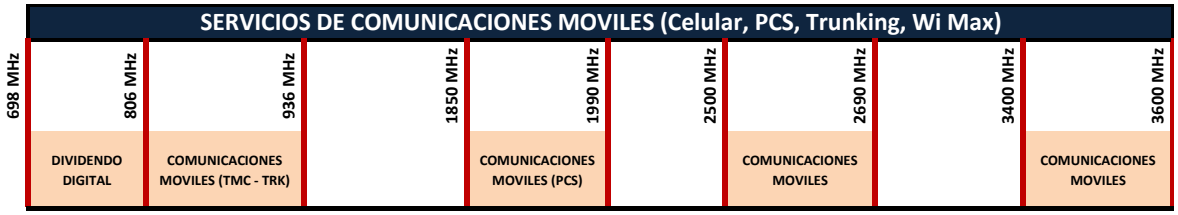
La Ley 37 de 1993 definió el servicio de telefonía móvil celular como un servicio público de telecomunicaciones, no domiciliario, de ámbito y cubrimiento nacional, que proporciona en sí mismo capacidad completa para la comunicación telefónica entre usuarios móviles y, a través de la interconexión con la red telefónica pública conmutada (RTPC), entre aquellos y usuarios fijos, haciendo uso de una red de telefonía móvil celular, en la que la parte del espectro radioeléctrico asignado constituye su elemento principal.

Esta misma ley, definió las redes de telefonía móvil celular como las redes de telecomunicaciones, que interconectadas entre ellas o a través de la red

telefónica pública conmutada, permiten un cubrimiento nacional, destinadas principalmente a la prestación al público del servicio de telefonía móvil celular en las cuales el espectro radioeléctrico asignado se divide en canales discretos, los cuales a su vez son asignados en grupos de células geográficas para cubrir un área. Los canales discretos son susceptibles de ser reutilizados en diferentes células dentro del área de cubrimiento[24].

La Figura 43 muestra el espectro radioeléctrico actualmente atribuido a comunicaciones móviles:

Figura 43 Comunicaciones Móviles (Celular, PCS, Trunking, Wi MAX) - Bandas de frecuencia atribuidas



Fuente: CINTEL

5.1.2.3.1 Red Celular GSM

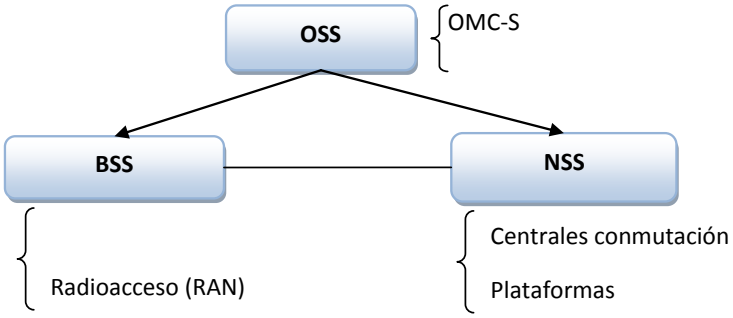
En la Figura 44 Subsistemas del sistema GSM, se muestran los tres subsistemas de una red celular GSM:

- Subsistema de Soporte de Operaciones (OSS, Operation Support Subsystem)

[24] **Fuente: Ley 37 de 1993**

- Subsistema de Estaciones Base (BSS, Base Station Subsystem)
- Subsistema de Conmutación (NSS, Network Switching System)

Figura 44 Subsistemas del sistema GSM



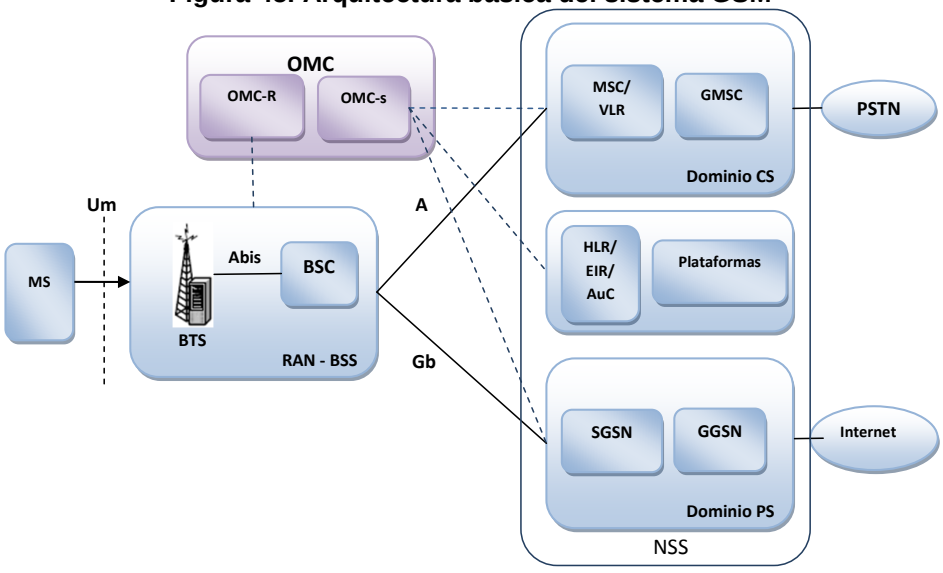
Fuente: CINTEL

- Subsistema de Soporte de Operaciones (OSS, Operation Support Subsystem): Está conectado con todos los subsistemas y es el encargado de ejecutar todas las funciones de gestión, tales como administración del sistema, generación de estadísticas (KPI), configuración de la red, gestión de desempeño, gestión de fallas y tareas de mantenimiento. Generalmente, el OSS se divide en dos centros de operación y mantenimiento (OMC): OMC-R para los elementos del radioacceso (BSS) y OMC-S para los elementos de conmutación (NSS).
- Subsistema de estaciones Base (BSS, Base Station Subsystem): Es el subsistema encargado de todas las funciones relacionadas con la interfaz de radio. Pertenecen a este subsistema la radiobase transceptora (BTS, Base Transceiver Station), el controlador de estaciones base (BSC, Base Station Controller) y la unidad de transcodificación.

- Subsistema de Conmutación (NSS, Network Switching System): Es el subsistema encargado de conmutar las llamadas de usuario de voz y datos tanto internas como hacia redes externas. Se compone básicamente de: las centrales de conmutación para red móvil (MSC, Mobile Switching Center), los elementos de control de movilidad – HLR y VLR, los elementos de control de equipos - EIR, los elementos de autenticación -AuC y las plataformas de otros servicios, como por ejemplo el SMSC (Short Message Service Center) encargado del servicio de mensajes cortos de texto. Para el soporte de servicios de datos (GPRS – EDGE) se requiere la introducción de una nueva clase de elementos funcionales, denominados nodos de soporte GPRS (GSN, GPRS Support Nodes). Hay dos tipos de nodos GSN: El SGSN y el GGSN.

La Figura 45 muestra los detalles de los subsistemas mencionados:

Figura 45. Arquitectura básica del sistema GSM



Fuente: CINTEL

A continuación se describen los subsistemas BSS y NSS.

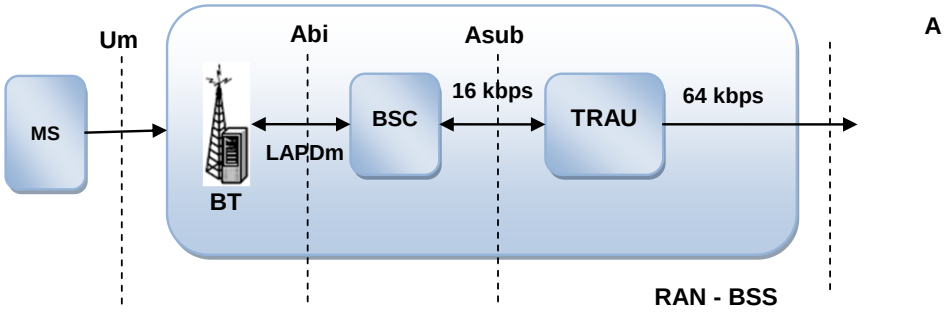
El subsistema BSS posee los siguientes componentes principales, en la Figura 46:

- ESTACIÓN BASE (BTS, Base Transceiver Station): Es el elemento de red que implementa la interfaz de aire, proporcionando los canales de radio para señalización y tráfico. Aparte de las funciones de radiofrecuencia, también implementa algunas funciones de capa 2 como servir de terminación para el protocolo LAPDm.
- CONTROLADOR DE ESTACIONES BASE (BSC, Base StationController): Es el elemento que controla a las BTS, administra los recursos de radio (ej.: asignación de canales) y concentra el tráfico proveniente de las BTSs (es una central de conmutación pequeña). Implementa también algunas funciones de radio relacionadas con la movilidad como el handoverintra-BSC. La BSC también implementa las interfaces hacia otros subsistemas como la interfaz Gb hacia el SGSN y la interfaz A25 hacia la red de Core.
- UNIDAD DE TRANSCODIFICACIÓN (TRAU, Transcoding Rate and Adaptation Unit): Es un elemento de red ubicado exactamente entre la BSC y la MSC, corresponde al sistema BSS pero se ubica en las premisas de la MSC. Se encarga de comprimir o descomprimir la voz entre la MS y la MSC. Básicamente, hace una transcodificación de 16 kbps (canal de

[25] **Propiamente es la interfaz Asub, sin embargo las funciones lógicas de la interfaz son implementadas por la BSC, la TRAU solo hace el cambio de codificación para los canales de voz.**

voz típico Full Rate codificado con LPC a 13kbps) a 64 kbps26 (PCM) y viceversa.

Figura 46. Componentes del Subsistema BSS.



Fuente: CINTEL

El subsistema NSS tiene los siguientes componentes principales:

- Central de Conmutación: Es el elemento de red responsable de las funciones de conmutación de circuitos, gestiona el establecimiento de llamadas desde y hacia los usuarios GSM. Adicionalmente, concentra el tráfico de BSS y se encarga de coordinar el traspaso de llamada para continuidad del servicio (Handover, Intra-MSC e Inter-MSC/BSC). Actúa de la mano con el VLR para todo lo relacionado con manejo de la movilidad, generalmente en implementaciones comerciales. El VLR es un modulo más de la MSC, a lo que se denomina MSC/VLR.
- VLR (Visitor Location Register): Es una base de datos de orden local (para una parte del área de servicio) contiene información de usuario básica de tipo dinámico (que varía constantemente),

[26] **La MSC es básicamente una central telefónica convencional con manejo de movilidad**

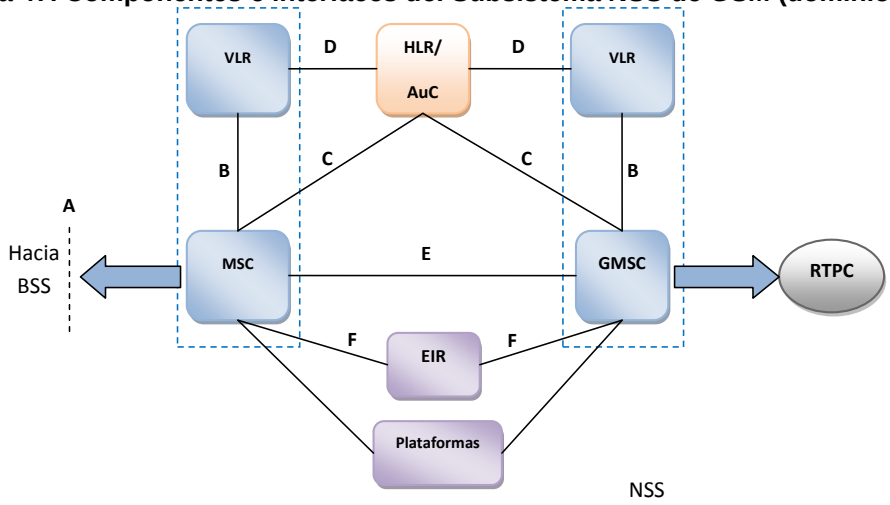
como en las operaciones de control de movilidad. También se encarga de asignar el MSRN (Mobile Subscriber Roaming Number) que sirve para realizar el enrutamiento de llamadas. Típicamente, este elemento de red está integrado dentro de la MSC.

- HLR (Home Location Register): Es una base de datos central o distribuida, que guarda el perfil de suscriptor (la información administrativa) de cada usuario dentro de la red GSM. Dada la criticidad de la información almacenada en el HLR, siempre se asocia con un AuC (Authentication Center), que se encarga de funciones complementarias asociadas a la seguridad (autenticación de usuarios y cifrado).
- EIR, Equipment Identity Register: Como se mencionó anteriormente, GSM separa al aparato terminal del suscriptor. Este elemento de red se encarga de verificar si los dispositivos terminales están habilitados para operar en la red GSM, por ejemplo, que el equipo sea compatible con la red y que no sea robado (esta es la principal utilidad). También clasifica a los dispositivos en 3 listas, una blanca (para aquellos sin inconvenientes), una gris (para aquellos que tengan alguna característica problemática) y una negra (para aquellos robados).
- Gateway MSC (MSC de interconexión): Es una MSC convencional, pero que se encarga específicamente de aquellas conexiones con redes externas. Puede contener tarjetas especiales para realizar las labores de interfaz y es el elemento de red que se encarga de comunicar a la red GSM con la RTPC.
- SGSN (Serving GPRS Support Node): Es responsable de la entrega de los paquetes de datos desde y hacia los usuarios, dentro de su área de servicio. Haciendo la analogía, el SGSN es la central de conmutación (MSC) del dominio de datos y por

tanto se encarga de las funciones de movilidad y manejo de usuarios (registro, autenticación y tarificación). Nótese que al igual que la MSC, el SGSN tiene una base de datos dinámica para el manejo de los usuarios de datos, denominada SLR (SGSN LocationRegister).

- GGSN (GPRS Gateway Support Node): Como su nombre lo sugiere, es el elemento que se que encarga de las labores de interfaz de la red GPRS con otras redes de datos (especialmente internet). Básicamente, convierte los paquetes de la red GRPS al formato adecuado de la red de destino, en la mayoría de los casos IP.

Figura 47. Componentes e interfaces del Subsistema NSS de GSM (dominio CS)



Fuente: CINTEL

En la arquitectura GSM, el tráfico se concentra en las BSCs y MCSs. Estos nodos generalmente se encuentran concentrados en pocas edificaciones, el motivo fundamental es que el tráfico de la interfaz Abis utiliza menor ancho de banda y por lo tanto demanda menores recursos de transmisión en larga distancia. La interfaz A generalmente es local (en la misma edificación) dado que se multiplica por 4 la capacidad de transmisión después de la TRAU.

Los elementos más críticos de la red GSM son, en su orden:

- HLR
- MSC
- BSC
- BTS

Sin embargo, el HLR es la máquina que tiene mayor protección. El elemento está duplicado en sitio, tiene una máquina gemela en otra ubicación geográfica y posee capacidad de conmutación automática. Para eventos de catástrofe en zonas geográficas puntuales, los elementos más vulnerables son las BTSs, ya que los elementos sensibles se encuentran en las premisas del operador, típicamente situados en ciudades capitales con edificaciones sismo-resistentes y con redundancia eléctrica.

Los principales elementos físicos de la red de celular GSM expuestos a amenazas naturales son:

- Redes subterráneas de fibra óptica
- Edificaciones donde se encuentran instalados el HLR, MSC y BSC y energía de respaldo.
- Gabinetes y shelters donde se encuentran instalados las BTS y energía de respaldo.
- Torres, antenas en sitios de transmisión donde se encuentran instalados los equipos de microondas y/o comunicación satelital y la energía de respaldo.

5.1.2.3.2 Red Celular UMTS

UMTS presenta dos modificaciones principales con relación a GSM: en la interfaz de radio y en los elementos de core. En la interfaz de radio, la modificación principal respecto a la arquitectura GSM es la inclusión del

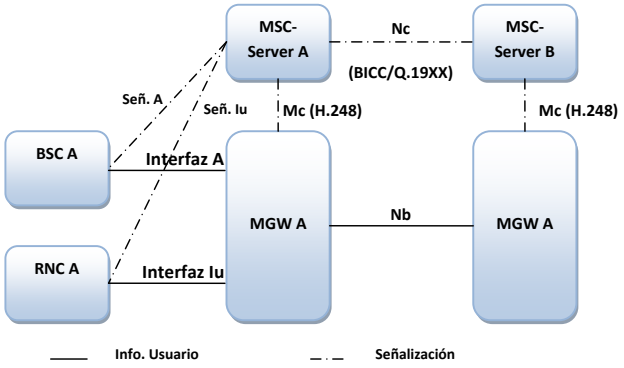
subsistema RNS. En este subsistema, se encuentra la red de acceso UMTS (denominada UTRAN, UMTS Terrestrial Radio Access Network), compuesta por dos elementos principales:

- Node B: Es el elemento lógico que sirve a una o más celdas UMTS y es responsable de la transmisión y recepción radioeléctrica hacia y desde las MSs. Los nodos B se conectan a los RNCs a través de los interfaces Iu-b y a las MSs a través de los interfaces Uu. (fuente: UMTS fórum).
- RNC (Radio Network Controller): Elemento de red que se encarga del control de los nodos B, específicamente del control de recursos de radio y handover, entre otros. El RNC se conecta a los elementos de Core a través de la interfaz Iu. Hay una interfaz Iu para las aplicaciones CS (Circuit Switched) denominada Iu-CS y otra para las aplicaciones PS (Packet Switched) denominada Iu-PS. (fuente: UMTS Forum).

En los elementos de core, la principal modificación de esta versión fue la introducción de la arquitectura de control independiente de la portadora (BICC, Bearer Independent Call Control), que se muestra en la Figura 48. Básicamente, esta arquitectura plantea que las funciones de la MSC del sistema GSMo R99 se reparten entre dos nuevos elementos de red:

- MSC-Server encargado de las funciones de control (control de llamadas y movilidad).
- Media Gateway (MGW, originalmente denominada CS-MGW) encargada(s) de las funciones de transporte o manipulación de flujos de información (control de portadora, funciones de control de recursos de transmisión).

Figura 48. Arquitectura de Red BICC

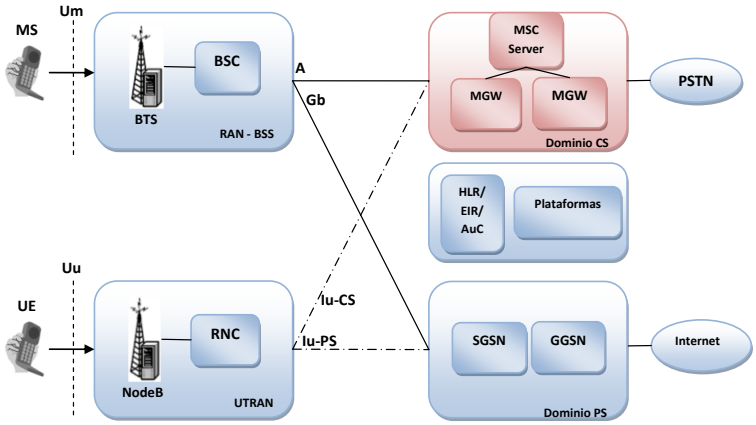


Fuente: CINTEL

Nota: La función de VLR está integrada en el MSC-Server, por lo cual no se dibuja en el diagrama.

La Figura 49 muestra como los nuevos elementos de red, descritos anteriormente, reemplazan a la MSC de la arquitectura GSM o 3GPP R99.

Figura 49 Arquitectura de Red 3GPP R4



Fuente: CINTEL

En la arquitectura GSM, el tráfico se concentra en las BSCs y MGWs (únicamente el tráfico de señalización llega al Softswitch). Estos nodos

generalmente se encuentran concentrados en edificaciones en las premisas del usuario (ciudades intermedias). El motivo fundamental es ahorrar costos de transmisión nacional.

Los elementos más críticos de la red son en su orden:

- HLR
- Softswitch
- MGW
- RNC
- Node B

Sin embargo, el HLR es la máquina que tiene mayor protección dado que el elemento está duplicado en sitio y tiene una máquina gemela en otra ubicación geográfica con capacidad de conmutación automática. Para eventos de catástrofe en zonas geográficas puntuales, los elementos más vulnerables son las BTSs, las BSCs y las MGWs, ya que los elementos sensibles se encuentran en las premisas del operador, típicamente situados en ciudades capitales con edificaciones sismo-resistentes y con redundancia eléctrica.

Los principales elementos físicos de la red de celular UMTS, expuestos a amenazas naturales son:

- Redes subterráneas de fibra óptica
- Edificaciones donde se encuentran instalados el HLR, el Softswitch, la MGW, el RNC y energía de respaldo.
- Gabinetes y shelters donde se encuentran instalados las Nodos y energía de respaldo.

- Torres, antenas en sitios de transmisión donde se encuentran instalados los equipos de microondas y/o comunicación satelital y la energía de respaldo.

5.1.2.4 Servicios de Valor Agregado (INTERNET)

Los servicios de valor agregado son aquellos que utilizan como soporte servicios básicos, telemáticos, de difusión, o cualquier combinación de éstos, y con ellos proporcionan la capacidad completa para el envío o intercambio de información, agregando otras facilidades al servicio de soporte o satisfaciendo nuevas necesidades específicas de telecomunicaciones. Dentro de estos servicios se incluye el servicio de acceso a INTERNET.

Como se estableció en el numeral 0 de este documento, se considera como servicio vital el acceso a INTERNET, ya que actualmente no se puede concebir el desarrollo de ninguna de las actividades básicas del ser humano en cualquier sector de la sociedad y de la economía que no haga uso intensivo de las diferentes facilidades que presenta este servicio.

A continuación se presentan las particularidades de los dos principales accesos a INTERNET: la red de TPBCL y la red móvil.

5.1.2.4.1 Acceso INTERNET fijo soportado en TPBCL - xDSL

Del análisis de penetración presentado en este documento, es claro que las redes de TPBCL soportan 1´293.532 accesos de xDSL (equivalente al 2,9% de la penetración de INTERNET) y 50.603 accesos conmutados (equivalentes al 0,1% de la penetración de INTERNET), razón por la cual se ha priorizado el análisis de los accesos xDSL con el fin de identificar los elementos básicos de esta red.

La familia de tecnologías DSL – "*Digital Suscriber Line" se ha* diseñado para aprovechar la red de cobre telefónica ya existente con el objetivo de lograr banda ancha y altas velocidades de transferencia de información. En la Tabla 19 se describen las diversas variaciones que presenta este tipo de acceso.

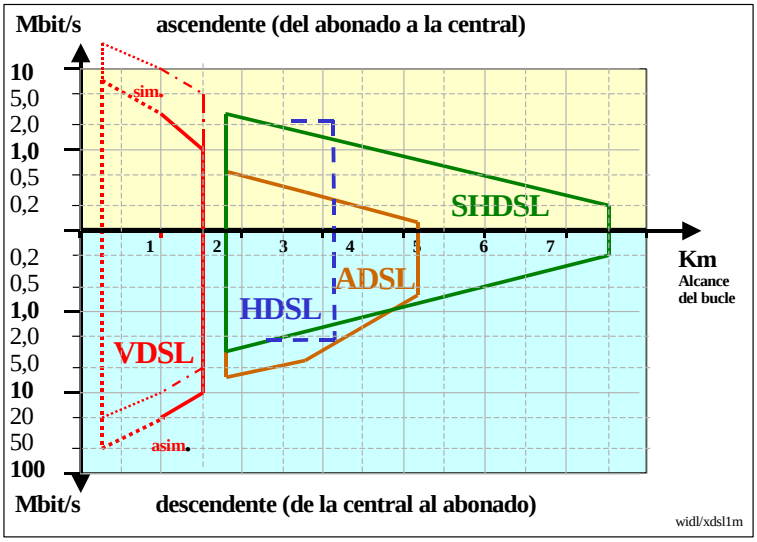
Tabla 19. Familias xDSL

Familia XDSL					
Nombre	**Significado**	**Velocidad**	**Distancia**	**Modo**	**Característica**
HDSL/HDSL2	DSL de alta velocidad	1,544 Mbps	4,5 KM	Simétrico	HDSL - 2 pares de hilos de cobre
		2,048 Mbps		Simétrico	HDSL2 - un par de hilos de cobre
SDSL	DSL de único par	768 kbps	3 Km	Simétrico	Un par de hilos de cobre
ADSL	DSL asimétrico	1,5 Mbps a 8 Mbps	5,5 Km	Downstream (Descendente)	Un par de hilos de cobre
		16 Kbps a 640 Kbps		Upstream (Ascendente)	Longitud mínima para el bucle: 5,5 Km.
UDSL	DSL unidireccional	1.5Mbps a 6Mbps	4,5 Km	Simétrico	Versión unidireccional de HDSL, utiliza el doble de la velocidad.
RADSL	DSL de velocidad adaptable	640Kbps a 2.2Mbps	5,5 KM	Downstream	Utiliza un par de hilos. Adapta la velocidad de datos a las condiciones de la línea.
		272 Kbps a 1088 Kbps		Upstream	
CDSL	DSL de consumidor	Hasta 1 Mbps	5,5 KM	Downstream	Un par de hilos. Necesita equipos remotos en el usuario final.
		16 a 128 Kbps		Upstream	
IDSL	DSL de RDSI	Igual que el Interfaz básico (BRI) de RDSI	5,5 Km	Simétrico	Un par de hilos. Llamado "Bri sin Conmutador".
VDSL	DSL de muy alta velocidad	13 a 52 Mbps	1,5 Km	Downstream	300 a 1500 m de longitud máxima para el bucle. Necesita una red de fibra y ATM.
		1,5 a 6 Mbps		Upstream	
SHDSL	DSL simétrico de alta velocidad.	192 kbps hasta 2.312 Mbps en pasos de 128 Kbps	4,5 Km	Simétrico	Un par de hilos de cobre

Fuente: CINTEL

Actualmente, ADSL es la tecnología con mayor demanda y aplicación en el mercado de xDSL. Con la evolución tecnológica y la transición a las NGN, se tendrá el uso masivo de las nuevas versiones de ADSL, SHDSL y posteriormente de VDSL. Las diferencias de velocidades y alcances para estas tecnologías se presentan en la Figura 50.

Figura 50. Alcance y velocidad de transmisión de datos en los sistemas XDSL (para un sólo par sin regenerador/amplificador)



Fuente: UIT-D

Los componentes básicos de DSL son:

- CPE: La terminación de una red de DSL en el usuario es provista por el CPE (Customer Premise Equipment), también llamado como la unidad de terminación remota xDSL (XTU-R) o modem, router o bridge DSL. Cuando el CPE provee servicios de voz así como también servicios de datos, es conocido como dispositivo de acceso integrado (IAD: Integrated Access Device).

- COE: Llamado Central Office Equipment, incluye a los grandes equipos de conmutación de las Telco y los multiplexores de acceso DSL (DSLAM). El DSLAM también conocido como Unidad Central de Terminación (XTU-C: Terminating Unit – Central) es el encargado de agregar el tráfico de múltiples CPEs y switches a la red principal, ya sea de voz y/o datos
- CO: Conocida como Central Office es la instalación física que alberga el COE y el MDF.
- MDF: También conocido como el marco principal de distribución (Main Distribution Frame), se refiere a la terminación de todos los pares de cobre en todos los bastidores y planta física que entran en el CO. El MDF ofrece muchas cross-connects que permiten habilitar diversos equipos en la CO para proveer servicios locales.
- DLC: Son sistemas multiplexadores de voz (Digital LoopCarrier) que mejoran la eficiencia en el tráfico TDM que transporta los servicios de voz a un cliente extendiendo fibra óptica a la planta de distribución local de cobre. El DLC impide que la mayoría de servicios DSL de trabajo como la transmisión de frecuencias, sean bloqueadas.
- RT: Los equipos terminales remotos (Remote Terminal) son concentradores DSLAM desplegados en la franja de proveedores de servicio (a través de cobre) que prestan el servicio a los lugares que están fuera del área de cobertura del DSL de una CO.

Los principales elementos físicos de la red de valor agregado de acceso a INTERNET soportada sobre la red de telefonía pública básica conmutada, expuestos a amenazas naturales, son naturalmente los mismos que los de TPBCL dado que esta red es su soporte:

- Redes aéreas de cobre
- Redes subterráneas de fibra óptica
- Edificaciones donde se encuentran instalados los DSLAM junto a las centrales de conmutación o softswitches y energía de respaldo.
- Gabinetes donde se encuentran instalados los concentradores remotos, gateways y energía de respaldo.
- Armarios
- Torres, antenas y cuartos de equipos de sitios de transmisión donde se encuentran instalados los equipos de microondas y/o comunicación satelital y la energía de respaldo, para cuando se utiliza espectro radioeléctrico para los enlaces a nivel troncal o primario y cuando se hace uso de acceso fijo inalámbrico (wireless local loop).

5.1.2.4.2 Acceso INTERNET móvil soportado en las redes celulares

Acceso a INTERNET soportado en GSM

Las redes de GSM manejan tanto tráfico de voz como de datos en dos modos de operación: conmutación de circuitos y conmutación de paquetes. En el modo de conmutación de circuitos se dedica un circuito a un usuario durante toda la duración de la llamada, en conmutación de paquetes se asignan canales de uso compartido. La conmutación por paquetes es más eficiente que la conmutación por circuitos. La tasa estándar de un canal GSM es 22,8 Kbps.

GPRS (General Packet Radio Service) permite la implementación de una arquitectura de core basada en IP para aplicaciones de datos, la cual es útil y expandible para aplicaciones integradas de voz y datos en 3G.

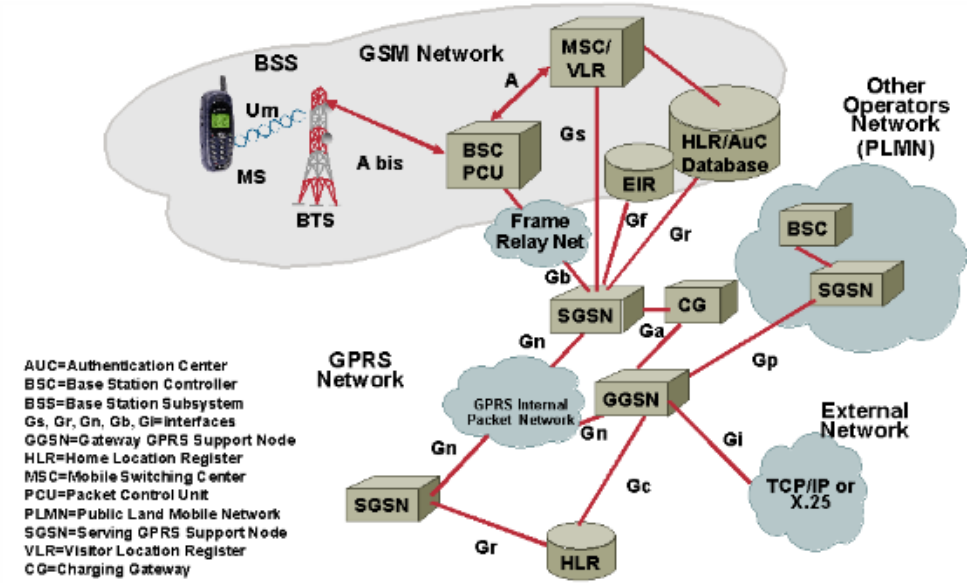
La Tabla 20 presenta las principales modificaciones de los elementos de red de GSM para operar como GPRS y la Figura 51 las interfaces GPRS.

Tabla 20Elementos de Red GPRS

Elemento de Red GSM	Actualización requerida para GPRS
BTS	Actualización de software
BSC	Actualización de software y la instalación de un nuevo hardware conocido como PCU (packet control unit). Este direcciona el tráfico de datos hacia la GPRS y puede ser un elemento separado asociado con la BSC.
Nodos de soporte GPRS	El despliegue de GPRS requiere la instalación de nuevos elementos de core: el nodo de soporte de servicio GPRS (Serving GPRS SupportNode SGSN) y el nodo de soporte de gateway de GPRS (gateway GPRS supportnode GGSN)
Bases de datos (HLR, VLR, etc)	Todas las bases de datos requieren actualización de software para manejar los nuevos modelos de llamada y las funciones introducidas por GPRS

Fuente: CISCO: Overview of GSM, GPRS and UMTS

Figura 51. Interfaces GPRS



Fuente: CISCO: Overview of GSM, GPRS and UMTS

En conclusión, los elementos más críticos de la red de valor agregado de acceso a INTERNET GPRS son los mismos que los de GSM, pero con las modificaciones anotadas en la Tabla 20:

- HLR
- MSC + SGSN + GGSN
- BSC + PCU
- BTS

Sin embargo, el HLR es la máquina que tiene mayor protección. El elemento está duplicado en sitio, tiene una máquina gemela en otra ubicación geográfica y posee capacidad de conmutación automática. Para eventos de catástrofe en zonas geográficas puntuales, los elementos más vulnerables

son las BTSs, ya que los elementos sensibles se encuentran en las premisas del operador, típicamente situados en ciudades capitales con edificaciones sismo-resistentes y con redundancia eléctrica.

Los principales elementos físicos de la red de valor agregado de acceso a INTERNET móvil GPRS expuestos a amenazas naturales son:

- Redes subterráneas de fibra óptica.
- Edificaciones donde se encuentran instalados el HLR, MSC + SGSN + GGSN, BSC + PCU y energía de respaldo.
- Gabinetes y shelters donde se encuentran instalados las BTS y energía de respaldo.
- Torres, antenas en sitios de transmisión donde se encuentran instalados los equipos de microondas y/o comunicación satelital y la energía de respaldo.

Acceso a INTERNET soportado en UMTS

UMTS (Universal Mobile Telecommunications System) es un sistema de telecomunicaciones móviles de tercera generación, que permite proveer servicios móviles de banda ancha.

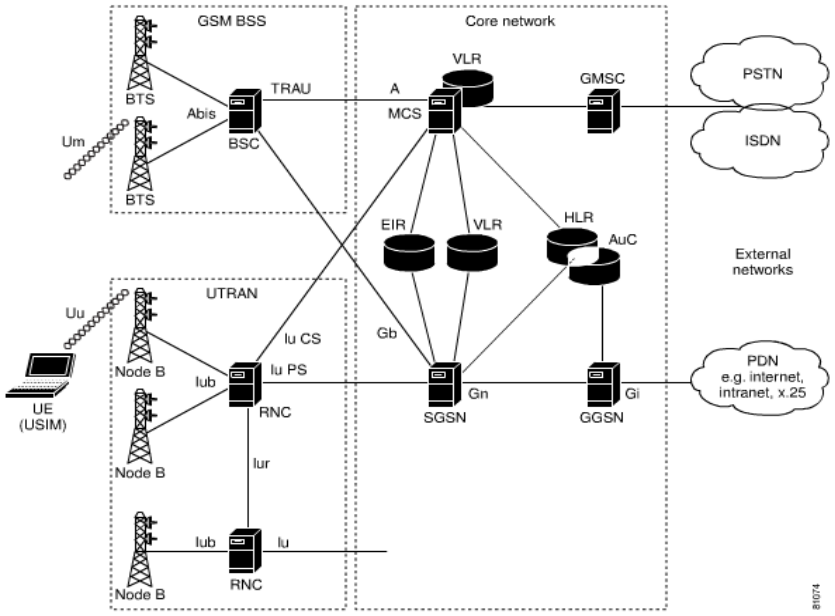
El sistema UMTS está diseñado para enviar y recibir fotos, gráficos, comunicaciones de video, y cualquiera otra comunicación de multimedia, además de voz y datos. La UMTS evoluciona hacia una red totalmente IP, extendiendo la segunda generación GSM / GPRS y usando WCDMA. El GPRS es el punto de convergencia entre 2G y UMTS 3G.

La Figura 52 muestra cómo a través de la red UMTS se accede a INTERNET, lo cual permite concluir que la red de valor agregado de acceso a INTERNET móvil, comporta los mismos elementos de UMTS, así:

- HLR
- Softswitch
- MGW
- RNC
- Node B

Sin embargo, el HLR es la máquina que tiene mayor protección. El elemento está duplicado en sitio, tiene una máquina gemela en otra ubicación geográfica y tiene capacidad de conmutación automática. Para eventos de catástrofe en zonas geográficas puntuales, los elementos más vulnerables son las BTSs, las BSCs y las MGWs, ya que los elementos sensibles se encuentran en las premisas del operador, típicamente situados en ciudades capitales con edificaciones sismo-resistentes y con redundancia eléctrica.

Figura 52. Arquitectura UMTS



Fuente: CISCO: Overview of GSM, GPRS and UMTS

Los principales elementos físicos de la red de valor agregado de acceso a INTERNET UMTS expuestos a amenazas naturales son:

- Redes subterráneas de fibra óptica
- Edificaciones donde se encuentran instalados el HLR, el Softswitch, la MGW, el RNC, GGSN, SGSN y energía de respaldo.
- Gabinetes y shelters donde se encuentran instalados las Nodos y energía de respaldo.
- Torres, antenas en sitios de transmisión donde se encuentran instalados los equipos de microondas y/o comunicación satelital y la energía de respaldo.

5.1.2.5 Servicios de Radiodifusión Sonora AM & FM

Este servicio de radiocomunicaciones es definido por el Plan Técnico de Radiodifusión Sonora AM y FM de Agosto de 2010, como el servicio de radiocomunicación cuyas emisiones se destinan a ser recibidas por el público en general.

La banda atribuida para el servicio de radiodifusión sonora AM en Colombia es:

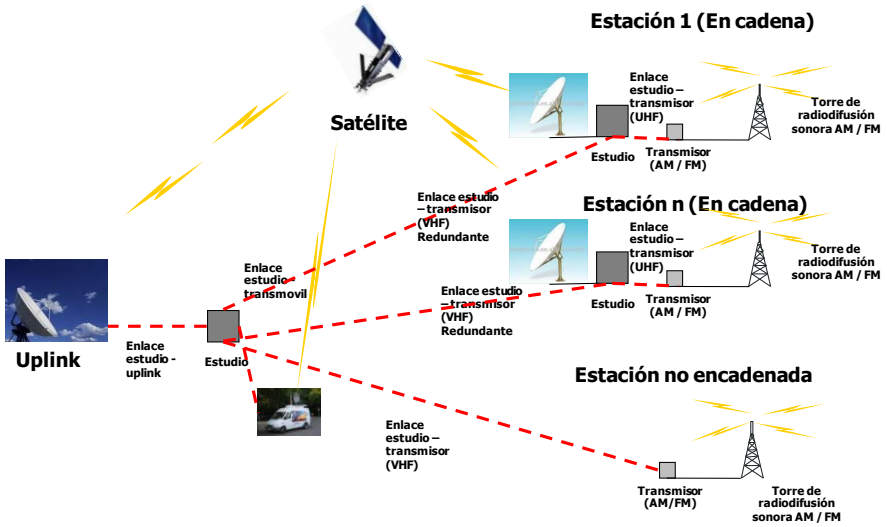
Servicio de Radiodifusión Sonora AM - Ondas Hectométricas	535 kHz - 1705 kHz

La banda atribuida para el servicio de radiodifusión sonora FM en Colombia es:

Servicio de Radiodifusión Sonora FM	88 MHz - 108 MHz

La Figura 53 presenta la topología general de red de los servicios de radiodifusión sonora.

Figura 53. Topología general de red de los servicios de radiodifusión sonora A.M. y F.M.



Fuente: CINTEL

Los principales elementos físicos de la red de radiodifusión sonora AM y FM expuestos a amenazas naturales son:

- Edificaciones donde se encuentran instalados el estudio, el telepuerto y energía de respaldo.
- El satélite utilizado con relación a su disponibilidad.
- Torres, antenas y cuartos de equipos de sitios de transmisión donde se encuentran instaladas las antenas de recepción satelital, los equipos de microondas y los transmisores de radiodifusión sonora y la energía de respaldo.

5.1.2.6 Servicios de Televisión

La Ley 182 de 1995 define el servicio de televisión como un servicio público dirigido al público sin excepción, consistente en la emisión, transmisión,

difusión, distribución, radiación y recepción de señales de audio y video en forma simultánea.

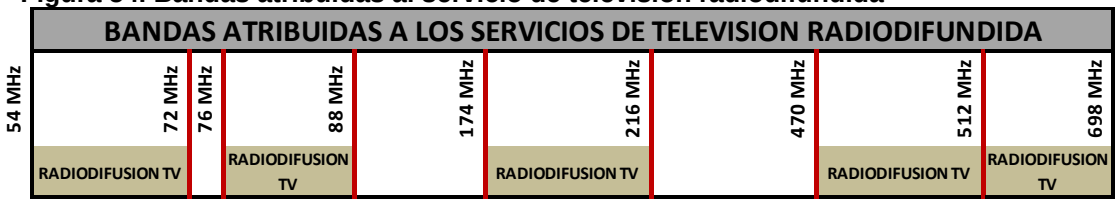
Según el medio que se utilice para la distribución de la señal de televisión a la audiencia, ésta puede ser:

- **Radiodifundida:** cuando la señal de televisión se distribuye a través del espectro radioeléctrico previsto para tal fin en las bandas de VHF y UHF, sin guía artificial.
- **Cableada y cerrada:** si para distribuir la señal de televisión se utiliza un medio físico de manera exclusiva o compartida con otros servicios de telecomunicaciones.
- **Satelital:** cuando la señal de televisión llega a la audiencia desde un satélite de distribución directa.

5.1.2.6.1 Servicio de Televisión Radiodifundida

La televisión radiodifundida opera en las bandas de frecuencia que se ven en la Figura 54.

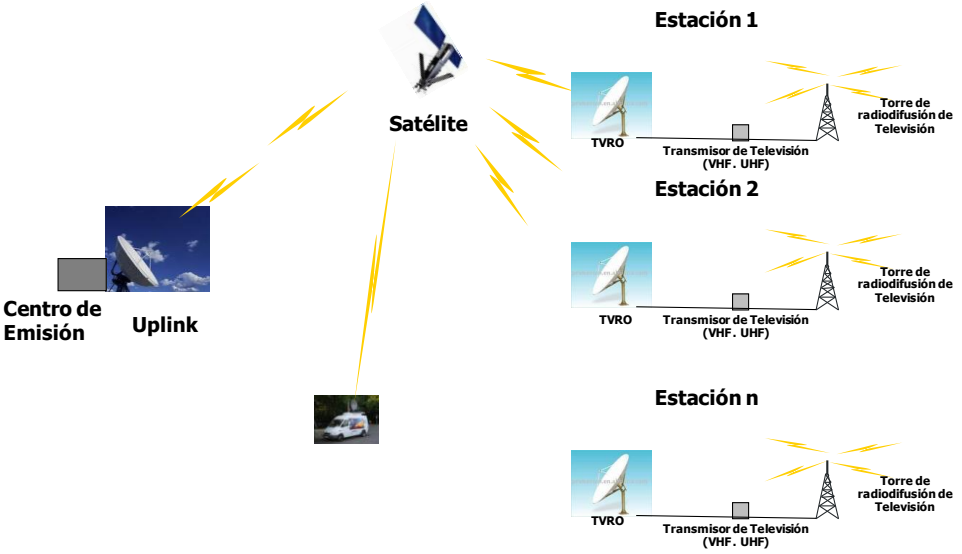
Figura 54. Bandas atribuidas al servicio de televisión radiodifundida



Fuente: CINTEL

La topología general de red de este servicio se presenta en la Figura 55 a continuación:

Figura 55. Topología general de red de los servicios de televisión radiodifundida



Fuente: CINTEL

Los principales elementos físicos de la red de televisión radiodifundida, expuestos a amenazas naturales son:

- Edificaciones donde se encuentran instalados el centro de emisión, el uplink (telepuerto) y energía de respaldo.
- El satélite utilizado con relación a su disponibilidad.
- Torres, antenas y cuartos de equipos de sitios de transmisión donde se encuentran instaladas las antenas de recepción satelital (Television Reception Only TVRO) y los transmisores de televisión radiodifundida y la energía de respaldo.

5.1.2.6.2 Servicio de televisión por cable

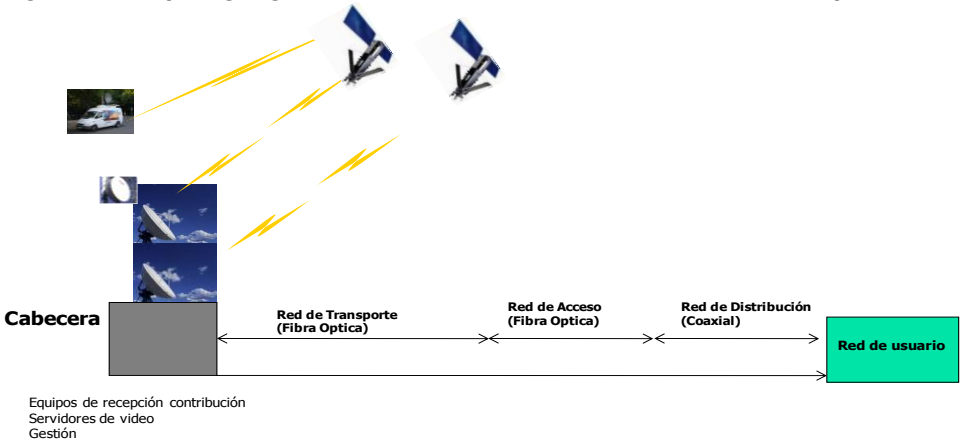
La topología de la red de televisión por cable se presenta en la Figura 56, donde es claro que la porción neurálgica de esta red es la cabecera, que recibe y adapta las señales de televisión recibidas para su distribución en la red. Adicionalmente, la cabecera gestiona los equipos y servicios de la red y

centraliza su mantenimiento. Los equipos que se encuentran en la cabecera son antenas parabólicas (TVRO) que reciben señales de TV provenientes de los diferentes satélites utilizados por los generadores de contenido, microondas y/o fibra óptica para señales de contribución de otras cabeceras, antenas de recepción de televisión terrestre y radiodifusión sonora típicamente FM.

Los principales elementos físicos de la red de televisión radiodifundida, expuestos a amenazas naturales son:

- Edificaciones donde se encuentra instalada la cabecera y energía de respaldo.
- El satélite utilizado con relación a su disponibilidad.
- Torres, antenas y cuartos de equipos de sitios de transmisión donde se encuentran instaladas las antenas de recepción satelital (Television Reception Only TVRO) y equipos de microondas y energía de respaldo.
- Redes aéreas de coaxial
- Redes subterráneas y aéreas de fibra óptica

Figura 56. Topología general de red de los servicios de televisión por cable



Fuente: CINTEL

5.1.2.7 Servicio de Móvil Marítimo

El Decreto 2061 de 1996, que reglamentó el servicio de móvil marítimo, lo define como el servicio de telecomunicaciones móvil que se presta entre estaciones costeras y estaciones de barco, entre estaciones de barco o entre estaciones de comunicaciones a bordo asociadas que serán utilizadas para labores propias del medio marítimo y fluvial. El servicio móvil marítimo incluye el servicio auxiliar de ayuda el cual tiene por objeto prestar la seguridad de la vida humana y socorro en aguas territoriales y puertos de la República de Colombia.

Las estaciones [27] asociadas a la red de móvil marítimo, de acuerdo con el Decreto en mención son:

- Estación costera: Estación terrestre del servicio móvil marítimo.
- Estación de barco: Estación móvil del servicio móvil marítimo a bordo de un barco no amarrado de manera permanente y que no sea una estación de embarcación o dispositivo de salvamento.
- Estación de comunicaciones a bordo: Estación móvil de baja potencia del servicio móvil marítimo destinada a las comunicaciones internas a bordo de un barco, entre un barco y

[27] Estación: Uno o más transmisores o receptores, o una combinación de transmisores y receptores, incluyendo las instalaciones accesorias, necesarios para asegurar un servicio de radiocomunicación, o el servicio de radioastronomía en un lugar determinado. Las estaciones se clasificarán según el servicio en el que participen de una manera permanente o temporal.

sus botes y balsas durante ejercicios u operaciones de salvamento, o para las comunicaciones dentro de un grupo de barcos empujados o remolcados, así como para instrucciones de amarre y atraque.

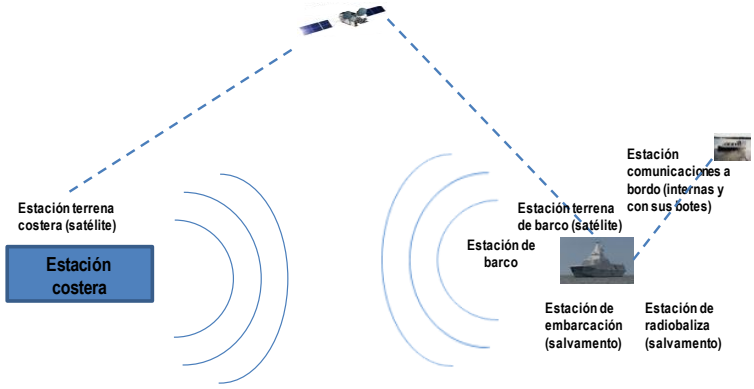
- Estación de embarcación o dispositivo de salvamento: Estación móvil del servicio móvil marítimo o del servicio móvil aeronáutico, destinada exclusivamente a las necesidades de los náufragos e instalada en una embarcación, balsa o cualquier otro equipo o dispositivo de salvamento.
- Estación de radiobaliza de localización de siniestros: Estación del servicio móvil cuyas emisiones están destinadas a facilitar las operaciones de búsqueda y salvamento.
- Estación portuaria: Estación costera del servicio de operaciones portuarias.
- Estación terrena costera: Estación terrena del servicio fijo por satélite o en algunos casos del servicio móvil marítimo por satélite instalada en tierra, en un punto determinado, con el fin de establecer un enlace de conexión en el servicio móvil marítimo por satélite.
- Estación terrena de barco: Estación terrena móvil del servicio móvil marítimo por satélite instalada a bordo de un barco.
- Estación terrestre: Estación del servicio móvil, no destinada a ser utilizada en movimiento.

Entre los servicios de móvil marítimo están incluidos el servicio de movimiento de barcos, que se considera como el servicio de seguridad, distinto del servicio de operaciones portuarias, entre estaciones costeras y estaciones de barco, entre estaciones de barco, cuyos mensajes se refieren únicamente a los movimientos de los barcos; y el servicio de operaciones portuarias que es el que se presta en un puerto o en sus cercanías, entre

estaciones costeras y estaciones de barco, o entre estaciones de barco, cuyos mensajes se refieren únicamente a las operaciones, movimiento y seguridad de los barcos y, en casos de urgencia, a la salvaguardia de las personas.

La Figura 57 muestra de manera esquemática la topología general de red del servicio de móvil marítimo.

Figura 57. Servicio Móvil Marítimo - Topología general de red



Fuente: CINTEL

Las bandas atribuidas al servicio de móvil marítimo son:

Tabla 21. Bandas de frecuencia atribuidas al servicio de Móvil Marítimo

MÓVIL MARÍTIMO			
R9 kHz - 14 kHz	R315 kHz - 325 kHz	6200 kHz - 6525 kHz	156,025 MHz - 162,025 MHz
14 kHz - 19,95 kHz	R405 kHz - 415 kHz	8100 kHz - 8195 kHz	156,4875 MHz - 156,5625 MHz
20,05 kHz - 70 kHz	415 kHz - 495 kHz	8195 kHz - 8815 kHz	156,7625 MHz- 157,45 MHz
70 kHz - 90 kHz	505 kHz - 510 kHz	12230 kHz - 13200 kHz	160,6 MHz - 162,05 MHz
R90 kHz - 110 kHz	2065 kHz - 2107 kHz	16360 kHz - 17410 kHz	216 MHz-220 MHz

110 kHz - 130 kHz	2170 kHz - 2173,5 kHz	18780 kHz - 18900 kHz	R 5470 MHz - 5570 MHz
130 kHz - 135,7 kHz	2173,5 kHz - 2190,5 kHz	19680 kHz - 19800 kHz	R5570 MHz - 5650 MHz
135,7 kHz - 137,8 kHz	2190,5 kHz - 2194 kHz	22000 kHz - 22855 kHz	R8850 MHz - 9000 MHz
137,8 kHz - 160 kHz	4000 kHz - 4063 kHz	25070 kHz - 25210 kHz	R9200 MHz- 9300 MHz
R285 kHz - 315 kHz	4063 kHz - 4438 kHz	26100 kHz - 26175 kHz	

Fuente: Cuadro Nacional de Atribución de Frecuencias 2010 (R = radionavegación)

Los principales elementos físicos de la red de móvil marítimo, expuestos a amenazas naturales son:

- Edificaciones donde se encuentran instaladas las estaciones costeras y energía de respaldo.
- El satélite utilizado con relación a su disponibilidad
- Torres, antenas y cuartos de equipos de sitios de transmisión donde se encuentran instaladas las antenas de los equipos de satélite, radio y energía de respaldo.

NOTA: No se toma en cuenta la vulnerabilidad de los móviles, materia fuera del alcance del presente estudio.

5.1.2.8 Servicio de Móvil Aeronáutico

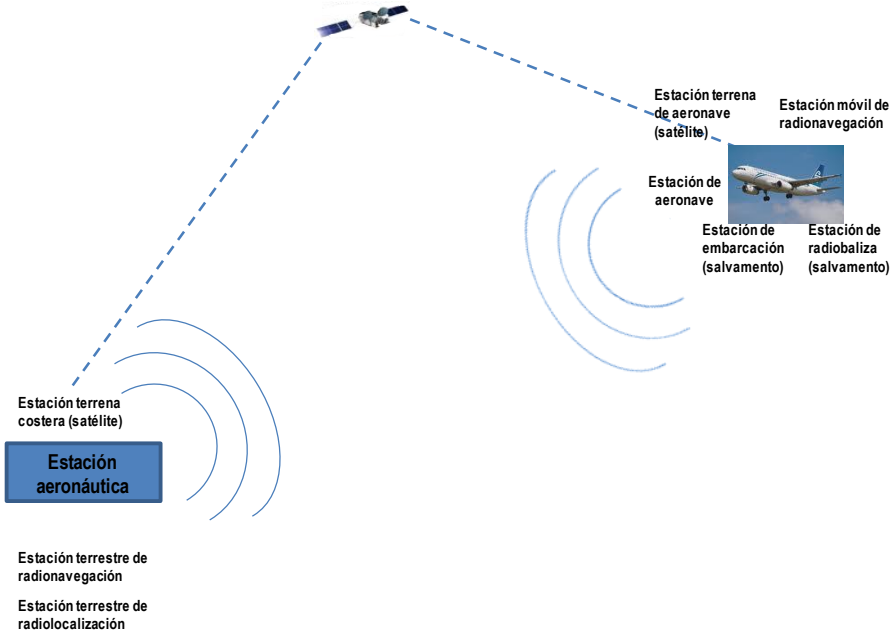
De acuerdo con el Decreto 1029 de 1998, el Servicio Móvil Aeronáutico es el servicio móvil entre estaciones aeronáuticas y estaciones de aeronave, o entre estaciones de aeronave, en el que también pueden participar las estaciones de embarcación o dispositivos de salvamento; también pueden considerarse incluidas en este servicio, las estaciones de radiobaliza de localización de siniestros que operen en las frecuencias de socorro y de urgencia designadas.

Las estaciones consideradas por el Decreto 1029, son:

- Estación aeronáutica: Estación terrestre del servicio móvil aeronáutico. En ciertos casos, una estación aeronáutica puede estar instalada, por ejemplo, a bordo de un barco o de una plataforma sobre el mar.
- Estación de aeronave: Estación móvil del servicio móvil aeronáutico instalada a bordo de una aeronave, que no sea una estación de embarcación o dispositivo de salvamento.
- Estación móvil de radionavegación: Estación del servicio de radionavegación destinada a ser utilizada en movimiento o mientras esté detenida en puntos no especificados.
- Estación terrena aeronáutica: Estación terrena del servicio fijo por satélite o, en algunos casos, del servicio móvil aeronáutico por satélite instalada en tierra en un punto determinado, con el fin de establecer un enlace de conexión en el servicio móvil aeronáutico por satélite.
- Estación terrena de aeronave: Estación terrena móvil del servicio móvil aeronáutico por satélite instalada a bordo de una aeronave.
- Estación terrestre de radionavegación: Estación del servicio de radionavegación no destinada a ser utilizada en movimiento.
- Estación terrestre de radiolocalización: Estación del servicio de radiolocalización no destinada a ser utilizada en movimiento.

La Figura 58 muestra de manera esquemática la topología general de red del servicio de móvil aeronáutico.

Figura 58. Servicio Móvil Aeronáutico - Topología general de red



FUENTE: CINTEL

Las bandas atribuidas al servicio de móvil aeronáutico son:

Tabla 22. Bandas de frecuencia atribuidas al servicio de Móvil Aeronáutico

MÓVIL AERONÁUTICO				
R190 kHz - 200 kHz	5450 kHz - 5480 kHz	21294 kHz - 22000 kHz	R5000 MHz- 5010 MHz	R15,43 GHz - 15,63 GHz
R200 kHz - 275 kHz	5480 kHz - 5680 kHz	23200 kHz - 23350 kHz	R5010 MHz - 5030 MHz	R15,63 GHz - 15,7 GHz
R275 kHz - 285 kHz	5680 kHz - 5730 kHz	R74,8 MHz - 75,2 MHz	R5030 MHz - 5091 MHz	R24,25 GHz - 24,45 GHz
R285 kHz - 315 kHz	6525 kHz - 6685 kHz	R108 MHz - 117,975 MHz	R5091 MHz - 5150 MHz	R24,45 GHz - 24,65 GHz
R325 kHz - 335 kHz	6685 kHz - 6765 kHz	117,975 MHz - 137 MHz	R5150 MHz - 5250 MHz	R31,8 GHz - 32 GHz
R335 kHz - 405 kHz	8815 kHz - 8965 kHz	R960 MHz- 1164 MHz	R5350 MHz - 5460 MHz	R32 GHz - 32,3 GHz
R405 kHz - 415 kHz	8965 kHz - 9040 kHz	R1164 MHz- 1215 MHz	R5460 MHz - 5470 MHz	R32,3 GHz- 33 GHz
R510 kHz - 525 kHz	10005 kHz - 10100 kHz	R1300 MHz - 1350 MHz	R8750 MHz - 8850 MHz	R33 GHz - 33,4 GHz
R525 kHz - 535 kHz	11175 kHz - 11275 kHz	R1559 MHz - 1610 MHz	R9000 MHz- 9200 MHz	

MÓVIL AERONÁUTICO				
R1705 kHz - 1800 kHz	11275 kHz - 11400 kHz	R1610 MHz- 1610,6 MHz	R9300 MHz- 9500 MHz	
2850 kHz - 3025 kHz	13200 kHz - 13260 kHz	R1610,6 MHz - 1613,8 MHz	R9500 MHz - 9800 MHz	
3025 kHz - 3155 kHz	13260 kHz - 13360 kHz	R1613,8 MHz- 1626,5 MHz	R13,25 GHz - 13,4 GHz	
3400 kHz - 3500 kHz	15010 kHz - 15100 kHz	R2700 MHz- 2900 MHz	R14 GHz - 14,25 GHz	
4650 kHz- 4700 kHz	17900 kHz - 17970 kHz	R2900 MHz - 3100 MHz	R14,25 GHz - 14,3 GHz	
4700 kHz - 4750 kHz	17970 kHz - 18030 kHz	R4200 MHz - 4400 MHz	R15,4 GHz - 15,43 GHz	

Fuente: Cuadro Nacional de Atribución de Frecuencias 2010 (R = radionavegación)

Los principales elementos físicos de la red de móvil aeronáutico, expuestos a amenazas naturales son:

- Edificaciones donde se encuentran instaladas las estaciones aeronáuticas, terrestres de radionavegación y radiolocalización y terrenas aeronáuticas y energía de respaldo.
- El satélite utilizado con relación a su disponibilidad
- Torres, antenas y cuartos de equipos de sitios de transmisión donde se encuentran instaladas las antenas de los equipos de satélite, radio y energía de respaldo.

NOTA: No se toma en cuenta la vulnerabilidad de los móviles, materia fuera del alcance del presente estudio.

5.1.2.9 Servicio de Radioaficionados

Las bandas atribuidas para radioaficionados son:

Tabla 23. Bandas atribuidas a Radioaficionados

SERVICIO	BANDAS ATRIBUIDAS	
Banda Ciudadana / Servicios Especiales	26,960 MHz - 27,410 MHz	
Banda Ciudadana / Servicio Auxiliar de Ayuda	27,035 MHz - 27,075	
Aficionados	1800 kHz - 1850 kHz	24890 kHz - 24990 kHz
	1850 kHz - 2000 kHz	28 MHz - 29,7 MHz
	3500 kHz - 3750 kHz	50 MHz- 54 MHz
	3750 kHz - 4000 kHz	144 MHz - 146 MHz
	7000 kHz - 7100 kHz	146 MHz - 148 MHz
	7100 kHz - 7200 kHz	220 MHz - 225 MHz
	7200 kHz - 7300 kHz	430 MHz - 432 MHz
	14000 kHz - 14250 kHz	432 MHz - 438 MHz
	14250 kHz - 14350 kHz	438 MHz - 440 MHz
	18068 kHz - 18168 kHz	24 GHz - 24,05 GHz
	21000 kHz - 21450 kHz	

Fuente: Cuadro Nacional de Atribución de Frecuencias

La red de radioaficionados es una red bastante extensa que logra su integridad con base en las comunicaciones individuales de cada radioaficionado. La configuración de una estación de radioaficionado se ilustra en la Figura 59.

Los principales elementos físicos de la red de radioaficionados, expuestos a amenazas naturales son:

- Edificaciones donde se encuentran instalados los mástiles, antenas y cuartos de equipos de radio y energía de respaldo. Típicamente, estas estaciones se encuentran localizadas en casas de habitación.

Figura 59. Estaciones de radioaficionado

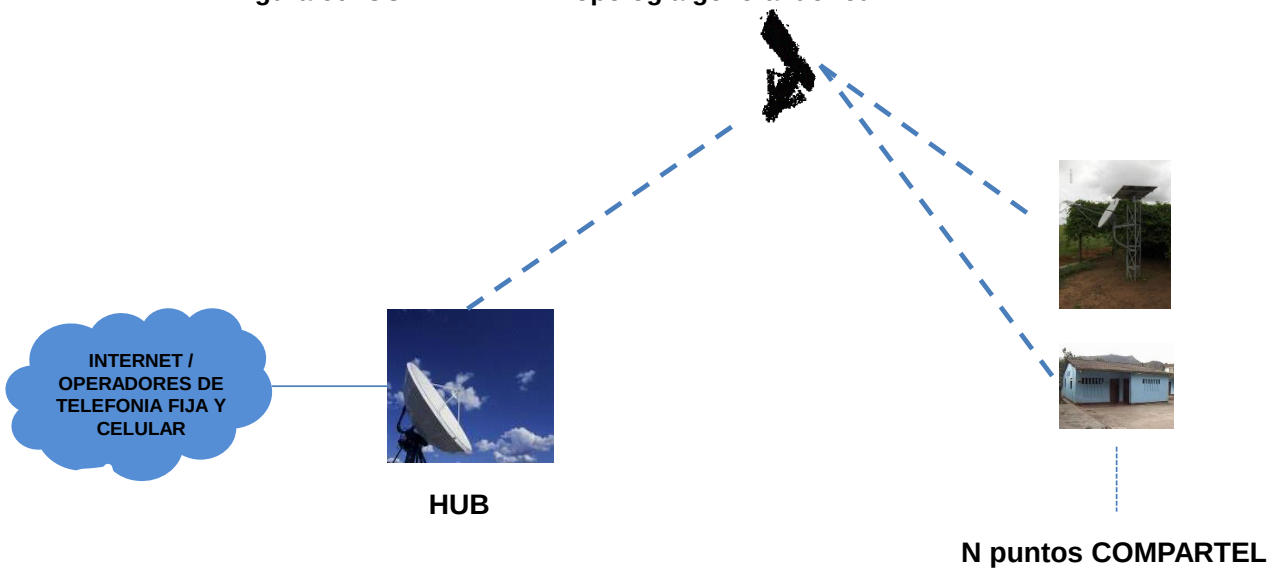
Fuente: CINTEL

5.1.2.10 Red COMPARTEL

El programa de COMPARTEL del Ministerio de Tecnologías de la Información y las Comunicaciones, tiene como objetivo dar conectividad a las zonas apartadas del país y a los estratos bajos, a través de la telefonía rural y el servicio de internet.

Actualmente, dieciséis operadores prestan los servicios de telefonía e Internet, utilizando en su gran mayoría como medio de transmisión la transmisión satelital.

Figura 60. COMPARTEL - Topología general de red



Fuente: CINTEL

Los principales elementos físicos de la red de COMPARTEL, expuestos a amenazas naturales son:

- Edificación donde se encuentra instalado el HUB, sus torres, mástiles, antenas y cuartos de equipos y energía de respaldo.
- Edificaciones donde se encuentran instalados los puntos COMPARTEL con sus mástiles, antenas y cuartos de equipos y energía de respaldo. Típicamente estos puntos son Telecentros y otros se encuentran localizados en escuelas, instituciones prestadoras de servicios de salud, instituciones oficiales, batallones, etc.
- El satélite utilizado con relación a su disponibilidad

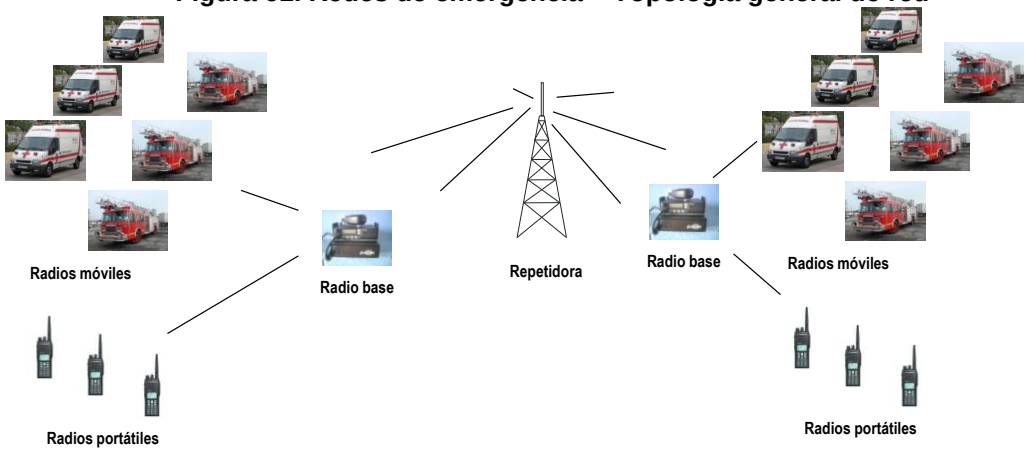
5.1.2.11 Redes de comunicaciones de emergencia

Dentro de las redes de comunicaciones de emergencias se han considerado las redes de:

- Comités Locales para Atención de Desastres - CLOPAD
- Comités Regionales para Atención de Desastres - CREPAD
- Cruz Roja
- Defensa Civil
- Cuerpo de Bomberos
- Alcaldía

Las anteriores redes utilizan sistemas de monocanales de voz o radio convencional, en las bandas de VHF, con la topología de red que se muestra en la siguiente figura.

Figura 61. Redes de emergencia – Topología general de red



Fuente: CINTEL

Los principales elementos físicos de estas redes, expuestos a amenazas naturales son:

- Edificaciones donde se encuentran instaladas las estaciones base y energía de respaldo.
- Torres, antenas y cuartos de equipos de sitios de transmisión donde se encuentran instaladas las repetidoras y la energía de respaldo.

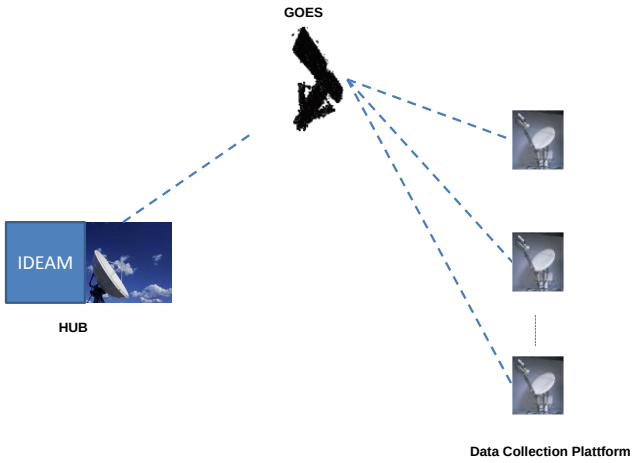
NOTA: No se toma en cuenta la vulnerabilidad de los móviles y portátiles, materia fuera del alcance del presente estudio.

5.1.2.12 Redes de Telemetría

Las redes de telemetría son utilizadas para monitorear de manera permanente y en tiempo real, los diferentes fenómenos asociados con los eventos naturales desastrosos.

La gran mayoría de estas redes tienen topologías como la mostrada en la Figura 62, aunque algunas se soportan sobre redes de microondas o la red celular.

Figura 62 Redes de Telemetría - Topología general de red



Fuente: CINTEL

Los principales elementos físicos de las redes de telemetría, expuestos a amenazas naturales son:

- Edificación donde se encuentra instalado el HUB sus torres, mástiles, antenas y cuartos de equipos y energía de respaldo.
- Gabinetes donde se encuentran instalados los sensores, equipos de medición y monitoreo, junto con los equipos VSAT asociados.
- El satélite utilizado con relación a su disponibilidad.

5.2 VULNERABILIDAD DE LAS REDES VITALES DE TELECOMUNICACIONES

El análisis de vulnerabilidad de las redes vitales de telecomunicaciones ante amenazas naturales se abordará, iniciando por determinar de manera integral las vulnerabilidades como características intrínsecas[28] de la infraestructura de telecomunicaciones, y dentro de éstas, identificar y acotar aquellas relacionadas con la vulnerabilidad física y funcional ante amenazas naturales (volcán, sismo, tsunami, inundación).

Una aproximación para el análisis de infraestructura de telecomunicaciones, de amplia aceptación, utilizada en diferentes estudios de análisis de vulnerabilidad dentro de los cuales se destaca el análisis de la disponibilidad y robustez de la infraestructura europea de comunicaciones electrónicas realizado por Alcatel Lucent en 2007, es la de tomar la infraestructura de telecomunicaciones como compuesta de ocho elementos básicos.

Los ocho elementos o componentes de la infraestructura de acuerdo con esta aproximación son:

- Instalaciones físicas: dentro de este componente están todas las edificaciones donde se encuentran instalados los equipos de telecomunicaciones, tanto de core como de acceso, e incluye torres y ductos.

[28] **De acuerdo con el estudio referenciado de ALCATEL LUCENT la vulnerabilidad es una característica intrínseca de una infraestructura o sistema que lo hacen susceptible al daño al ser explotada por una amenaza.**

- Energía Eléctrica: dentro de este componente se encuentra la infraestructura de energía comercial y la infraestructura de energía de respaldo: UPS, baterías, motogeneradores, tanques de combustible y cualquiera otra fuente de energía alternativa como eólica o solar.
- Hardware: comprende los componentes electrónicos y físicos que conforman los nodos de red, incluyendo los paquetes de circuitos electrónicos, las tarjetas, los chips semiconductores y los cables de cobre y de fibra óptica de transmisión.
- Software: bajo este componente se contempla todo el software conexo al desarrollo, operación y mantenimiento de la infraestructura.
- Redes: bajo este componente se incluyen la configuración topológica de las redes, la sincronización, la redundancia y la diversidad física y lógica
- Tráfico: este componente incluye la información transmitida a través de la infraestructura, los patrones de tráfico y las estadísticas,
  interceptación y daño de la información.
- Humano: El componente humano incluye conductas intencionales y no intencionales, limitaciones físicas y mentales, deficiencia en la educación y la formación, en las interfaces hombre-máquina y en la formación ética.
- Política: Está constituido por el marco político y regulatorio de los servicios y redes de telecomunicaciones, incluye los acuerdos, normas, políticas y regulaciones.

Ahora bien, en desarrollo del estudio de disponibilidad y robustez de las redes de telecomunicaciones europeas ya mencionado y, con base en la consulta de expertos de la industria, el gobierno, centros de investigación y

academia, se priorizaron las siguientes vulnerabilidades en cada uno de los elementos componentes de la infraestructura tratados, así:

Tabla 24. Valoración de las principales vulnerabilidades intrínsecas en redes de Telecomunicaciones en Europa

Componente de infraestructura	Vulnerabilidades	Porcentaje de importancia relativa en Europa
Instalaciones físicas	Dependencia de otras infraestructuras	56%
	Remotamente manejada	56%
	No cumplimiento de protocolos y procedimientos establecidos	38%
	Exposición a elementos	38%
Energía Eléctrica	Limitaciones del suministro	64%
	Destrucción física	55%
	Dependencia del combustible	36%
Hardware	Al ambiente (temperatura, humedad, polvo, luz solar, inundaciones)	65%
	Ciclo de vida (repuestos, reemplazo de equipos, capacidad de reparación, envejecimiento y obsolescencia)	53%
	Energía electromagnética (EMI, EMC, ESD, RF, EMP, HEMP, IR)	47%
Software	Complejidad de los programas	82%
	Habilidad para controlar	45%

Componente de infraestructura	Vulnerabilidades	Porcentaje de importancia relativa en Europa
	Errores en códigos	45%
	Mutabilidad del despliegue de códigos	41%
Tráfico	Autenticación errónea	63%
	Encapsulación de contenido malicioso	56%
	Insuficiente inventario de componentes críticos	44%
	Encriptación (prevención de observabilidad)	44%
Redes	Interconexión (interoperabilidad, interdependencia, conflictos)	68%
	Complejidad	62%
	Puntos de concentración (congestión)	50%
Humano	Conocimiento (falta, distracción, engaño, confusión)	67%
	Ética (lealtades divididas, codicia, mala intención)	53%
	Entorno de usuario (interfaz de usuario, funciones, , cultura corporativa)	40%
Política	Interpretación errada	50%
	Excesiva regulación	50%
	Desactualización	45%
	No implementada (parcial o totalmente)	45%

Fuente: European Commission, Information Society and Media, Directorate General, Availability and Robustness of Electronic Communications Infrastructures, Alcatel Lucent, 2007

Tomando en consideración esta aproximación y en el contexto del análisis de vulnerabilidades físicas de la infraestructura de telecomunicaciones ante amenazas naturales, el estudio se centrará en las siguientes vulnerabilidades:

Tabla 25. Vulnerabilidades de redes de Telecomunicaciones ante amenazas naturales consideradas en el presente estudio

Componente de infraestructura	Vulnerabilidades
Instalaciones físicas	Exposición a elementos (vulnerabilidad de hardware a su interior)
Energía Eléctrica	Limitaciones del suministro
Redes	Puntos de concentración (congestión)

Fuente: CINTEL

En el estudio de Townsend & Moss[29] sobre el comportamiento de la infraestructura de telecomunicaciones en desastres, se puntualiza que haciendo uso del análisis histórico de los últimos veinte años de los grandes desastres ocurridos en el mundo, se concluye que las principales causas para que las telecomunicaciones fallen ante una situación de desastre son:

[29] **TELECOMMUNICATIONS INFRASTRUCTURE IN DISASTERS: *Preparing Cities for Crisis Communications* - By Anthony M. Townsend & Mitchell L. Moss -Center for Catastrophe Preparedness and Response & Robert F. Wagner Graduate School of Public Service New York University, April 2005**

Tabla 26. Principales causas para que las Telecomunicaciones fallen ante situaciones de desastre

No.	Causa de falla
1	Destrucción física de los componentes de red
2	Disrupción del suministro de energía eléctrica
3	Congestión de red

Fuente: Townsend & Moss

Por otro lado, en el estudio del Gobierno Canadiense[30] para determinar la vulnerabilidad de sus comunicaciones móviles ante eventos desastrosos de origen natural, se definieron como componentes básicos de la infraestructura de telecomunicaciones los siguientes:

- Edificaciones: usadas típicamente para albergar equipos de conmutación, radio, equipos periféricos y equipos de respaldo de energía.
- Energía Eléctrica: Todos los componentes activos de las redes de telecomunicaciones dependen para su funcionamiento del suministro de energía eléctrica, es decir, que éste se constituye en componente básico de las redes tanto a nivel del suministro comercial como de los equipos de respaldo de energía albergados en edificaciones.

[30] **Government of Canada - Office of Critical Infrastructure Protection and Emergency Preparedness -The Vulnerability of Mobile Telecommunications to Natural Hazards - 2001**

- Enlaces de transmisión: a través de diferentes medios, tales como: cobre, coaxial, fibra óptica, microondas, satélite.
- Torres de Telecomunicaciones
- Antenas

Tomando en consideración los antecedentes internacionales mencionados y otros que se listan como material de referencia, la vulnerabilidad física de las redes e infraestructura de telecomunicaciones en zonas vulnerables expuestas a eventos naturales desastrosos se centrará en los componentes de infraestructura considerados en la Tabla 27, los cuales son producto de la desagregación de redes de telecomunicaciones a nivel de componentes físicos y que están dentro de la ortodoxia de estos análisis a nivel internacional.

Tabla 27. Elementos básicos del sistema de telecomunicaciones

ELEMENTOS BASICOS SISTEMA DE TELECOMUNICACIONES

ELEMENTOS / SERVICIOS	EDIFICACIONES	ARMARIOS / GABINETES / SHELTERS	TORRES / ANTENAS	REDES AEREAS (POSTES)		REDES SUBTERRANEAS (CANALIZACION /DUCTOS)		ESPECTRO RADIOELECTRICO
				FIBRA OPTICA	COBRE	FIBRA OPTICA	COBRE	
SERVICIO PORTADOR	Centro de Operaciones Nodos conectantes internacionales, Nodos de agregación nacional; Nodos de Servicio Municipal Transmisores y repetidores Equipos de Radio /satelite Energía de respaldo		Nodos de agregación nacional; Nodos de Servicio Municipal (Radiotransmisión (MW / Satélite))	Redes aéreas sobre infraestructura eléctrica / postes		Redes canalizadas y ductadas		MW / Satélite
TELEFONIA PUBLICA BASICA CONMUTADA	Centrales de Conmutación Softswitch Energía de respaldo	Armarios / Concentradores /gateways Energía de respaldo	Sitios de Radiotransmisión (MW / WLL)	Red Troncal	Red Primaria/ Red Secundaria	Red Troncal	Red Primaria/ Red Secundaria	MW / WLL
TELEFONIA MOVIL CELULAR	BSC / MSC - Softswitch // Pequeñas para BTS y Nodos B en zonas urbanas	Gabinetes & Shelters: BTS / Nodos B / Gateways	MW para enlace BTS / Nodos y Radio Access Network	Redes aéreas sobre infraestructura eléctrica / postes (Red Troncal entre MSC - Softswitch y conexión a otros operadores)		Redes canalizadas y ductadas (Red Troncal entre MSC - Softswitch y conexión a otros operadores)		MW para enlace BTS / Nodos y Radio Access Network
VALOR AGREGADO (INTERNET FIJO)	Centro de Operaciones / Nodos conectante nacional e internacional / DSLAM	Armarios	Sitios de Radiotransmisión (MW / WLL)	Redes aéreas sobre infraestructura eléctrica / postes (Red Troncal)	Redes aéreas sobre infraestructura eléctrica / postes (Red Primaria/ Red Secundaria)	Redes canalizadas y ductadas (Troncal)	Redes canalizadas y ductadas (Primaria / Secundaria)	MW / WLL
VALOR AGREGADO (INTERNET MOVIL)	Centro de Operaciones / Nodos conectante nacional e internacional / SGSN (Service GPRS Support Node) GGSN (Gateway GPRS Support Node)	Gabinetes / Shelters BS / Nodos B	Estaciones Base / Nodos (Radio Access Network - MW para enlace de la base)	Redes aéreas sobre infraestructura eléctrica / postes (Red Troncal entre MSC y conexión a otros operadores)		Redes canalizadas y ductadas (Red Troncal entre MSC y conexión a otros operadores)		Radio Access Network - MW para enlace de la base
TELEVISION RADIODIFUNDIDA	Centro de Emisión / Telepuerto Transmisores en sitio de radiodifusión		Sitio de Radiodifusión (Satelite - MW para enlace centro de emisión - transmisor)					Satelite/MW para red de transporte - radiodifusión
TELEVISION POR CABLE	Cabecera		Microondas y Parabólica Cabecera	Red Transporte / Acceso /Distribución	Coaxial Red Distribución	Red Transporte / Acceso /Distribución	Coaxial Red Distribución	Enlace satelital cabecera, microondas
RADIODIFUSION SONORA AM / FM	Estudio / Telepuerto Transmisores en sitio de radiodifusión		Sitio de Radiodifusión (Satelite - MW para enlace estudio - transmisor)					Satelite /MW para enlace estudio - transmisor
REDES DE EMERGENCIA	Base (Institución)		Sitios de Radiotransmisión (Repetidora)					VHF para red de radio
MOVIL MARITIMO	Estación costera (satélite / HF /VHF/UHF)	Gabinetes de ayuda a la navegación	Sitio de Radiotransmisión (HF / VHF / UHF)					HF / VHF / UHF /Satélite
MOVIL AERONAUTICO	Estación aeronáutica (satélite / HF / VHF / UHF)	Gabinetes de ayuda a la navegación	Sitio de Radiotransmisión (HF / VHF / UHF)					HF / VHF / UHF /Satélite
TELEMETRIA	HUB Estación central (Institución)	Gabinetes de telemetria						Satélite / MW /Espectro celular
RADIOAFICIONADOS	Casa		Sitio de Transmisión					HF / VHF /UHF
COMPARTEL	HUB /// Institución: Escuela / Hospital / Batallón / Alcaldia		Sitio de Transmisión (Enlace Satelital - MW)					Satelite/MW

NOTA: Las edificaciones que albergan componentes de core de todas las redes normalmente son edificiaciones sismoresistentes, con previsiones para inundaciones y con respaldo de energía
(*) En el caso de radioaficionaddos y puntos compartel, la estructura de transmisión funciona en el mismo sitio de la casa o institución

Fuente: CINTEL

La vulnerabilidad física[31] se define como la condición que tiene un determinado elemento en función de sus características físicas y de ubicación, de ser susceptible al daño en la presencia de una amenaza específica. La vulnerabilidad física se expresa como:

Vulnerabilidad física = Amenaza en el sitio de ubicación del elemento / Resistencia a la amenaza

En el numeral 5.3 del presente documento, se presentan los daños que se podrían ocasionar en la infraestructura de telecomunicaciones, vulnerabilidad física, ante el evento de ocurrencia de una amenaza de origen natural como las analizadas, los cuales dependen de la resistencia del elemento y de la amenaza y, cuya materialización dependerá de la ubicación del elemento y de la ocurrencia del evento.

La vulnerabilidad funcional de un servicio es la susceptibilidad para continuar siendo prestado en las condiciones normales de calidad y cobertura. La vulnerabilidad funcional para los diferentes servicios de telecomunicaciones objeto de este estudio, depende de:

- La vulnerabilidad física de cada uno de los elementos de la red comprometidos en la prestación del servicio.
- Las redundancias a nivel de redes (medios y diversidad de interconexión).

[31] **Ministerio del Interior y de la Justicia - Dirección de Gestión de Riesgos - Corporación Osso - Estudio de vulnerabilidad física y funcional a fenómenos volcánicos en el área de influencia del volcán Galeras - 2009**

- Suministro de energía eléctrica, el cual es básico para la operación de todos los elementos activos de las redes de telecomunicaciones, factor exógeno al sistema que se mitiga mediante la utilización de sistemas de respaldo de energía. Es decir, que dependerá de la existencia del respaldo de energía y de su autonomía, en ausencia del suministro comercial de energía eléctrica.
- Aumento inusitado del tráfico, el cual desborda los recursos limitados de las redes diseñados para situaciones normales, lo cual causa la congestión y el "infarto" en las redes de servicios tales como telefonía móvil celular, telefonía pública básica conmutada e Internet.

En el numeral 5.4 de este documento, se trata pormenorizadamente la vulnerabilidad funcional de los servicios de telecomunicaciones considerados como vitales, sobre los cuales se elaboró el modelo de vulnerabilidad de redes de telecomunicaciones.

5.3 VULNERABILIDAD FÍSICA DE LOS ELEMENTOS DE LAS REDES VITALES DE TELECOMUNICACIONES

Como resultado del análisis previo, se obtiene que los principales elementos de las redes de telecomunicaciones, a nivel agregado, sobre los cuales se centrará el presente estudio son:

- Edificaciones
- Armarios, Gabinetes, Shelters
- Torres – Antenas – Espectro radioeléctrico
- Redes aéreas de fibra óptica y de cobre
- Redes subterráneas de fibra óptica y de cobre

5.3.1 Edificaciones

Son aquellas construcciones que albergan en su interior equipos de telecomunicaciones utilizados para la prestación de los servicios de telecomunicaciones.

Por su importancia dentro de la red, tamaño y características constructivas se han considerado dos tipos básicos de edificaciones, tal como se presenta en la Tabla 28.

Tabla 28. Tipos de edificaciones

TIPO DE EDIFICACIONES

TIPO DE EDIFICACION	EQUIPO INSTALADO
Grandes Edificaciones	• **Servicio Portador:** Centro de Operaciones, nodos conectantes internacionales, nodos de agregación nacional; nodos de servicio municipal, equipos de transmisión y repetición de fibra óptica • **Telefonía Pública básica Conmutada y acceso a INTERNET fijo** : centrales de conmutación, softswitches, DSLAM • **Telefonía móvil celular y acceso a INTERNET móvil:** HLR, MSC, BSC, softswitch, MGW, RNC, SGSN, GGSN, PCU • **Radiodifusión Sonora AM & FM:** estudios, telepuerto • **Televisión radiodifundida:** centro de emisión, telepuerto • **Televisión por cable:** Cabecera • **Móvil marítimo:** estaciones satelitales y terrenas costeras • **Móvil aeronáutico:** estaciones satelitales y terrenas aeronáuticas • **Compartel (operadores satelitales):** Hub • **Redes de Telemetria:** Hub
Medianas y pequeñas edificaciones, cuartos de equipos	• **Servicio Portador:** add & drop multiplexers, equipos de microondas y/o comunicación satelital • **Telefonía Pública básica Conmutada y acceso a INTERNET fijo** : equipos de microondas, WLL y/o comunicación satelital • **Telefonía móvil celular y acceso a INTERNET móvil:** equipos de microondas y/o comunicación satelital • **Radiodifusión Sonora AM & FM:** sitios de transmisión donde se encuentran instaladas las antenas de recepción satelital, los equipos de microondas y los transmisores de radiodifusión sonora • **Televisión radiodifundida:** sitios de transmisión donde se encuentran instaladas las antenas de recepción satelital (Television Reception Only TVRO) y los transmisores de televisión radiodifundida • **Televisión por cable:** sitios donde se encuentran instaladas las antenas de recepción satelital (Television Reception Only TVRO) y equipos de microondas • **Móvil marítimo:** sitios de transmisión donde se encuentran instaladas las antenas de los equipos de satélite, radio y gabinetes de ayuda a la navegación • **Móvil aeronáutico:** sitios de transmisión donde se encuentran instaladas las antenas de los equipos de satélite, radio y gabinetes de ayuda a la navegación • **Compartel (operadores satelitales):** puntos COMPARTEL con sus mástiles, antenas y cuartos de equipos • **Comunicaciones de Emergencia:** estaciones base, sitios de transmisión donde se encuentran instaladas las repetidoras • **Redes de Telemetria:** Gabinetes de medida • **Radioaficionados:** Casas

Fuente: CINTEL

Estas edificaciones son aquellas dentro de las cuales se encuentran instalados y en funcionamiento equipos de telecomunicaciones así:

- Servicio Portador:
  - Centro de Operaciones
  - Nodos conectantes internacionales
  - Nodos de agregación nacional
  - Nodos de servicio municipal
  - Transmisores y repetidores
  - Equipos de radio /satélite
- Telefonía pública básica conmutada y acceso a INTERNET fijo :

  - Centrales de conmutación, softswitches, DSLAM
  - Equipos de microondas, estaciones base de soluciones inalámbricas (wireless local loop – WLL) y/o comunicación satelital
- Telefonía móvil celular y acceso a INTERNET móvil:
  - HLR, MSC, BSC, softswitch, MGW, RNC, SGSN, GGSN, PCU
  - equipos de microondas y/o comunicación satelital
- Radiodifusión Sonora AM & FM:
  - Estudios, telepuerto
  - Sitios de transmisión donde se encuentran instaladas las antenas de recepción satelital, los equipos de microondas y los transmisores de radiodifusión sonora
- Televisión radiodifundida:
  - Centro de emisión, telepuerto
  - Sitios de transmisión donde se encuentran instaladas las antenas de recepción satelital (Television Reception Only TVRO) y los transmisores de televisión radiodifundida
- Televisión por cable:
  - Cabecera donde se encuentran instaladas las antenas de recepción satelital (Television Reception Only TVRO) y equipos de microondas
- Móvil marítimo:
  - Estaciones costeras
  - Sitios de transmisión donde se encuentran instaladas las antenas de los equipos de satélite, radio y gabinetes de ayuda a la navegación
- Móvil aeronáutico:

- estaciones aeronáuticas
- sitios de transmisión donde se encuentran instaladas las antenas de los equipos de satélite, radio y gabinetes de ayuda a la navegación

- Compartel (operadores satelitales):
  - Hub
  - puntos COMPARTEL con sus mástiles, antenas y cuartos de equipos
- Redes de Comunicaciones de Emergencia:
  - estaciones base
  - sitios de transmisión donde se encuentran instaladas las repetidoras
- Redes de Telemetría
  - Hub
  - sitios de transmisión donde se encuentran instalados los gabinetes de telemetría
- Radioaficionados
  - Estaciones de radioaficionados (casas)

5.3.1.1 Resistencia y vulnerabilidad de las edificaciones

La Norma Sismo Resistente NSR 10, que reemplazó a la NSR 98, en el literal a de su numeral 2.5.1.1, define las estaciones indispensables como aquellas edificaciones de atención a la comunidad que deben funcionar durante y después de un sismo, y cuya operación no puede ser trasladada rápidamente a un lugar alterno y, en su literal b, establece que todas las edificaciones que componen aeropuertos, estaciones ferroviarias y sistemas masivos de transporte, centrales telefónicas, de telecomunicación y de

radiodifusión, se consideran edificaciones indispensables, incluyendo las estructuras que alberguen plantas de generación eléctrica de emergencia, los tanques y estructuras que formen parte de sus sistemas contra incendio, y los accesos, peatonales y vehiculares. Esto permite concluir que su diseño, construcción y supervisión técnica debe someterse, como edificaciones indispensables, a la norma NSR 10, entre otras.

Tomando en consideración que el actual estudio no profundiza sobre las características constructivas de las edificaciones utilizadas en el sector de las telecomunicaciones para albergar infraestructura de equipos, se ha supuesto que:

- La mayoría de pequeñas y medianas edificaciones destinadas a albergar equipos de transmisión vía radio, conexas a los diferentes servicios, no están construidas con norma NSR 98, ni han sido sometidas a reforzamiento estructural y que,
- Las grandes edificaciones donde se encuentran instalados equipos de core de los servicios considerados en este estudio, en su gran mayoría, están construidas bajo norma NSR 98 o han sido sometidas a proyectos de reforzamiento estructural.

Adicionalmente, en el modelo desarrollado se tomará en cuenta no sólo la resistencia y vulnerabilidad intrínseca de los elementos de red (cumplimiento o no de la NSR 98), sino las características de los suelos y la tipología de las construcciones de las zonas donde se encuentran instalados estos elementos. Esto se hará mediante la consulta y aplicación de los estudios y zonificaciones realizadas para el Municipio de Armenia por las autoridades nacionales en la materia.

Bajo estos supuestos, las edificaciones pequeñas y medianas, donde se instalan normalmente equipos de radio, es decir sitios de transmisión, probablemente se verán notoriamente más afectadas ante la ocurrencia de un evento natural, que las grandes edificaciones diseñadas y construidas bajo la norma NSR 98 que deben soportar el estrés producido por los sismos tal como se referencia a continuación y de manera análoga, debieran resistir otras amenazas materializadas como estrés a la construcción.

5.3.1.1.1 Resistencia y vulnerabilidad de las grandes edificaciones con relación a los sismos

- Temblores de poca intensidad sin daño,
- Temblores moderados sin daño estructural, pero posiblemente con algún daño a los elementos no estructurales y
- Temblores fuertes con daños a elementos estructurales y no estructurales pero sin colapso.

5.3.1.1.2 Resistencia y vulnerabilidad de las grandes edificaciones con relación a los volcanes

- Nube de ceniza volcánica: La nube de ceniza volcánica, con relación a las edificaciones, tiene dos efectos básicos: el deterioro a mediano plazo que causa en los materiales de construcción y el peso o presión que aquella causa sobre las terrazas de las edificaciones cuando se acumula sobre éstas. Tomando en consideración que las grandes edificaciones de telecomunicaciones están diseñadas y construidas para resistir alto estrés de carga, se supone para este estudio que las acumulaciones moderadas de cenizas en sus terrazas no deben causar su colapso.
- Flujos de lava, material piroclástico y lodos: Tomando en consideración que la temperatura de estos flujos puede alcanzar hasta los 1000º C y que su velocidad puede llegar a

los 300 km por hora, y dado que el flujo de lodos arrastra grandes rocas, troncos, construcciones civiles, entre otros, es altamente probable que las edificaciones resulten destruidas, arrasadas, enterradas o con graves fallas estructurales, si están a su paso.

- Caída de material piroclástico y proyectiles: La caída de piroclastos corresponde a los fragmentos eyectados a la atmósfera durante una erupción explosiva y que se depositan por gravedad (debido a su peso). Los fragmentos más finos son generalmente transportados por el viento, incluso a grandes distancias. Los fragmentos de mayor tamaño tienen una proyección balística y se depositan en un radio cercano (5 Km) al centro de emisión. Los proyectiles balísticos se originan en el material volcánico que en el momento de su emisión se encuentra como líquido o sólido y en el curso de su trayectoria alcanza el estado sólido o semisólido. Sus dimensiones pueden ser hasta de 50 cm, con densidad de 0,5 a 2,5 g/cm^3, típicamente 1 g/cm^3. El alcance de estos proyectiles depende principalmente de la velocidad de emisión (la cual se encuentra generalmente en el rango de 100 a 600 m/seg) y del ángulo de emisión. El alcance de los proyectiles varía dentro de un rango que va de los 0 a los 12 kilómetros y la energía del impacto depende de su masa y densidad.[32]
- Tomando en consideración lo anterior y la temperatura de estos materiales, es altamente probable que las edificaciones

[32] **Fuente: Plan PEVOLCA Anexo 1 Glosario de términos vulcanológicos, Dirección General de Seguridad y Emergencias, Gobierno de Canarias, 2010.**

INGEOMINAS, Boletín Geológico issn-o120-1425vol. 40 (2-3): 1-122, 2003 Bogotá, D.C., 2001.

ubicadas en las zonas de caída de este material volcánico (piroclastos y proyectiles balísticos), resulten con daños estructurales y destruidas por incendio.

5.3.1.1.3 Resistencia y vulnerabilidad de las grandes edificaciones con relación a los Tsunamis

Como ya se mencionó, se supone que las grandes edificaciones diseñadas y construidas bajo la norma NSR 98 que deben soportar el estrés mecánico producido por los sismos, de manera análoga deberán resistir otras amenazas tal como las de tsunami materializadas como estrés a la construcción.

Bajo este supuesto, las edificaciones pequeñas y medianas, donde se instalan normalmente equipos de radio, es decir sitios de transmisión, probablemente se verán notoriamente más afectadas ante la ocurrencia de un Tsunami, que las grandes edificaciones diseñadas y construidas bajo la norma NSR 98, que se podrían ver afectadas de la siguiente forma:

- Golpes de ola de poca intensidad sin daño
- Golpes de ola moderados sin daño estructural, pero posiblemente con algún daño a los elementos no estructurales y
- Golpes de ola fuertes con daños a elementos estructurales y no estructurales pero sin colapso.
- Fuerzas leves laterales provenientes de corrientes de agua y material arrastrado sin daño.
- Fuerzas moderadas laterales provenientes de corrientes de agua y material arrastrado sin daño estructural, pero posiblemente con algún daño a los elementos no estructurales.

- Fuerzas laterales fuertes provenientes de corrientes de agua y material arrastrado con daños a elementos estructurales y no estructurales pero sin colapso.
- Inundaciones de agua salobre que podrán causar daños menores a pisos y paredes, pero sin daño estructural.

5.3.1.1.4 Resistencia y vulnerabilidad de las grandes edificaciones con relación a las inundaciones de agua dulce

- Inundaciones de agua dulce, que podrán causar daños menores a pisos y paredes, pero sin daño estructural.

5.3.1.2 Posibles daños a las edificaciones de telecomunicaciones ante eventos naturales

Para el análisis de posibles daños ante las diferentes amenazas consideradas, se contempla que sólo las grandes construcciones dedicadas a albergar los nodos de conexión nacional e internacional (portador), centrales de conmutación fijas y móviles y/o equipos de core de redes de nueva generación, estudios, centros de emisión y telepuertos, están diseñadas y construidas bajo norma NSR 98 o reforzadas estructuralmente y que el resto de edificaciones medianas y pequeñas no satisfacen la norma sismoresistente NSR 98, que en principio es la situación más probable y por lo cual es el escenario con el que se modelará.[33]

33En este escenario se contempla que los equipos, racks de equipos, ductos de aire, bandejas de cables, se encuentran adecuadamente fijados al cielo raso y al piso de los salones de las edificaciones. En la ciudad de Bogotá, de manera específica se contempla en el Decreto 412 de septiembre de 2010 que para la construcción de la infraestructura de las centrales, subcentrales

5.3.1.2.1 Posibles daños a las edificaciones de telecomunicaciones ante eventos sísmicos

Con base en la resistencia de las edificaciones, tratada en el numeral 5.3.1.1 de este documento, se ha elaborado la Tabla 29, que registra los posibles daños a las edificaciones según tipo.

Tabla 29. Eventos sísmicos – Posibles daños a edificaciones

POSIBLES DAÑOS A EDIFICACIONES Supuesto: Sólo las grandes edificaciones cumplen NSR 98 (ESCENARIO DE ANALISIS)				
Tipo de Edificación	**Temblores de muy baja intensidad (Vibración)**	**Temblores de baja intensidad (Vibración)**	**Temblores de intensidad moderada (Vibración)**	**Temblores de alta intensidad (Vibración, fallas y grietas en la superficie terrestre, licuefacción)**
Grandes Edificaciones	Sin daño	Sin daño	Sin daño estructural, pero posiblemente con algún daño a los elementos no estructurales	Daños a elementos estructurales y no estructurales pero sin colapso.
Medianas, pequeñas edificaciones, cuartos de equipos	Sin daño	Agrietamiento	Agrietamiento, desplazamiento de cimientos.	Agrietamiento, desplazamiento de cimientos, destrucción estructuras portantes, colapso de columnas, paredes y cubiertas:

Fuente: CINTEL

En la Tabla 72 se registran los estimativos de vulnerabilidad física de las edificaciones ante eventos sísmicos de diferente magnitud, según juicio de expertos sectoriales.

---

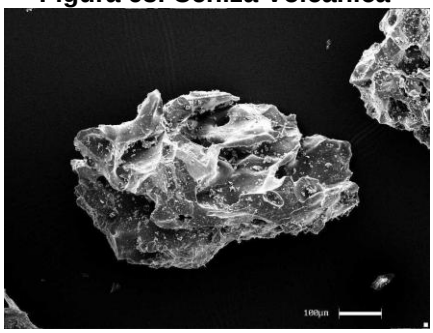
y los salones de Distribución de servicios de telecomunicaciones, la empresa prestadora debe presentar, entre otros, el estudio técnico estructural, según las normas vigentes para los diferentes elementos que conforman la subestación. Norma Sismo Resistente NSR-10 (Ley 400 de 1997, y Decreto Nacional 926 de 2010). Sin embargo, aunque este Decreto es de reciente promulgación y es sólo para Bogotá, permite inferir que en el corto plazo se deberá desarrollar una reglamentación similar en los demás municipios de Colombia.

5.3.1.2.2 Posibles daños a las edificaciones de telecomunicaciones ante volcanes

Posibles daños a las edificaciones de telecomunicaciones causados por cenizas volcánicas

Aunque las erupciones volcánicas implican diferentes amenazas, las cenizas volcánicas expulsadas por el volcán pueden ser depositadas a cientos o miles de kilómetros del cráter del volcán, es decir, que es la amenaza volcánica con más área de influencia potencial.

Figura 63. Ceniza Volcánica



Fuente: Review of Impacts of Volcanic Ash on Electricity Distribution Systems, Broadcasting and Communication Networks, Auckland Engineering Lifelines Group Project AELG-19, Auckland, NZ, APRIL 2009

La ceniza volcánica básicamente tiene dos efectos sobre las edificaciones: el primero, es el relacionado con la carga vertical que ocasiona su deposición sobre las terrazas de las edificaciones y el segundo, es el deterioro de los materiales exteriores.

La magnitud de estos efectos depende del espesor de la ceniza, su masa y su composición química, de la forma de la terraza del edificio, de su construcción, orientación y cercanía con otros edificios. La carga de la ceniza en la terraza se puede calcular utilizando la siguiente ecuación:

$$\text{Presión (kPa)} = \frac{\text{espesor de la capa de ceniza (m) x densidad de la ceniza (kg/m}^3\text{) x gravedad (9,8 m/s}^2\text{)}}{1000}$$

El proyecto AELG-19, Auckland, NZ, realizado por Auckland Engineering LifelinesGroup conformado por Thomas Wilson (University of Canterbury),MicheleDaly (KestrelGroup) y David Johnston (GNS Science), estimó la probabilidad de falla de terrazas planas de edificaciones por acumulación de cenizas, como se muestra en la Tabla 30.

Tabla 30. Volcán – Nube de Cenizas – Posibles daños a edificaciones- Proyecto AELG-19

Component	Risk Factors		Probability of Failure				Cause	Comments
Buildings - flat roofs								
			Ash thickness 5-100mm		Ash thickness >100mm		Weight of ash causing structural failure of roof	Roof collapse is one of the few instances when a catastrophic thickness of ash will enter a building's environment which may damage electrical equipment. Only flat, long span roofs considered as they are the most vulnerable to roof collapse.
			Fine grained (<1 mm)	Coarse grained (>1 mm)	Fine grained (<1 mm)	Coarse grained (>1 mm)		
		Moist or Wet ash	Low-Medium	Low-Medium	Medium-high	Medium-high	Collapse, buckling due to ash loading	
		Dry ash	Low	Low	Medium	Medium		

Fuente: Review of Impacts of Volcanic Ash on Electricity Distribution Systems, Broadcasting and Communication Networks, Auckland Engineering Lifelines Group Project AELG-19, Auckland, NZ, April 2009

La Tabla 31 registra el posible daño a las edificaciones por acumulación de ceniza volcánica en sus terrazas.

Tabla 31. Volcán – Nube de Cenizas - Posible daños a edificaciones

POSIBLES DAÑOS A EDIFICACIONES POR LA ACUMULACION DE CENIZAS VOLCANICAS	
Tipo de edificación	**Posible daño**
Grandes Edificaciones	Colapso de terrazas debido a fallas estructurales por peso de cenizas volcánicas
Medianas, pequeñas edificaciones, cuartos de equipos	Colapso de terrazas debido a fallas estructurales por peso de cenizas volcánicas

Fuente: CINTEL

Posibles daños a las edificaciones de telecomunicaciones causados por flujos de lava, material piroclástico y lodos.

Como ya se mencionó, estos flujos se caracterizan por sus altas temperaturas, alta velocidad y fuerza del material arrastrado, con alto poder destructivo.

La Tabla 32 registra el posible daño a las edificaciones por estos flujos volcánicos.

Tabla 32. Volcán – Flujos de lava, material piroclástico y lodos - Posible daños a edificaciones

POSIBLES DAÑOS A EDIFICACIONES POR FLUJOS DE LAVA, MATERIAL PIROCLASTICO Y LODOS	
Tipo de edificación	**Posible daño (causado por fuerzas y presiones laterales)**
Grandes Edificaciones	Agrietamiento, desplazamiento de cimientos, destrucción estructuras portantes, colapso de columnas, paredes y cubiertas, incendio, enterramiento, arrastre, parcial o total
Medianas, pequeñas edificaciones, cuartos de equipos	Agrietamiento, desplazamiento de cimientos, destrucción estructuras portantes, colapso de columnas, paredes y cubiertas, incendio, enterramiento, arrastre, parcial o total

Fuente: CINTEL

Posibles daños a las edificaciones de telecomunicaciones causados por caída de material piroclástico y proyectiles

Este fenómeno que ya fue caracterizado previamente y, cuya zona de influencia es muy cercana al volcán, tiene un poder altamente destructivo, dada la velocidad y dimensión de los proyectiles y su incandescencia.

La Tabla 33 registra el posible daño a las edificaciones por la caída de este tipo de material volcánico.

Tabla 33. Volcán – Caída de material piroclástico y proyectiles - Posible daños a edificaciones

POSIBLES DAÑOS A EDIFICACIONES POR POR CAIDA DE MATERIAL PIROCLASTICO Y PROYECTILES	
Tipo de edificación	**Posible daño (Impactos de material y rocas incandescentes con trayectoria parabólica)**
Grandes Edificaciones	Agrietamiento, desplazamiento de cimientos, destrucción estructuras portantes, colapso de columnas, paredes y cubiertas, incendio, enterramiento parcial o total
Medianas, pequeñas edificaciones, cuartos de equipos	Agrietamiento, desplazamiento de cimientos, destrucción estructuras portantes, colapso de columnas, paredes y cubiertas, incendio, enterramiento parcial o total

Fuente: CINTEL

En la Tabla 73 se registran los estimativos de vulnerabilidad física de las edificaciones ante eventos volcánicos, según juicio de expertos sectoriales.

5.3.1.2.3 Posibles daños a las edificaciones de telecomunicaciones ante tsunamis

De acuerdo con el análisis de resistencia de las edificaciones presentado en el numeral 5.3.1.1 de este documento, se han elaborado las tablas de posibles daños a las edificaciones por los tres fenómenos básicos relacionados con la ocurrencia de un tsunami.

- Fuerzas laterales provenientes de golpes de ola y licuación del terreno
- Fuerzas laterales provenientes de corrientes de agua y material arrastrado
- Inundación de agua salobre

Tabla 34. Tsunami – Golpes de Ola y Fuerzas laterales provenientes de corrientes de agua y material arrastrado y licuación del terreno - Posible daños a edificaciones

POSIBLES DAÑOS A EDIFICACIONES POR GOLPE DE OLA Y FUERZAS LATERALES PROVENIENTES DE CORRIENTES DE AGUA Y MATERIAL ARRASTRADO Y LIUACION DEL TERRENO	
Tipo de edificación	**Posible daño**
Grandes Edificaciones	Agrietamiento, desplazamiento de cimientos, destrucción estructuras portantes, colapso de columnas, paredes y cubiertas, enterramiento, arrastre, parcial o total
Medianas, pequeñas edificaciones, cuartos de equipos	Agrietamiento, desplazamiento de cimientos, destrucción estructuras portantes, colapso de columnas, paredes y cubiertas, enterramiento, arrastre, parcial o total

Fuente: CINTEL

Tabla 35. Tsunami – Inundación de agua salobre - Posible daños a edificaciones

POSIBLES DAÑOS A EDIFICACIONES POR INUNDACION DE AGUA SALOBRE	
Tipo de edificación	**Posible daño**
Grandes Edificaciones	Daños en los acabados de pisos y paredes. Anegación de la edificación
Medianas, pequeñas edificaciones, cuartos de equipos	Daños en los acabados de pisos y paredes. Pisos levantados y paredes debilitadas. Anegación de la edificación

Fuente: CINTEL

En la Tabla 74 se registran los estimativos de vulnerabilidad física de las edificaciones ante tsunamis, según juicio de expertos sectoriales.

5.3.1.2.4 Posibles daños a las edificaciones de telecomunicaciones ante inundaciones de agua dulce

Normalmente, las grandes edificaciones adicionalmente a la aplicación de la Norma Sismo Resistente NSR 98, contemplan en su diseño y construcción los estudios de riesgos de inundación, entre otros, los cuales consultan lógicamente, dentro de las buenas prácticas de ingeniería, el histórico del comportamiento de los niveles de las cuencas hidrográficas circundantes y la existencia de inundaciones y sus niveles en el sitio donde se proyecta realizar una construcción de este tipo.

Los cuartos de equipos, donde normalmente se instalan los equipos de radio, son ubicados en su gran mayoría en sitios elevados por encima de la cota del terreno al cual pretenden cubrir con un servicio de telecomunicaciones dado. Para su ubicación, dentro del site survey realizado siguiendo las buenas prácticas de ingeniería, se trata de ubicar el sitio de transmisión – recepción en la parte más alta de los cerros o en sus laderas, buscando tener línea de vista para los sistemas de antenas, en terrenos estables y geológicamente aptos para este tipo de construcciones que como es lógico, involucra la instalación de una torre de telecomunicaciones.

Por lo anterior, se podría suponer en líneas generales, que las edificaciones donde se instalan equipos de telecomunicaciones tienen baja exposición a este tipo de eventos. Sin embargo, en caso de darse éstas, los posibles daños a las edificaciones se presentan en la Tabla 36.

Tabla 36. Inundaciones – Posible daños a edificaciones

POSIBLES DAÑOS A EDIFICACIONES POR INUNDACIONES DE AGUA DULCE	
Tipo de edificación	**Posible daño**
Grandes Edificaciones	Daños en los acabados de pisos y paredes. Anegación de la edificación
Medianas, pequeñas edificaciones, cuartos de equipos	Daños en los acabados de pisos y paredes. Pisos levantados y paredes debilitadas. Anegación de la edificación

Fuente: CINTEL

En la Tabla 75 se registran los estimativos de vulnerabilidad física de las edificaciones ante inundaciones, según juicio de expertos sectoriales.

5.3.1.3 Posibles daños a los equipos de telecomunicaciones dentro de edificaciones ante eventos naturales

A continuación se presentan las tablas que registran los posibles daños a los equipos de telecomunicaciones y sus periféricos, instalados al interior de las edificaciones, ante las amenazas naturales tratadas y ante el daño de la edificación ya analizado.

5.3.1.3.1 Ante eventos sísmicos

Tabla 37. Eventos sísmicos – Posibles daños a equipos de telecomunicaciones dentro de edificaciones

POSIBLES DAÑOS A EQUIPO DE TELECOMUNICACIONES INSTALADOS DENTRO DE EDIFICACIONES Supuesto: Sólo las grandes edificaciones cumplen NSR 98 (ESCENARIO DE ANALISIS)				
Tipo de Edificación	Temblores de muy baja intensidad (Vibración)	Temblores de baja intensidad (Vibración)	Temblores de intensidad moderada (Vibración)	Temblores de alta intensidad (Vibración, fallas y grietas en la superficie terrestre, licuefacción)
Grandes Edificaciones	Sin daño	Sin daño	Destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, cortos circuitos y/o incendio	Destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, cortos circuitos y/o incendio
Cuartos de Equipos	Sin daño	Sin daño	Destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, cortos circuitos y/o incendio	Destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, cortos circuitos y/o incendio

Fuente: CINTEL

5.3.1.3.2 Ante volcanes

Adicionalmente a los fenómenos ya tratados con relación a los eventos volcánicos, es necesario precisar que la ceniza no solo afecta a la edificación en sí, sino a los equipos instalados en su interior y exterior.

En la Tabla 38 se muestran las probabilidades de fallas a equipos, causadas por cenizas volcánicas, estudiadas por Group Project AELG-19, Auckland, NZ, de 2009.

Tabla 38. Volcán – Nube de Cenizas – Posible afectación a equipo de telecomunicaciones - Proyecto AELG-19

Component	Risk Factors		Probability of Failure				Cause	Comments
			Ash thickness 1-5mm		Ash thickness >5mm			
			Fine grained (<1 mm)	Coarse grained (>1 mm)	Fine grained (<1 mm)	Coarse grained (>1 mm)		
Air conditioning and air handling systems								
Building (large) e.g. telephone exchange communication data centre	Unsealed air-intake (fresh-air cooling)	Moist or Wet ash	Medium	Low	High	Medium	Clogged in-intakes system shuts down	
		Dry ash	Low-medium	Low	Medium	Low		
	Sealed air-intake (high-speed condenser fan)	Moist or Wet ash	Low	Low	Medium	Low-medium		
		Dry ash	Low	Low	Low	Low		
	Sealed air-intake (low-speed condenser fan)	Moist or Wet ash	Medium	Low	High	Medium	Clogged in-intakes system shuts down	
		Dry ash	Low	Low	Low-medium	Low		
Diesel generators	Typically air-intake – Unsealed	Moist or Wet ash	Medium	Low	Medium-High	Low-Medium	Clogged in-intakes system shuts down	
		Dry ash	Low	Low	Low	Low		
Electrical equipment & computers								
		Moist or Wet ash	Medium	Low	High	Low-Medium	shorting corrosion	Probability increases if ash has high salt concentration (> 2%)
		Dry ash	Low	Low	Low	Low		

Fuente: Review of Impacts of Volcanic Ash on Electricity Distribution Systems, Broadcasting and Communication Networks, Auckland Engineering Lifelines Group Project AELG-19, Auckland, NZ, APRIL 2009

La Tabla 39 registra de manera agregada los posibles daños a equipos de telecomunicaciones dentro de edificaciones, ante los diferentes fenómenos volcánicos.

Tabla 39. Volcanes – Posibles daños a equipos de telecomunicaciones dentro de edificaciones

POSIBLES DAÑOS A EQUIPO DE TELECOMUNICACIONES INSTALADOS DENTRO DE EDIFICACIONES				
Tipo de edificación	NUBE DE CENIZA (AFECTACION DE FUNCIONAMIENTO)	CAIDA DE CENIZA (AFECTACION POR PESO - COLAPSO DE TERRAZA)	FLUJOS DE LAVA, MATERIAL PIROCLASTICO Y LODOS	CAIDA DE MATERIAL PIROCLASTICO Y PROYECTILES
Grandes Edificaciones	• Equipos de aire acondicionado y equipos de energía de respaldo: obstrucción en intercambiadores y entradas de aire y corrosión. • Equipo electrónico: contaminación interior del equipo, obstrucción de filtros, aumento de temperatura, cortos circuitos e incendio	Destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, cortos circuitos e incendio	Destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, cortos circuitos e incendio	Destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, cortos circuitos e incendio
Medianas, pequeñas edificaciones, cuartos de equipos	• Equipos de aire acondicionado y equipos de energía de respaldo: obstrucción en intercambiadores y entradas de aire y corrosión. • Equipo electrónico: contaminación interior del equipo, obstrucción de filtros, aumento de temperatura, cortos circuitos e incendio	Destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, cortos circuitos e incendio	Destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, cortos circuitos e incendio	Destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, cortos circuitos e incendio

Fuente: CINTEL

5.3.1.3.3 Ante tsunami

Tabla 40. Tsunami – Posibles daños a equipos de telecomunicaciones dentro de edificaciones

POSIBLES DAÑOS A EQUIPO DE TELECOMUNICACIONES INSTALADOS DENTRO DE EDIFICACIONES			
Tipo de edificación	Fuerzas laterales provenientes de golpes de ola	Fuerzas laterales provenientes de corrientes de agua y material arrastrado	Inundación agua salobre:
Grandes Edificaciones	Destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, cortos circuitos y/o incendio	Destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, arrastre, cortos circuitos y/o incendio	Destrucción de equipos de telecomunicaciones y energía por cortos circuitos y/o incendios, daños residuales por contaminación salina
Medianas, pequeñas edificaciones, cuartos de equipos	Destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, cortos circuitos y/o incendio	Destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, arrastre, cortos circuitos y/o incendio	Destrucción de equipos de telecomunicaciones y energía por cortos circuitos y/o incendios, daños residuales por contaminación salina

Fuente: CINTEL

5.3.1.3.4 Ante inundaciones de agua dulce

Tabla 41. Inundaciones – Posibles daños a equipos de telecomunicaciones dentro de edificaciones

POSIBLES DAÑOS A EQUIPO DE TELECOMUNICACIONES INSTALADOS DENTRO DE EDIFICACIONES	
Tipo de edificación	**Inundación agua dulce**
Grandes Edificaciones	Destrucción de equipos de telecomunicaciones y energía por cortos circuitos y/o incendios
Medianas, pequeñas edificaciones, cuartos de equipos	Destrucción de equipos de telecomunicaciones y energía por cortos circuitos y/o incendios

Fuente: CINTEL

En las tablas Tabla 72, Tabla 73, Tabla 74 y Tabla 75 se registran los estimativos de vulnerabilidad física de los equipos de telecomunicaciones y sus periféricos ante los diferentes eventos naturales tratados, según juicio de expertos sectoriales.

5.3.2 Torres - Antenas

Son todas aquellas estructuras metálicas que sirven de soporte mecánico a los sistemas de antenas utilizados por los diferentes servicios de telecomunicaciones vitales.

A continuación, se detallan los tipos de antenas que se utilizan para la prestación de los diferentes servicios de telecomunicaciones considerados.

5.3.2.1 Servicio Portador

Antenas de microondas y parabólicas instaladas en sus propias bases con las cuales se presta el servicio portador complementariamente a la red de fibra óptica, en lugares geográfica y topográficamente de difícil acceso.

5.3.2.2 Servicio de Telefonía Pública Básica conmutada y acceso a INTERNET fijo

Antenas de microondas y parabólicas instaladas en sus propias bases con las cuales se complementa o se da redundancia a la red troncal y/o primaria; antenas de acceso fijo inalámbrico (wireless local loop), cuando se presta el servicio a través de esta modalidad.

5.3.2.3 Servicio de Telefonía Móvil Celular y acceso a INTERNET móvil

Antenas de cubrimiento de las BTS/NODOS, microondas y/o comunicación satelital de enlace de la BTS/NODOS con sus elementos de orden superior.

5.3.2.4 Servicio de Radiodifusión Sonora AM & FM

Antenas de microondas y/o parabólicas instaladas en sus propias bases para enlace con estudio y antenas de radiodifusión AM o FM.

5.3.2.5 Servicio de Televisión Radiodifundida

Parabólicas (TVRO – Television Reception Only) instaladas en sus propias bases para enlace con centro de emisión y antenas de televisión radiodifundida VHF - UHF.

5.3.2.6 Servicio de Televisión por Cable

Antenas de microondas y parabólicas (TVRO) instaladas en la cabecera en sus propias bases para señales de contribución.

5.3.2.7 Servicio de Móvil Marítimo

Antenas de microondas y/o parabólicas instaladas en sus propias bases en estaciones costeras.

5.3.2.8 Servicio de Móvil Aeronáutico

Antenas de microondas y/o parabólicas instaladas en sus propias bases en estaciones aeronáuticas.

5.3.2.9 COMPARTEL

Antenas parabólicas instaladas en sus propias bases (HUB) y mástiles con VSAT en puntos COMPARTEL.

5.3.2.10 Redes de comunicaciones de emergencia

Antenas de bases y repetidoras.

5.3.2.11 Redes de telemetría

Antenas parabólicas instaladas en sus propias bases (HUB) y mástiles con VSAT en estaciones de medición.

5.3.2.12 Servicio de Radioaficionados

Mástiles con dipolos.

5.3.2.13 Resistencia y vulnerabilidad de las torres

Las torres utilizadas en los servicios de telecomunicaciones, poseen varios diseños de acuerdo, básicamente, con la cantidad prevista de antenas a instalar en ella, su geometría, área, peso, orientación, velocidad del viento y restricciones de espacio, entre otros.

El diseño de las torres utilizadas por los diferentes prestadores de servicios de telecomunicaciones, se realiza con base en las normas AISC última edición, ASCE report 52, EIA/TIA 222 F (1996), ANSI/ASCE 10-90 (1991),

ACI 318 última edición, NSR10[34] y está sujeto al análisis de verticalidad y giro torsional, cargas sobre la estructura, entre otros.

En el Anexo I de la norma EIA/TIA 222 F, se recomienda que una empresa especializada en geotecnia realice un estudio geotécnico de suelo en el sitio de emplazamiento de cada torre a fin de determinar el tipo de suelo específico y sus características físicas únicas, y también, para obtener datos que permitan desarrollar parámetros de diseño seguros, alternativas de fundación económicas y procedimientos de instalación adecuados.

El proceso de selección del sitio donde se instalará la torre, implica la consecución de un suelo normal cohesivo, con la capacidad portante y capacidad horizontal por metro de profundidad adecuada. Se evalúa geotécnicamente, se analiza su vulnerabilidad sísmica y se evitan terrenos rocosos, pantanosos o arenosos.

Los tipos de torres varían de acuerdo con las necesidades, los tipos más comunes son: auto soportadas, cuadradas y rendadas triangulares.

Las torres diseñadas y construidas bajo las normas mencionadas, y tomando en consideración que se diseñan típicamente para soportar viento de hasta 160 Km por hora incidiendo sobre las caras de mayor área de las antenas instaladas, con relación a las diferentes amenazas naturales debieran entonces soportar el estrés mecánico producido por los sismos tal como se

---

[34] Es de puntualizar, sin embargo, que de acuerdo con el numeral A.1.2.4 — EXCEPCIONES —, del Reglamento de Construcciones Sismo Resistentes, NSR-10, éste no se aplica al diseño y construcción de estructuras especiales tales como puentes, torres de transmisión, torres y equipos industriales, muelles, estructuras hidráulicas y todas aquellas construcciones diferentes de edificaciones.

referencia a continuación y, de manera análoga, debieran resistir otras amenazas materializadas como estrés mecánico a la estructura de la torre.

5.3.2.13.1 Con relación a los sismos

- Temblores de poca intensidad sin daño.
- Temblores moderados con posibles cambios en la verticalidad.
- Un temblor fuerte con daños a elementos estructurales y no estructurales, con cambios notorios en la verticalidad y caída de torres[35].

5.3.2.13.2 Con relación a los volcanes

- Caída de ceniza volcánica : La nube de ceniza volcánica, con relación a las torres y antenas tiene dos efectos básicos, el deterioro a mediano plazo que causa en los materiales de construcción y el peso o presión que ésta causa sobre las plataformas de la torre y en los sistemas radiantes cuando se acumula sobre ellas. Tomando en consideración que las torres de telecomunicaciones están diseñadas y construidas con factores de sobre carga y vientos de 160 Km por hora, se supone para este estudio que las acumulaciones moderadas de cenizas en la torre y en las antenas no deben causar su colapso, ni su caída.

---

[35]El informe preliminar sobre el terremoto ocurrido en Chile en febrero de 2010, preparado por Technical Council on Lifeline Earthquake Engineering (TCLEE), en las regiones VII y VIII fue común que las antenas se desprendieran de sus torres, que las celdas instaladas sobre terrazas de edificios comerciales se dañaran cuando el edificio se afectó estructuralmente Un operador reportó problemas con las antenas en el 50% de sus sitios. Se cayeron al menos dos torres. Alrededor del 70% al 80% de las celdas en las regiones VII y VIII tuvieron problemas con equipo o daños de la antena. Esta tasa se reduce al 50% en la V región, sobre todo en sitios ubicados en los techos (Technical Council on Lifeline Earthquake Engineering (TCLEE) Preliminary Report 27 February 2010 Mw8.8 Offshore Maule, Chile Earthquake)

- Flujos de lava, material piroclástico y lodos: Es altamente probable que las torres y sistemas radiantes instalados en ellas resulten destruidos, arrasados, enterrados o con graves fallas estructurales, si están a su paso.
- Caída de material piroclástico y proyectiles: Es altamente probable que las torres y sistemas radiantes instaladas en ellas, ubicadas en las zonas de caída de este material volcánico (piroclastos y proyectiles balísticos), resulten con daños estructurales y destruidas por incendio.

5.3.2.13.3 Con relación a los tsunamis

- Inundaciones ocasionales que no socaven los cimientos de la torre o generen oxidación a sus elementos estructurales.
- Golpes de ola de poca intensidad sin daño.
- Golpes de ola moderados sin daño estructural, pero posiblemente con algún cambio en la verticalidad.
- Golpes de ola fuertes con daños a elementos estructurales y no estructurales con cambios notorios en la verticalidad y caída de la torre.
- Fuerzas leves laterales provenientes de corrientes de agua y material arrastrado sin daño.
- Fuerzas moderadas laterales provenientes de corrientes de agua y material arrastrado sin daño estructural, pero posiblemente con algún daño a los elementos no estructurales y algún cambio en la verticalidad.
- Fuerzas laterales fuertes provenientes de corrientes de agua y material arrastrado con daños a elementos estructurales y no estructurales con cambios notorios en la verticalidad y caída de la torre.

5.3.2.13.4 Con relación a las inundaciones de agua dulce

- Inundaciones ocasionales que no generen deslizamientos

5.3.2.14 Posibles daños de las torres de telecomunicaciones y las antenas instaladas ante eventos naturales

Con base en la resistencia de las torres, tratada en el numeral 5.3.2.13 de este documento, se presentan las tablas de posibles daños a torres y antenas según tipo de amenaza.

5.3.2.14.1 Ante eventos sísmicos

Tabla 42. Eventos sísmicos – Posibles daños a Torres

POSIBLES DAÑOS A TORRES Supuesto: Las torres cumplen con las normas AISC última edición, ASCE report 52, EIA/TIA 222 F (1996), ANSI/ASCE 10-90 (1991), ACI 318 última edición y NSR98				
	Temblores de muy baja intensidad (Vibración)	Temblores de baja intensidad (Vibración)	Temblores de intensidad moderada (Vibración)	Temblores de alta intensidad (Vibración, fallas y grietas en la superficie terrestre, licuefacción)
Torres	Sin daño	Sin daño	Posibles cambios en la verticalidad	Daños a elementos estructurales y no estructurales, con cambios notorios en la verticalidad y caída de torres

Fuente: CINTEL

Tabla 43. Eventos sísmicos – Posibles daños a Antenas

POSIBLES DAÑOS A ANTENAS Supuesto: Antenas instaladas según mejores prácticas				
	Temblores de muy baja intensidad (Vibración)	Temblores de baja intensidad (Vibración)	Temblores de intensidad moderada (Vibración)	Temblores de alta intensidad (Vibración, fallas y grietas en la superficie terrestre, licuefacción)
Antenas	Sin daño	Sin daño	Desapuntamiento de antenas por movimiento y deformación de las torres.	Desapuntamiento de antenas por movimiento y deformación de las torres , pérdida total o parcial de los sistemas de antenas por caida de estos o por caida de la torre

Fuente: CINTEL

5.3.2.14.2 Ante volcanes

En la Tabla 44 se muestran las probabilidades de fallas de torres, mástiles, redes aéreas y antenas, causadas por cenizas volcánicas, estudiadas por el Proyecto AELG-19.

Tabla 44. Volcán – Nube de Cenizas – Posible afectación de torres, mástiles, redes aéreas y antenas - Proyecto AELG-19

Component	Risk Factors		Probability of Failure				Cause	Comments
Lines, Cables, Masts, Aerials, Antennae, Towers								
Above ground			Ash thickness 5-100mm		Ash thickness >100mm			
			Fine grained (<1 mm)	Coarse grained (>1 mm)	Fine grained (<1 mm)	Coarse grained (>1 mm)		
		Moist or Wet ash	Low-Medium	Low	High	Low-medium	Collapse, buckling due to ash loading	Fine grained ash adheres more to structures; coarser grained ash falls off (wind and rain)
		Dry ash	Low	Low	Medium	Low	Collapse due to trees falling	Underground cables not affected

Fuente: Review of Impacts of Volcanic Ash on Electricity Distribution Systems, Broadcasting and Communication Networks, Auckland Engineering Lifelines Group Project AELG-19, Auckland, NZ, APRIL 2009.

Las tablas Tabla 45 y Tabla 46, registran de manera agregada los posibles daños a torres y antenas, ante los diferentes fenómenos volcánicos.

Tabla 45. Volcanes – Posibles daños a Torres

POSIBLES DAÑOS A TORRES				
	NUBE DE CENIZA (AFECTACION DE FUNCIONAMIENTO)	CAIDA DE CENIZA (AFECTACION POR PESO)	FLUJOS DE LAVA, MATERIAL PIROCLASTICO Y LODOS	CAIDA DE MATERIAL PIROCLASTICO Y PROYECTILES
Torres	Deterioro a mediano plazo por corrosión	Colapso (baja probabilidad)	Agrietamiento, desplazamiento de cimientos de la base de la torre, deformación, caida, arrastre, enterramiento parcial o total, incineración	Agrietamiento, desplazamiento de cimientos de la base de la torre, deformación, caida, enterramiento parcial o total, incineración

Fuente: CINTEL

Tabla 46. Volcanes – Posibles daños a Antenas

POSIBLES DAÑOS A ANTENAS				
	NUBE DE CENIZA (AFECTACION DE FUNCIONAMIENTO)	CAIDA DE CENIZA (AFECTACION POR PESO)	FLUJOS DE LAVA, MATERIAL PIROCLASTICO Y LODOS	CAIDA DE MATERIAL PIROCLASTICO Y PROYECTILES
Antenas	Deterioro a mediano plazo por corrosión (Ver Afectación de Espectro radioeléctrico)	Colapso (baja probabilidad)	Desapuntamiento de antenas por movimiento y deformación de las torres , pérdida total o parcial de los sistemas de antenas por caida de estos o por caida de la torre , destrucción, arrastre e incineración	Desapuntamiento de antenas por impacto y deformación de las torres , pérdida total o parcial de los sistemas de antenas por caida de estos o por caida de la torre , destrucción e incineración

Fuente: CINTEL

5.3.2.14.3 Ante tsunamis

Tabla 47. Tsunami – Posibles daños a Torres

POSIBLES DAÑOS A TORRES			
	Fuerzas laterales provenientes de golpes de ola y licuación del terreno	Fuerzas laterales provenientes de corrientes de agua y material arrastrado	Inundación agua salobre:
Torres	Daños a elementos estructurales y no estructurales, con cambios notorios en la verticalidad y caída de torres	Daños a elementos estructurales y no estructurales, con cambios notorios en la verticalidad y caída de torres	Socavación de cimientos de la torre / Oxidación a mediano plazo de sus elementos estructurales

Fuente: CINTEL

Tabla 48. Tsunami – Posibles daños a Antenas

POSIBLES DAÑOS A ANTENAS			
	Fuerzas laterales provenientes de golpes de ola y licuación del terreno	Fuerzas laterales provenientes de corrientes de agua y material arrastrado	Inundación agua salobre:
Antenas	Desapuntamiento de antenas por movimiento y deformación de las torres , pérdida total o parcial de los sistemas de antenas por caida de estos o por caida de la torre , destrucción, arrastre	Desapuntamiento de antenas por movimiento y deformación de las torres , pérdida total o parcial de los sistemas de antenas por caida de estos o por caida de la torre , destrucción, arrastre	

Fuente: CINTEL

5.3.2.14.4 Ante inundaciones de agua dulce

Tabla 49. Inundaciones de agua dulce – Posibles daños a torres y antenas

POSIBLES DAÑOS A TORRES Y ANTENAS POR INUNDACIONES DE AGUA DULCE	
	Posible daño
Torres	Socavación de cimientos de la torre
Antenas	

Fuente: CINTEL

En las tablas Tabla 72, Tabla 73, Tabla 74 y Tabla 75 se registran los estimativos de vulnerabilidad física de las torres y antenas ante los diferentes eventos naturales tratados, según juicio de expertos sectoriales.

5.3.2.15 Espectro radioeléctrico

El espectro radioeléctrico es utilizado por varios servicios de telecomunicaciones, ya sea como el medio básico de transmisión o como el respaldo o backup a los otros medios de transmisión.

5.3.2.15.1 Utilización básica del espectro radioeléctrico

Servicio Portador

El servicio portador utiliza enlaces de microondas por encima de 1 GHz y enlaces satelitales en banda C (3,7 GHz a 4,2 GHz y 5,92 GHz a 6,42 GHz) y banda KU (10,7 GHz a 12,75 GHz y 13 GHz a 15 GHz) con el cual presta el servicio portador complementariamente a la red de fibra óptica, en lugares geográfica y topográficamente de difícil acceso.

Servicio de Telefonía Pública Básica Conmutada y acceso a INTERNET fijo

Estos servicios utilizan enlaces de microondas por encima de 1 GHz y enlaces satelitales en banda C (3,7 GHz a 4,2 GHz y 5,92 GHz a 6,42 GHz) y banda KU (10,7 GHz a 12,75 GHz y 13 GHz a 15 GHz) con el cual complementa o se da redundancia a la red troncal y/o primaria; adicionalmente utilizan las bandas de 300 MHz, 900 MHz, 1,5 GHz, 1,9 GHz y 2,5 GHz para aplicaciones de acceso fijo inalámbrico (wireless local loop), cuando se presta el servicio a través de esta modalidad.

Servicio de Telefonía Móvil Celular y acceso a INTERNET móvil

Este servicio utiliza enlaces de microondas por encima de 1 GHz para enlazar sus BTS y NODOS con los BSC y las bandas de frecuencias de 806 MHz a 936 MHz, 1850 MHz a 1990 MHz como medio para cubrimiento en sus estaciones.

Servicio de Radiodifusión Sonora AM & FM

Este servicio utiliza la banda de 300 MHz para los enlaces estudio transmisor, enlaces satelitales en banda C (3,7 GHz a 4,2 GHz y 5,92 GHz a 6,42 GHz) y banda KU (10,7 GHz a 12,75 GHz y 13 GHz a 15 GHz) con el mismo propósito y las bandas de 535 kHz a 1705 kHz y 88 MHz a 108 MHz para radiodifundir la señal en AM y en FM respectivamente.

Servicio de Televisión Radiodifundida

La televisión radiodifundida utiliza para su red de transporte enlaces satelitales en banda C (3,7 GHz a 4,2 GHz y 5,92 GHz a 6,42 GHz) y banda KU (10,7 GHz a 12,75 GHz y 13 GHz a 15 GHz) y algunos enlaces en banda de 6 GHz y las bandas de 54 MHz a 72 MHz, 76 MHz a 88 MHz, 174 MHz a 216 MHz, 470 MHz a 512 MHz y 512 MHz a 698 MHz para la red de radiodifusión de sus señales.

Servicio de Televisión por Cable

El servicio de televisión por cable utiliza microondas por encima de 1 GHz y enlaces satelitales en banda C (3,7 GHz a 4,2 GHz y 5,92 GHz a 6,42 GHz) y banda KU (10,7 GHz a 12,75 GHz y 13 GHz a 15 GHz) para señales de contribución.

Servicio de Móvil Marítimo

Las bandas asignadas para los servicios de móvil marítimo son:

MOVIL MARITIMO			
R9 kHz - 14 kHz	R315 kHz - 325 kHz	6200 kHz - 6525 kHz	156,025 MHz - 162,025 MHz
14 kHz - 19,95 kHz	R405 kHz - 415 kHz	8100 kHz - 8195 kHz	156,4875 MHz - 156,5625 MHz
20,05 kHz - 70 kHz	415 kHz - 495 kHz	8195 kHz - 8815 kHz	156,7625 MHz- 157,45 MHz
70 kHz - 90 kHz	505 kHz - 510 kHz	12230 kHz - 13200 kHz	160,6 MHz - 162,05 MHz
R90 kHz - 110 kHz	2065 kHz - 2107 kHz	16360 kHz - 17410 kHz	216 MHz-220 MHz
110 kHz - 130 kHz	2170 kHz - 2173,5 kHz	18780 kHz - 18900 kHz	R 5470 MHz - 5570 MHz
130 kHz - 135,7 kHz	2173,5 kHz - 2190,5 kHz	19680 kHz - 19800 kHz	R5570 MHz - 5650 MHz
135,7 kHz - 137,8 kHz	2190,5 kHz - 2194 kHz	22000 kHz - 22855 kHz	R8850 MHz - 9000 MHz
137,8 kHz - 160 kHz	4000 kHz - 4063 kHz	25070 kHz - 25210 kHz	R9200 MHz- 9300 MHz
R285 kHz - 315 kHz	4063 kHz - 4438 kHz	26100 kHz - 26175 kHz	

Fuente: Cuadro Nacional de Atribución de Frecuencias 2010

Servicio de Móvil Aeronáutico

Las bandas asignadas para los servicios de móvil aeronáutico son:

MOVIL AERONAUTICO				
R190 kHz - 200 kHz	5450 kHz - 5480 kHz	21294 kHz - 22000 kHz	R5000 MHz- 5010 MHz	R15,43 GHz - 15,63 GHz
R200 kHz - 275 kHz	5480 kHz - 5680 kHz	23200 kHz - 23350 kHz	R5010 MHz - 5030 MHz	R15,63 GHz - 15,7 GHz
R275 kHz - 285 kHz	5680 kHz - 5730 kHz	R74,8 MHz - 75,2 MHz	R5030 MHz - 5091 MHz	R24,25 GHz - 24,45 GHz
R285 kHz - 315 kHz	6525 kHz - 6685 kHz	R108 MHz - 117,975 MHz	R5091 MHz - 5150 MHz	R24,45 GHz - 24,65 GHz
R325 kHz - 335 kHz	6685 kHz - 6765 kHz	117,975 MHz - 137 MHz	R5150 MHz - 5250 MHz	R31,8 GHz - 32 GHz
R335 kHz - 405 kHz	8815 kHz - 8965 kHz	R960 MHz- 1164 MHz	R5350 MHz - 5460 MHz	R32 GHz - 32,3 GHz
R405 kHz - 415 kHz	8965 kHz - 9040 kHz	R1164 MHz- 1215 MHz	R5460 MHz - 5470 MHz	R32,3 GHz- 33 GHz
R510 kHz - 525 kHz	10005 kHz - 10100 kHz	R1300 MHz - 1350 MHz	R8750 MHz - 8850 MHz	R33 GHz - 33,4 GHz
R525 kHz - 535 kHz	11175 kHz - 11275 kHz	R1559 MHz - 1610 MHz	R9000 MHz- 9200 MHz	
R1705 kHz - 1800 kHz	11275 kHz - 11400 kHz	R1610 MHz- 1610,6 MHz	R9300 MHz- 9500 MHz	
2850 kHz - 3025 kHz	13200 kHz - 13260 kHz	R1610,6 MHz - 1613,8 MHz	R9500 MHz - 9800 MHz	
3025 kHz - 3155 kHz	13260 kHz - 13360 kHz	R1613,8 MHz- 1626,5 MHz	R13,25 GHz - 13,4 GHz	
3400 kHz - 3500 kHz	15010 kHz - 15100 kHz	R2700 MHz- 2900 MHz	R14 GHz - 14,25 GHz	
4650 kHz- 4700 kHz	17900 kHz - 17970 kHz	R2900 MHz - 3100 MHz	R14,25 GHz - 14,3 GHz	
4700 kHz - 4750 kHz	17970 kHz - 18030 kHz	R4200 MHz - 4400 MHz	R15,4 GHz - 15,43 GHz	

Fuente: Cuadro Nacional de Atribución de Frecuencias 2010

Servicio de Radioaficionados

Las bandas asignadas para el servicio de radioaficionados son:

SERVICIO	BANDAS ATRIBUIDAS	
Banda Ciudadana / Servicios Especiales	26,960 MHz - 27,410 MHz	
Banda Ciudadana / Servicio Auxiliar de Ayuda	27,035 MHz - 27,075	
Aficionados	1800 kHz - 1850 kHz	24890 kHz - 24990 kHz
	1850 kHz - 2000 kHz	28 MHz - 29,7 MHz
	3500 kHz - 3750 kHz	50 MHz- 54 MHz
	3750 kHz - 4000 kHz	144 MHz - 146 MHz
	7000 kHz - 7100 kHz	146 MHz - 148 MHz
	7100 kHz - 7200 kHz	220 MHz - 225 MHz
	7200 kHz - 7300 kHz	430 MHz - 432 MHz
	14000 kHz - 14250 kHz	432 MHz - 438 MHz
	14250 kHz - 14350 kHz	438 MHz - 440 MHz
	18068 kHz - 18168 kHz	24 GHz - 24,05 GHz
	21000 kHz - 21450 kHz	

Fuente: Cuadro Nacional de Atribución de Frecuencias 2010

COMPARTEL

Utiliza enlaces satelitales en banda C (3,7 GHz a 4,2 GHz y 5,92 GHz a 6,42 GHz) y banda KU (10,7 GHz a 12,75 GHz y 13 GHz a 15 GHz).

Redes de comunicaciones de emergencia

Utilizan frecuencias específicas en VHF y UHF hasta 470 MHz.

5.3.2.15.2 Vulnerabilidad del espectro radioeléctrico

Las ondas electromagnéticas se propagan en el vacío y por lo tanto, cualquier partícula podría llegar a afectar las condiciones de propagación de las ondas electromagnéticas en función de su tamaño y densidad en el ambiente.

En el proyecto AELG-19, en el cual se estudia la vulnerabilidad del espectro radioeléctrico ante la presencia de cenizas volcánicas, se tomaron como antecedentes las principales erupciones volcánicas de los últimos 25 años a nivel internacional, lo cual desde el punto de vista de experiencia mostró que no existe ningún antecedente de disrupción de los servicios de telecomunicaciones a causa de la polución del medio de propagación.

A nivel teórico y tomando en consideración el tamaño de la ceniza, el estudio mencionado introduce una probabilidad de falla en los servicios de telecomunicaciones, tal como se presenta en la Tabla 50, causada por estática originada en descargas eléctricas y desvanecimiento.

Tabla 50. Volcán – Nube de Cenizas – Posible afectación a sistemas de telecomunicaciones por polución del espectro radioeléctrico - Proyecto AELG-19

Component	Risk Factors		Probability of Failure				Cause	Comments
			Ash thickness 5-100mm		Ash thickness >100mm			
			Fine grained (<1 mm)	Coarse grained (>1 mm)	Fine grained (<1 mm)	Coarse grained (>1 mm)		
Signal transmission and attenuation								
Low Frequency	AM radio, HF maritime and aeronautical	Moist or Wet ash	Low-Medium	Low-Medium	Medium	Medium	Static caused by lightning Signal drop-out	
		Dry ash	Low-Medium	Low-Medium	Medium	Medium		
High frequency	FM radio, VHF, UHF, cellular, microwave linking, satellite	Moist or Wet ash	Low-Medium	Low-Medium	Low-Medium	Low-Medium	Static caused by lightning Signal drop-out	
		Dry ash	Low	Low	Low	Low		

Fuente: Review of Impacts of VolcanicAsh on Electricity DistributionSystems, Broadcasting andCommunication Networks, Auckland Engineering Lifelines GroupProject AELG-19, Auckland, NZ, APRIL 2009

Por otro lado, en el análisis realizado[36] después de la erupción del volcán islandés Eyjafjallajökull, el cual generó una nube de ceniza volcánica que se propagó por el norte y el centro de Europa, se parte de que las partículas de la nube volcánica están cargadas eléctricamente y se ubican a una altitud aproximada de 3 Km, razón por la cual se estima que podrían afectar los sistemas ubicados en estas zonas.

Figura 64. Volcán Eyjafjallajökull - Nube de Cenizas

FUENTE: NASA image courtesy Jeff Schmaltz, MODIS Rapid Response Team at NASA GSFC. CaptionbyHolliRiebeek.

[36] **En este documento se incluyen los resultados del estudio de Ismael Pellejero Ibáñez - Ingeniero de Telecomunicación, sobre el impacto de las cenizas en las comunicaciones que hacen uso del espectro radioeléctrico.**

Para las comunicaciones de HF, se hace la aproximación de tomar la nube de ceniza como un plasma, de características similares a la ionosfera, cuya concentración no es muy alta, pierde densidad en la medida que avanza y es dispersada por el viento, lo cual permite estimar que las comunicaciones de HF no se verían afectadas por la nube de cenizas, aunque podría presentarse algo de ruido.

En el estudio mencionado, para la banda de VHF se aproxima vía la teoría del radar, en la cual la nube se caracteriza por su “sección recta radar” (RCS). Cuanto mayor sea su RCS, mayor reflexión de las ondas de radio. La RCS depende del área geométrica de la nube, del diámetro y forma de sus partículas y de su reflectividad. Es decir, que entre más dispersa este la nube, menor será su reflectividad, lo que significa que entre más lejos del volcán su efecto es menor.

Finalmente, el estudio establece que las partículas de la nube parecen tener un tamaño del orden de los milímetros, luego afectarán en mayor medida a la banda de EHF (30-300 GHz). No obstante, en puntos donde la nube sea más densa y las partículas se agrupen con tamaños cercanos al centímetro, también se vería afectada la banda de SHF (3-30 GHz).Los efectos serían principalmente un aumento de la absorción (fading) y de la dispersión (scattering) y podrían llegar a afectar a algunos sistemas de comunicaciones por satélite.

El estudio concluye que las bandas de VHF y UHF solamente se verían afectadas en zonas muy próximas al volcán y que aún así, se trata de una cuestión difícil de predecir.

5.3.2.15.3 Posible afectación a sistemas de telecomunicaciones

Tomando en consideración los estudios previos se han estimado, en este estudio, las siguientes posibilidades de afectación de los sistemas de telecomunicaciones por cenizas volcánicas, Tabla 51.

Tabla 51. Volcán – Nube de Cenizas – Posible afectación a sistemas de telecomunicaciones por polución del espectro radioeléctrico

POSIBLE AFECTACION DE SISTEMAS QUE HACEN USO DEL ESPECTRO RADIOELECTRICO POR CENIZA VOLCANICA (POSIBLE RUIDO Y PEQUEÑOS DESVANECIMIENTOS EN FRECUENCIAS POR ENCIMA DE 3OO MHz, CON MAYOR PROBABILIDAD EN FRECUENCIAS ENTRE 30 GHz y 300 GHz)		
SERVICIOS DE TELECOMUNICACIONES CON INFRAESTRUCTURA INALAMBRICA	**Nube densa (En cercanía al volcan)**	**Nube dispersa de cenizas**
Servicio portador: microondas por encima de 1 GHz y enlaces satelitales en banda C (3,7 GHz a 4,2 GHz y 5,92 GHz a 6,42 GHz) y banda KU (10,7 GHz a 12,75 GHz y 13 GHz a 15 GHz)	**Medio - baja**	**Baja**
Servicio de Telefonía Pública Básica conmutada y acceso a INTERNET fijo: enlaces de microondas por encima de 1 GHz y enlaces satelitales en banda C (3,7 GHz a 4,2 GHz y 5,92 GHz a 6,42 GHz) y banda KU (10,7 GHz a 12,75 GHz y 13 GHz a 15 GHz) ; bandas de 300 MHz, 900 MHz, 1,5 GHz, 1,9 GHz y 2,5 GHz	**Medio - baja**	**Baja**
Servicio de Telefonía Móvil Celular y acceso a INTERNET móvil: enlaces de microondas por encima de 1 GHz y las bandas de 806 MHz a 936 MHz, 1850 MHz a 1990 MHz	**Medio - baja**	**Baja**
Servicio de Radiodifusión Sonora AM & FM: banda de 300 MHz , enlaces satelitales en banda C (3,7 GHz a 4,2 GHz y 5,92 GHz a 6,42 GHz) y banda KU (10,7 GHz a 12,75 GHz y 13 GHz a 15 GHz) y bandas de 535 kHz a 1705 kHz y 88 MHz a 108 MHz	**Medio - baja**	**Baja**
Servicio de Televisión Radiodifundida : enlaces satelitales en banda C (3,7 GHz a 4,2 GHz y 5,92 GHz a 6,42 GHz) y banda KU (10,7 GHz a 12,75 GHz y 13 GHz a 15 GHz), banda de 6 GHz y las bandas de 54 MHz a 72 MHz, 76 MHz a 88 MHz, 174 MHz a 216 MHz, 470 MHz a 512 MHz y 512 MHz a 698 MHz	**Medio - baja**	**Baja**
Servicio de Televisión por Suscripción: microondas por encima de 1 GHz y enlaces satelitales en banda C (3,7 GHz a 4,2 GHz y 5,92 GHz a 6,42 GHz) y banda KU (10,7 GHz a 12,75 GHz y 13 GHz a 15 GHz)	**Medio - baja**	**Baja**
Servicio de Móvil maritimo: múltiples bandas desde 9 kHz hasta 26 GHz	**Medio - baja**	**Baja**
Servicio de Móvil Aeronáutico: múltiples bandas desde 190 kHz hasta 33 GHz	**Medio - baja**	**Baja**
Servicio de radioaficionados y banda ciudadana: múltiples bandas desde 1800 kHz hasta 24 GHz	**Medio - baja**	**Baja**
Compartel: enlaces satelitales en banda C (3,7 GHz a 4,2 GHz y 5,92 GHz a 6,42 GHz) y banda KU (10,7 GHz a 12,75 GHz y 13 GHz a 15 GHz).	**Medio - baja**	**Baja**
Redes de comunicaciones de emergencia: frecuencias específicas en VHF y UHF hasta 470 MHz	**Medio - baja**	**Baja**

Fuente: CINTEL

5.3.3 Armarios, gabinetes y shelters

Son utilizados primordialmente por los servicios de telecomunicaciones, según se describe a continuación.

5.3.3.1 Servicio de Telefonía Pública Básica Conmutada y acceso a INTERNET fijo

- Armarios
- Gabinetes donde se encuentran instalados los concentradores remotos, gateways, estaciones base de soluciones inalámbricas (WLL).

5.3.3.2 Servicio de Telefonía Móvil Celular y acceso a INTERNET móvil

Gabinetes & Shelters donde se encuentran instalados las BS, Nodos B y Gateways.

5.3.3.3 Servicio de Móvil Marítimo

Gabinetes de ayuda a la navegación.

5.3.3.4 Servicio de Móvil Aeronáutico

Gabinetes de ayuda a la navegación.

5.3.3.5 Redes de telemetría

Gabinetes de telemetría.

5.3.3.6 Resistencia y vulnerabilidad de los armarios, gabinetes y shelters

Los armarios, gabinetes y shelters utilizados en los servicios de telecomunicaciones, poseen varios diseños, con especificaciones dimensionales, mecánicas y funcionales que varían según su aplicación específica y el operador de telecomunicaciones que hace uso de ellos.

Por el tipo de construcción y materiales utilizados, estos elementos están sujetos a las siguientes amenazas:

5.3.3.6.1 Con relación a los sismos

- Temblores de poca y moderada intensidad sin daño.
- Temblores fuertes con posibilidad de disrupción de red en presencia de agrietamientos de la superficie terrestre o fenómenos de licuefacción.

5.3.3.6.2 Con relación a los volcanes

- Caída de ceniza volcánica : La nube de ceniza volcánica, con relación a los armarios, gabinetes y shelters tiene tres efectos básicos: el deterioro a mediano plazo que causa en los materiales de construcción, el peso o presión que la acumulación de cenizas causa sobre la superficie superior de estos elementos y el mal funcionamiento en equipos de telecomunicaciones, periféricos y accesorios instados en su interior por contaminación interior del equipo, obstrucción de filtros, aumento de temperatura y cortos circuitos. Se supone para este estudio que las acumulaciones moderadas de cenizas en las superficies superiores de armarios, gabinetes y shelters no deben causar su colapso, ni su caída.
- Flujos de lava, material piroclástico y lodos: Es altamente probable que los armarios, gabinetes y shelters resulten destruidos, arrasados o enterrados, si están a su paso.
- Caída de material piroclástico y proyectiles: Es altamente probable que los armarios, gabinetes y shelters, ubicados en las zonas de caída de este material volcánico (piroclastos y proyectiles balísticos), resulten con daños estructurales y destruidos por incendio.

5.3.3.6.3 Con relación a los tsunamis

- Golpes de ola de poca intensidad sin daño a la estructura del armario, gabinete o shelter, pero con grandes posibilidades de inundaciones en su interior.
- Golpes de ola moderados y fuertes con agrietamiento, desplazamiento de cimientos, arrastre, enterramiento parcial o total, el cual causará destrucción por desprendimiento, por aplastamiento, arrastre, cortos circuitos y/o incendio, disrupción de red e inundaciones en su interior.
- Fuerzas leves laterales provenientes de corrientes de agua y material arrastrado sin daño, pero con grandes posibilidades de inundaciones en su interior.
- Fuerzas laterales moderadas y fuertes provenientes de corrientes de agua y material arrastrado con agrietamiento, desplazamiento de cimientos, arrastre, enterramiento parcial o total, el cual causará destrucción por desprendimiento, por aplastamiento, arrastre, cortos circuitos y/o incendio, disrupción de red e inundaciones en su interior.
- Inundaciones de agua salobre, que generarán el mal funcionamiento en equipos de telecomunicaciones, periféricos y accesorios instalados en su interior, por anegación del equipo, cortos circuitos y daños residuales por contaminación salina.

5.3.3.6.4 Con relación a las inundaciones de agua dulce

Inundaciones que generarán el mal funcionamiento en equipos de telecomunicaciones, periféricos y accesorios instalados en su interior por anegación del equipo y cortos circuitos.

5.3.3.7 Posibles daños de los armarios, gabinetes y shelters ante eventos naturales

Con base en la resistencia de estos elementos, tratada en el numeral 5.3.3.6 de este documento, se presentan las tablas de posibles daños según tipo de amenaza.

5.3.3.7.1 Ante eventos sísmicos

Tabla 52. Eventos sísmicos – Posibles daños a armarios, gabinetes y shelters

POSIBLES DAÑOS A ARMARIOS / GABINETES / SHELTERS				
	Temblores de muy baja intensidad (Vibración)	Temblores de baja intensidad (Vibración)	Temblores de intensidad moderada (Vibración)	Temblores de alta intensidad (Vibración, fallas y grietas en la superficie terrestre, licuefacción)
Armarios / Gabinetes / Shelters	Sin daño	Sin daño	Sin daño	Agrietamiento, desplazamiento de cimientos, disrupción de la red.

Fuente: CINTEL

5.3.3.7.2 Ante volcanes

En la Tabla 53 se muestran las probabilidades de fallas de torres, mástiles, redes aéreas y antenas, causadas por cenizas volcánicas, estudiadas por el proyecto AELG-19.

Tabla 53. Volcán – Nube de Cenizas – Posible afectación de armarios, gabinetes y shelters - Proyecto AELG-19

Component	Risk Factors		Probability of Failure				Cause	Comments
Roadside Cabinets (landline)								
Unsealed	Connectors (e.g. IDC Krone-type connectors, especially disconnect type)	Moist or Wet ash	Medium	Low	Medium	Low-Medium	Shorting, corrosion	Probability increases if ash has high salt concentration (> 2%)
		Dry ash	Low	Low	Low	Low		

Fuentes. Review of Impacts of Volcanic Ash on Electricity Distribution Systems, Broadcasting and Communication Networks, Auckland Engineering Lifelines Group Project AELG-19, Auckland, NZ, APRIL 2009.

La Tabla 54 registra de manera agregada los posibles daños a armarios, gabinetes y shelters, ante los diferentes fenómenos volcánicos.

Tabla 54. Volcanes – Posibles daños a armarios, gabinetes y shelters

POSIBLES DAÑOS A ARMARIOS, GABINETES & SHELTERS				
	NUBE DE CENIZA (AFECTACION DE FUNCIONAMIENTO)	CAIDA DE CENIZA (AFECTACION POR PESO)	FLUJOS DE LAVA, MATERIAL PIROCLASTICO Y LODOS	CAIDA DE MATERIAL PIROCLASTICO Y PROYECTILES
Armarios, gabinetes & shelters	• Equipos de aire acondicionado y equipos de energía de respaldo: obstrucción en intercambiadores y entradas de aire y corrosión. • Equipo electrónico: contaminación interior del equipo, obstrucción de filtros, aumento de temperatura, cortos circuitos e incendio	Colapso (baja probabilidad)	Agrietamiento, desplazamiento de cimientos, incendio, enterramiento, arrastre, parcial o total, lo cual casusa destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, cortos circuitos e incendio	Agrietamiento, desplazamiento de cimientos, incendio, enterramiento, arrastre, parcial o total, lo cual casusa destrucción de equipos de telecomunicaciones y energía por desprendimiento, por aplastamiento, cortos circuitos e incendio

Fuente: CINTEL

5.3.3.7.3 Ante tsunamis

Tabla 55. Tsunami – Posibles daños a armarios, gabinetes y shelters

POSIBLES DAÑOS A ARMARIOS , GABINETES & SHELTERS			
	Fuerzas laterales provenientes de golpes de ola y licuación del terreno	Fuerzas laterales provenientes de corrientes de agua y material arrastrado	Inundación agua salobre:
Armarios, gabinetes & shelters	Agrietamiento, desplazamiento de cimientos, arrastre, enterramiento parcial o total, el cual causará destrucción por desprendimiento, por aplastamiento, arrastre , cortos circuitos y/o incendio, disrupción de red e inundaciones en su interior	Agrietamiento, desplazamiento de cimientos, arrastre, enterramiento parcial o total, el cual causará destrucción por desprendimiento, por aplastamiento, arrastre , cortos circuitos y/o incendio, disrupción de red e inundaciones en su interior	Malfuncionamiento en equipos de telecomunicaciones, periféricos y accesorios instados en su interior por anegación del equipo y cortos circuitos y daños residuales por contaminación salina.

Fuente: CINTEL

5.3.3.7.4 Ante inundaciones de agua dulce

Tabla 56. Inundaciones de agua dulce – Posibles daños a armarios, gabinetes & shelters

POSIBLES DAÑOS A ARMARIOS, GABINETES & SHELTERS POR INUNDACIONES DE AGUA DULCE	
	Posible daño
Armarios, gabinetes & shelters	Malfuncionamiento en equipos de telecomunicaciones, periféricos y accesorios instados en su interior por anegación del equipo y cortos circuitos.

Fuente: CINTEL

En las tablas Tabla 72, Tabla 73, Tabla 74 y Tabla 75 se registran los estimativos de vulnerabilidad física de las torres y antenas ante los diferentes eventos naturales tratados, según juicio de expertos sectoriales.

5.3.4 Redes aéreas de fibra óptica y de cobre

Las redes aéreas de fibra óptica y de cobre están soportadas mecánicamente en torres y en postes.

A continuación, se detallan los tipos de redes que se utilizan para la prestación de los diferentes servicios de telecomunicaciones considerados.

5.3.4.1 Servicio Portador

- Redes de fibra óptica: Como ya se mencionó, que hacen uso de las torres de alta, media y baja tensión del sector eléctrico mediante la utilización de cables OPGW (Optical Fiber Ground Wire), de cables ADSS (self supporting aerial fiber) o de posteria específicamente diseñada para su soporte.

5.3.4.2 Servicio de Telefonía Pública Básica Conmutada y acceso a INTERNET fijo

- Redes de cobre primaria y secundaria sobre postes, cuya utilización depende de las facilidades de utilización de ductos y de las reglamentaciones municipales[37] sobre la materia.

---

37 Se citan algunos artículos de la Resolución 33 de 2001 del Departamento Administrativo de Planeación Distrital que ilustran las restricciones que existen a nivel municipal sobre la utilización de redes aéreas:

ARTÍCULO 3. Las redes aéreas se podrán instalar en el espacio público, siempre y cuando su infraestructura cumpla con la normatividad existente en materia de uso del espacio público, con las especificaciones técnicas para la correcta prestación del servicio y con las correspondientes normas de seguridad.

5.3.4.3 Servicio de Televisión por Cable

Redes de fibra óptica de transporte y acceso y redes de coaxial de distribución sobre postes, cuya utilización depende de las facilidades de utilización de ductos y de las reglamentaciones municipales sobre la materia.

5.3.4.4 Resistencia y vulnerabilidad de las torres y postes

El servicio portador utiliza torres de transporte y distribución de energía eléctrica como soporte estructural a la fibra óptica (OPGW o ADSS), las cuales se diseñan e instalan cumpliendo, aún cuando no existe la obligación como ya se mencionó, con la norma colombiana NSR – 98 (actualmente NSR - 10) y la americana para estructuras de transmisión ASCE 10-97.

ARTÍCULO 4. En las zonas urbanas que cuentan con postería, se permitirá únicamente la instalación de elementos como seccionadores, elementos de maniobras, indicadores de falla, condensadores, refuerzos, sin que implique aumento del número de postes en el espacio público.

ARTICULO 5. En el espacio público de las zonas urbanas pertenecientes a los estratos 4, 5 Y 6, en el de las zonas de conservación histórica y en la malla vial arterial principal y complementaria, no se podrán instalar nuevos postes, ni armarios ni demás elementos que conformen las redes aéreas.

ARTÍCULO 19. Los programas para la subterranización de las redes de servicios públicos, ubicadas en el espacio público de la ciudad, se deberán desarrollar dentro de los siguientes parámetros:

1. Todas las empresas prestado ras de servicios públicos contarán con un plazo igual al de la vigencia del Plan de Ordenamiento Territorial para subterranizar el 35% del cableado sobre el Sistema Vial y sobre los componentes del Espacio Público Construido, meta que incluye el 100 % del cableado sobre la malla vial arterial principal y complementario. Para ello, deberán certificar ante el Departamento Administrativo de Planeación Distrital, a más tardar dentro de los 90 días siguientes a la entrada en vigencia de la presente resolución, la magnitud de todas y cada una de sus redes existentes.

2. Las empresas prestadoras de servicios públicos, están obligadas a subterranizar el cableado de las redes, propuesto dentro del programa de subterranización.

Para el soporte estructural de las redes aéreas locales de cobre o de fibra óptica, se utilizan postes cuyos materiales y métodos de instalación, profundidad y diámetro de los hoyos para su instalación están normalizados al interior de la mayoría de los operadores de telecomunicaciones[38]. Los postes utilizados son:

- Postes de madera seleccionada por su dureza, tiempo de vida útil, resistencia a esfuerzos, necesidad de tratamientos especiales, entre otros. Se utilizan en algunos sitios de muy difícil acceso.
- Postes metálicos telescópicos tubulares en secciones, que cumplan con la condición que el esfuerzo horizontal normal a la rotura no sea inferior a 310 Kg para cables de cobre (poste de 8 y 9 metros) y de 700 Kg (postes de 18 y 20 metros) para cables de fibra óptica.
- Postes de concreto armado, de forma de tronco cónico o tronco piramidal, de sección circular u octogonal, construidos en concreto armado de 3.500 psi (24,5 MPa) a los veintiocho días (28) de fraguado y varillas corrugadas de media pulgada (1/2") de diámetro con fy=60.000 psi (420 MPa).
- Los postes de concreto, además de cumplir lo especificado en la norma NTC 1329 (Prefabricados en concreto. Postes de concreto armado para líneas aéreas de energía y telecomunicaciones), deben soportar en la punta cargas de

38 Manual de construcción de redes telefónicas locales. Telecom. Enero de 2004; Postes para líneas aéreas de telecomunicaciones. Especificación Técnica No. 012-002, Octubre de 2001, Invitación Pública No. 10143388, Empresa de Telecomunicaciones de Bogotá, S.A., Abril de 2010; Fundación para postes de concreto. TEL NIN-009. Empresas Públicas de Medellín. Diciembre de 2004.

trabajo nominal de 5001,5 N, carga de rotura de 750 Kg (7355 N) o superior.

Tomando en consideración lo anterior, las torres y postes con relación a las diferentes amenazas naturales debieran entonces soportar el esfuerzo mecánico producido por los sismos tal como se referencia a continuación y, de manera análoga, debieran resistir otras amenazas materializadas como estrés mecánico a la estructura de las torres y postes.

5.3.4.4.1 Con relación a los sismos

- Temblores de poca intensidad sin daño.
- Temblores moderados con posibles cambios en la verticalidad.
- Un temblor fuerte con daños a elementos estructurales y no estructurales, con cambios notorios en la verticalidad y caída de torres y postes.

5.3.4.4.2 Con relación a los volcanes

- Caída de ceniza volcánica: La nube de ceniza volcánica, con relación a las torres tiene dos efectos básicos: el deterioro a mediano plazo que causa en los materiales de construcción y, el peso o presión que esta causa sobre la estructura de la torre cuando se acumula sobre éstas.
- Flujos de lava, material piroclástico y lodos: Es altamente probable que las torres, postes y redes aéreas soportadas en estas estructuras resulten destruidas, arrasadas, enterradas o con graves fallas estructurales, si están a su paso.
- Caída de material piroclástico y proyectiles: Es altamente probable que las torres, postes y redes aéreas soportadas en estas estructuras, ubicadas en las zonas de caída de este

material volcánico (piroclastos y proyectiles balísticos), resulten con daños estructurales y destruidos por incendio.

5.3.4.4.3 Con relación a los tsunamis

- Inundaciones ocasionales que no socaven los cimientos de la torre o del poste.
- Golpes de ola de poca intensidad sin daño.
- Golpes de ola moderados sin daño estructural, pero posiblemente con algún cambio en la verticalidad.
- Golpes de ola fuertes con daños a elementos estructurales y no estructurales con cambios notorios en la verticalidad y caída de torres y postes.
- Fuerzas leves laterales provenientes de corrientes de agua y material arrastrado sin daño.
- Fuerzas moderadas laterales provenientes de corrientes de agua y material arrastrado sin daño estructural, pero posiblemente con algún daño a los elementos no estructurales y algún cambio en la verticalidad.
- Fuerzas laterales fuertes provenientes de corrientes de agua y material arrastrado con daños a elementos estructurales y no estructurales con cambios notorios en la verticalidad y caída de torres y postes.

5.3.4.4.4 Con relación a las inundaciones de agua dulce

Inundaciones ocasionales que no generen deslizamientos.

5.3.4.5 Posibles daños de las torres, postes y redes aéreas soportadas ante eventos naturales

Con base en la resistencia de las torres y postes, tratada en el numeral 5.3.4.4 de este documento, se presentan las tablas de posibles daños a

torres, postes y redes aéreas de fibra óptica, coaxial y cobre según tipo de amenaza.

5.3.4.5.1 Ante eventos sísmicos

Tabla 57. Eventos sísmicos – Posibles daños a torres de transmisión eléctrica soporte de redes aéreas de telecomunicaciones

POSIBLES DAÑOS A TORRES DE TRANSMISION SOPORTE DE REDES AEREAS Supuesto: Las torres cumplen con las normas NSR98 y ASCE 10-97				
	Temblores de muy baja intensidad (Vibración)	Temblores de baja intensidad (Vibración)	Temblores de intensidad moderada (Vibración)	Temblores de alta intensidad (Vibración, fallas y grietas en la superficie terrestre, licuefacción)
Torres	Sin daño	Sin daño	Posibles cambios en la verticalidad	Daños a elementos estructurales y no estructurales, con cambios notorios en la verticalidad y caída de torres

Fuente: CINTEL

Tabla 58. Eventos sísmicos – Posibles daños a postes soporte de redes aéreas de telecomunicaciones

POSIBLES DAÑOS A POSTES SOPORTE DE REDES AEREAS Supuesto: Los postes cumplen con las normas NTC 1329, NSR98 y normas de operador				
	Temblores de muy baja intensidad (Vibración)	Temblores de baja intensidad (Vibración)	Temblores de intensidad moderada (Vibración)	Temblores de alta intensidad (Vibración, fallas y grietas en la superficie terrestre, licuefacción)
Postes	Sin daño	Sin daño	Posibles cambios en la verticalidad	Cambios notorios en la verticalidad y caída de postes

Fuente: CINTEL

Tabla 59. Eventos sísmicos – Posibles daños a redes aéreas de fibra óptica, coaxial y cobre

POSIBLES DAÑOS A REDES AEREAS DE FIBRA OPTICA, COAXIAL Y COBRE Supuesto: Redes instaladas según mejores prácticas				
	Temblores de muy baja intensidad (Vibración)	Temblores de baja intensidad (Vibración)	Temblores de intensidad moderada (Vibración)	Temblores de alta intensidad (Vibración, fallas y grietas en la superficie terrestre, licuefacción)
Antenas	Sin daño	Sin daño	Stress mecánico sin daño	Disrupción total o parcial de las redes aéreas por caida de la torre

Fuente: CINTEL

5.3.4.5.2 Ante volcanes

En la Tabla 44, numeral 5.3.2.14.2, se muestran las probabilidades de fallas de torres de telecomunicaciones, mástiles, **redes aéreas** y antenas, causadas por cenizas volcánicas y, en la Tabla 60 a continuación, se presentan las probabilidades de fallas de torres eléctricas y postes, causadas por cenizas volcánicas, estudiadas por el proyecto AELG-19.

Tabla 60. Volcán – Nube de Cenizas – Posible afectación de torres eléctricas y postes - Proyecto AELG-19

Component	Risk Factors		Probability of Failure				Cause	Comments
Substation insulators – high voltage (*large surface area and irregular shape*)								
Typically high voltage with large surface area and irregular shape		Moist or Wet ash	Medium	Low	High	Low-Medium	Flashover	Probability increases if ash has high salt concentration (> 2%)
Substation and electrical yards (*step/touch potential*)								
Ground ballast (substrate)		Moist or Wet ash	Medium	Low	Medium-High	Low-Medium	Resistivity of ground ballast reduced following ashfall and ash is moistened	Step/touch potential is significantly reduced when ash on the ground is damp and possible electrocution could result.
		Dry ash	Low	Low	Low	Low		
Towers/ Poles								
			Ash thickness 5-100mm		Ash thickness >100mm			
			Fine grained (<1 mm)	Coarse grained (>1 mm)	Fine grained (<1 mm)	Coarse grained (>1 mm)		
		Moist or Wet ash	Low-Medium	Low	Medium-high	Low	Collapse, buckling due to ash loading	
		Dry ash	Low	Low	Medium	Low	Collapse due to trees falling	

Fuente: Review of Impacts of Volcanic Ash on Electricity Distribution Systems, Broadcasting and Communication Networks, Auckland Engineering Lifelines Group Project AELG-19, Auckland, NZ, APRIL 2009.

Las tablas Tabla 61, Tabla 62 y Tabla 63, registran de manera agregada los posibles daños a torres, postes y redes aéreas de fibra óptica, coaxial y cobre, ante los diferentes fenómenos volcánicos.

Tabla 61. Volcanes – Posibles daños a torres eléctricas soporte de redes aéreas de telecomunicaciones

POSIBLES DAÑOS A TORRES ELECTRICAS SOPORTE DE REDES AEREAS DE TELECOMUNICACIONES				
	NUBE DE CENIZA (AFECTACION DE FUNCIONAMIENTO)	CAIDA DE CENIZA (AFECTACION POR PESO)	FLUJOS DE LAVA, MATERIAL PIROCLASTICO Y LODOS	CAIDA DE MATERIAL PIROCLASTICO Y PROYECTILES
Torres Eléctricas	Deterioro a mediano plazo por corrosión	Colapso (baja probabilidad)	Agrietamiento, desplazamiento de cimientos de la base de la torre, deformación, caida, arrastre, enterramiento parcial o total, incineración	Agrietamiento, desplazamiento de cimientos de la base de la torre, deformación, caida, enterramiento parcial o total, incineración

Fuente: CINTEL

Tabla 62. Volcanes – Posibles daños a postes soporte de redes aéreas de telecomunicaciones

POSIBLES DAÑOS A POSTES SOPORTE DE REDES AEREAS DE TELECOMUNICACIONES				
	NUBE DE CENIZA (AFECTACION DE FUNCIONAMIENTO)	CAIDA DE CENIZA (AFECTACION POR PESO)	FLUJOS DE LAVA, MATERIAL PIROCLASTICO Y LODOS	CAIDA DE MATERIAL PIROCLASTICO Y PROYECTILES
Postes			Agrietamiento, desplazamiento de cimientos de la base del poste, deformación, caida, arrastre, enterramiento parcial o total, incineración	Agrietamiento, desplazamiento de cimientos de la base del poste, deformación, caida, enterramiento parcial o total, incineración

Fuente: CINTEL

Tabla 63. Volcanes – Posibles daños a redes aéreas de fibra óptica, coaxial y cobre

POSIBLES DAÑOS A REDES AEREAS DE FIBRA OPTICA, COBRE Y COAXIAL				
	NUBE DE CENIZA (AFECTACION DE FUNCIONAMIENTO)	CAIDA DE CENIZA (AFECTACION POR PESO)	FLUJOS DE LAVA, MATERIAL PIROCLASTICO Y LODOS	CAIDA DE MATERIAL PIROCLASTICO Y PROYECTILES
Redes aéreas de fibra óptica, cobre y coaxial		Colapso (baja probabilidad)	Disrupción total o parcial de las redes aéreas por caida de las torres y postes	Disrupción total o parcial de las redes aéreas por caida de las torres y postes

Fuente: CINTEL

5.3.4.5.3 Ante tsunamis

Tabla 64. Tsunami – Posibles daños a torres eléctricas soporte de redes aéreas de telecomunicaciones

POSIBLES DAÑOS A TORRES ELECTRICAS SOPORTE DE REDES AEREAS DE TELECOMUNICACIONES			
	Fuerzas laterales provenientes de golpes de ola y licuación del terreno	Fuerzas laterales provenientes de corrientes de agua y material arrastrado	Inundación agua salobre:
Torres Eléctricas	Daños a elementos estructurales y no estructurales, con cambios notorios en la verticalidad y caída de torres	Daños a elementos estructurales y no estructurales, con cambios notorios en la verticalidad y caída de torres	Socavación de cimientos de la torre / Oxidación a mediano plazo de sus elementos estructurales

Fuente: CINTEL

Tabla 65. Tsunami – Posibles daños a postes soporte de redes aéreas de telecomunicaciones

POSIBLES DAÑOS A POSTES SOPORTE DE REDES AEREAS DE TELECOMUNICACIONES			
	Fuerzas laterales provenientes de golpes de ola y licuación del terreno	Fuerzas laterales provenientes de corrientes de agua y material arrastrado	Inundación agua salobre:
Postes	Cambios notorios en la verticalidad y caída de postes	Cambios notorios en la verticalidad y caída de postes	Socavación de cimientos del poste

Fuente: CINTEL

Tabla 66. Tsunami – Posibles daños a redes aéreas de fibra óptica, coaxial y cobre

POSIBLES DAÑOS A REDES AEREAS DE FIBRA OPTICA, COAXIAL Y COBRE			
	Fuerzas laterales provenientes de golpes de ola y licuación del terreno	Fuerzas laterales provenientes de corrientes de agua y material arrastrado	Inundación agua salobre:
Redes aéreas de fibra óptica, coaxial y cobre	Disrupción total o parcial de las redes aéreas por inlcinación o caida del poste	Disrupción total o parcial de las redes aéreas por inlcinación o caida del poste	Disrupción total o parcial de las redes aéreas por inlcinación o caida del poste

Fuente: CINTEL

5.3.4.5.4 Ante inundaciones de agua dulce

Tabla 67. Inundaciones de agua dulce – Posibles daños a torres, postes y redes aéreas de fibra óptica, coaxial y cobre

POSIBLES DAÑOS A TORRES, POSTES Y REDES AEREAS POR INUNDACIONES DE AGUA DULCE	
	Posible daño
Torres y postes	Socavación de cimientos
Redes aéreas de fibra óptica, coaxial y cobre	Disrupción total o parcial de las redes aéreas por inclinación o caida de torres y postes

Fuente: CINTEL

En las tablas Tabla 72, Tabla 73, Tabla 74 y Tabla 75 se registran los estimativos de vulnerabilidad física de las torres y antenas ante los diferentes eventos naturales tratados, según juicio de expertos sectoriales.

5.3.5 Redes Subterráneas de fibra óptica y de cobre

Las redes subterráneas de fibra óptica y de cobre se encuentran instaladas dentro de la infraestructura canalizada de red, la cual se compone en líneas generales de: ductos, cámaras de inspección, cajas de paso y demás instalaciones indispensables para alojar, soportar y proteger las redes de fibra óptica y cobre.

A continuación se detallan los tipos de redes que se utilizan para la prestación de los diferentes servicios de telecomunicaciones considerados.

Servicio Portador

Redes subterráneas de fibra óptica. Como ya se mencionó, el servicio portador a nivel nacional hace uso de la infraestructura eléctrica o instala la fibra óptica en ductos y canalizaciones subterráneas.

Servicio de Telefonía Pública Básica Conmutada e INTERNET fijo soportado en TPBCL - xDSL

Redes subterráneas de fibra óptica (troncal) y de cobre (primaria y secundaria).

Servicio de Telefonía Móvil Celular (GSM/UMTS) e INTERNET móvil soportado en GSM/UMTS

Redes subterráneas de fibra óptica (core de la red y conectividad BS/Nodos B con BSC en ambientes con disponibilidad de fibra óptica).

5.3.5.1 Resistencia y vulnerabilidad de la red canalizada

Las redes canalizadas (ductos, cámaras de inspección, cajas de paso y demás instalaciones indispensables) se encuentran especificadas

ampliamente por los diferentes operadores de telecomunicaciones que hacen uso de ellas[39] .

Con base en lo anterior, las redes subterráneas de fibra óptica y cobre con relación a las diferentes amenazas naturales debieran entonces soportar:

5.3.5.2 Con relación a los sismos

- Temblores de poca intensidad sin daño.
- Temblores moderados sin daño.
- Temblores fuertes con disrupción de redes.

5.3.5.3 Con relación a los volcanes

- Caída de ceniza volcánica, sin daño.
- Flujos de lava, material piroclástico y lodos: disrupción de redes, si están a su paso.
- Caída de material piroclástico y proyectiles, sin daño.

5.3.5.4 Con relación a los tsunamis

- Inundaciones sin daño en redes de fibra óptica y mal funcionamiento en redes de cobre.
- Golpes de ola de poca intensidad sin daño.
- Golpes de ola fuerte y licuación del terreno: disrupción de redes.

---

[39] Manual de construcción de redes telefónicas locales. Telecom. Enero de 2004; Términos de Referencia Invitación Pública No. 10143388 de 2010, Empresa de Telecomunicaciones de Bogotá, S.A.; Especificaciones Técnicas Construcción de redes telefónicas, UNE, 2009; Normas Técnicas Colombianas.

- Fuerzas leves laterales provenientes de corrientes de agua y material arrastrado sin daño.
- Fuerzas moderadas laterales provenientes de corrientes de agua y material arrastrado sin daño en redes de fibra óptica y mal funcionamiento en redes de cobre.
- Fuerzas laterales fuertes provenientes de corrientes de agua y material arrastrado con disrupción de redes.

5.3.5.5 Con relación a las inundaciones de agua dulce

Inundaciones ocasionales.

5.3.6 Posibles daños de las redes subterráneas de fibra óptica y cobre

5.3.6.1 Ante eventos sísmicos

Tabla 68. Eventos sísmicos – Posibles daños a redes subterráneas de fibra óptica y cobre

POSIBLES DAÑOS A REDES SUBTERRANEAS DE FIBRA OPTICA, COAXIAL Y COBRE Supuesto: Redes instaladas según mejores prácticas				
	Temblores de muy baja intensidad (Vibración)	Temblores de baja intensidad (Vibración)	Temblores de intensidad moderada (Vibración)	Temblores de alta intensidad (Vibración, fallas y grietas en la superficie terrestre, licuefacción)
Redes de Fibra Optica	Sin daño	Sin daño	Sin daño	Agrietamiento y desplazamiento de ductos, destrucción: ----> Redes expuestas, disrupción de redes
Redes de Cobre	Sin daño	Sin daño	Sin daño	Agrietamiento y desplazamiento de ductos, destrucción: ----> Redes expuestas, disrupción de redes

Fuente: CINTEL

5.3.6.2 Ante volcanes

Tabla 69. Volcán – Posibles daños a redes subterráneas de fibra óptica y cobre

POSIBLES DAÑOS A REDES SUBTERRANEAS DE FIBRA OPTICA, COBRE Y COAXIAL				
	NUBE DE CENIZA (AFECTACION DE FUNCIONAMIENTO)	CAIDA DE CENIZA (AFECTACION POR PESO)	FLUJOS DE LAVA, MATERIAL PIROCLASTICO Y LODOS	CAIDA DE MATERIAL PIROCLASTICO Y PROYECTILES
Redes subterráneas de fibra óptica, cobre y coaxial	Sin daño	Sin daño	Disrupción total o parcial de las redes por arrastre de canalizaciones y ductos	Sin daño

Fuente: CINTEL

5.3.6.3 Ante tsunamis

Tabla 70. Tsunami – Posibles daños a redes subterráneas de fibra óptica y cobre

POSIBLES DAÑOS A REDES SUBTERRANEAS DE FIBRA OPTICA, COAXIAL Y COBRE			
	Fuerzas laterales provenientes de golpes de ola y licuación del terreno	Fuerzas laterales provenientes de corrientes de agua y material arrastrado	Inundación agua salobre:
Redes subterráneas de fibra óptica, coaxial y cobre	Disrupción total o parcial de las redes	Disrupción total o parcial de las redes	Malfuncionamiento total o parcial de las redes de cobre

Fuente: CINTEL

5.3.6.4 Ante inundaciones de agua dulce

Tabla 71. Inundaciones de agua dulce – Posibles daños a redes subterráneas de fibra óptica y cobre

POSIBLES DAÑOS A REDES SUBTERRANEAS DE FIBRA OPTICA, COAXIAL Y COBRE	
	Posible daño
Redes subterráneas de fibra óptica, coaxial y cobre	Malfuncionamiento total o parcial de las redes de cobre

Fuente: CINTEL

En las tablas Tabla 72, Tabla 73, Tabla 74 y Tabla 75 se registran los estimativos de vulnerabilidad física de las redes aéreas de fibra óptica y cobre ante los diferentes eventos naturales tratados, según juicio de expertos sectoriales.

5.3.7 Estimativos de vulnerabilidad física de los diferentes elementos de las redes de telecomunicaciones según tipo de amenaza

A continuación, se presentan los estimativos de vulnerabilidad física de los diferentes elementos de redes, según tipo de amenaza.

Estos estimativos se hicieron en consulta con los operadores que participaron en el presente estudio y deben ser de permanente ajuste según las experiencias nacionales e internacionales.

Tabla 72. Vulnerabilidad física de redes de telecomunicaciones ante amenazas sísmicas

MATRIZ DE VULNERABILIDAD FISICA DE REDES DE TELECOMUNICACIONES ANTE AMENAZAS SISMICAS					
ELEMENTOS DE RED		MUY BAJA INTENSIDAD	BAJA INTENSIDAD	MODERADA INTENSIDAD	ALTA INTENSIDAD
EDIFICACIONES	Grandes Edificaciones	0%	Baja	Baja	Media
	Medianas, pequeñas edificaciones, cuartos de equipos	Baja	Baja	Media	Alta
	Equipos instalados en grandes edificaciones	0%	0%	Baja	Baja
	Equipos instalados en Medianas, pequeñas edificaciones, cuartos de equipos (Sitios de Tx)	0%	0%	Baja	Media
ARMARIOS / GABINETES / SHELTERS	Armarios	0%	0%	0%	Baja
	Gabinetes y Shelters	0%	0%	0%	Baja
TORRES	Torres	0%	0%	Baja	Baja
	Antenas	0%	0%	Baja	Baja
	Espectro Radioeléctrico (Medio de Tx)	0%	0%	0%	0%
REDES AEREAS	Postes y Torres	0%	0%	Baja	Baja
	Fibra Optica (Medio de Tx)	0%	0%	Baja	Baja
	Cobre (Medio de Tx)	0%	0%	Baja	Baja
REDES SUBTERRANEAS	Canalizaciones / Ductos	0%	0%	0%	Baja
	Fibra Optica (Medio de Tx)	0%	0%	0%	Baja
	Cobre (Medio de Tx)	0%	0%	0%	Baja

NOTA: Los estimativos han sido efectuados tomando en consideración máxima exposición y que el fenomeno ocurre

Fuente: CINTEL

Tabla 73. Vulnerabilidad física de redes de telecomunicaciones ante amenazas volcánicas

MATRIZ DE VULNERABILIDAD FISICA DE REDES DE TELECOMUNICACIONES ANTE AMENAZAS VOLCANICAS					
ELEMENTOS DE RED		NUBE DE CENIZA (AFECTACION DE FUNCIONAMIENTO)	CAIDA DE CENIZA (AFECTACION POR PESO)	FLUJOS DE LAVA, MATERIAL PIROCLASTICO Y LODOS	CAIDA DE MATERIAL PIROCLASTICO Y PROYECTILES
EDIFICACIONES	Grandes Edificaciones	0%	Baja	Alta	Alta
	Medianas, pequeñas edificaciones, cuartos de equipos	0%	Media	Alta	Alta
	Equipos instalados en grandes edificaciones	Baja	Baja	Alta	Alta
	Equipos instalados en Medianas, pequeñas edificaciones, cuartos de equipos (Sitios de Tx)	Baja	Media	Alta	Alta
ARMARIOS / GABINETES	Armarios	Media	0%	Alta	Alta
	Gabinetes y Shelters	Media	Baja	Alta	Alta
TORRES	Torres	0%	Baja	Alta	Alta
	Antenas	0%	Baja	Alta	Alta
	Espectro Radioeléctrico (Medio de Tx)	Baja	0%	0%	0%
REDES AEREAS	Postes y Torres	0%	Baja	Alta	Alta
	Fibra Optica (Medio de Tx)	0%	Baja	Alta	Alta
	Cobre (Medio de Tx)	0%	Baja	Alta	Alta
REDES SUBTERRANEAS	Canalizaciones / Ductos	0%	0%	Baja	0%
	Fibra Optica (Medio de Tx)	0%	0%	Baja	0%
	Cobre (Medio de Tx)	0%	0%	Baja	0%

NOTA: Los estimativos han sido efectuados tomando en consideración máxima exposición y que el fenomeno ocurre

Fuente: CINTEL

Tabla 74. Vulnerabilidad física de redes de telecomunicaciones ante amenaza de tsunami

MATRIZ DE VULNERABILIDAD FISICA DE REDES DE TELECOMUNICACIONES ANTE TSUNAMI

ELEMENTOS DE RED		FUERZAS LATERALES PROVENIENTES DE GOLPE DE OLA Y LICUACION DEL TERRENO	FUERZAS LATERALES PROVENIENTES DE CORRIENTES DE AGUA Y MATERIAL ARRASTRADO	INUNDACION AGUA SALOBRE
EDIFICACIONES	Grandes Edificaciones	Media	Media	Baja
	Medianas, pequeñas edificaciones, cuartos de equipos	Alta	Alta	Baja
	Equipos instalados en grandes edificaciones	Alta	Alta	Alta
	Equipos instalados en Medianas, pequeñas edificaciones, cuartos de equipos (Sitios de Tx)	Alta	Alta	Alta
ARMARIOS / GABINETES /	Armarios	Alta	Alta	Alta
	Gabinetes y Shelters	Alta	Alta	Alta
TORRES	Torres	Alta	Alta	Baja
	Antenas	Alta	Alta	0%
	Espectro Radioeléctrico (Medio de Tx)	0%	0%	0%
REDES AEREAS	Postes y Torres	Alta	Alta	Baja
	Fibra Optica (Medio de Tx)	Alta	Alta	0%
	Cobre (Medio de Tx)	Alta	Alta	0%
REDES SUBTERRANEAS	Canalizaciones / Ductos	Media	Media	Alta
	Fibra Optica (Medio de Tx)	Baja	Baja	Baja
	Cobre (Medio de Tx)	Media	Media	Alta

NOTA: Los estimativos han sido efectuados tomando en consideración máxima exposición y que el fenomeno ocurre

Fuente: CINTEL

Tabla 75. Vulnerabilidad física de redes de telecomunicaciones ante amenaza de inundación

MATRIZ DE VULNERABILIDAD FISICA DE REDES DE TELECOMUNICACIONES ANTE AMENAZA DE INUNDACION

ELEMENTOS DE RED		> a 20 cm (alto de un andén)
EDIFICACIONES	Grandes Edificaciones	Baja
	Medianas, pequeñas edificaciones, cuartos de equipos	Baja
	Equipos instalados en grandes edificaciones	Alta
	Equipos instalados en Medianas, pequeñas edificaciones, cuartos de equipos (Sitios de Tx)	Alta
ARMARIOS / GABINETES / SHELTERS	Armarios	Alta
	Gabinetes y Shelters	Alta
TORRES	Torres	Baja
	Antenas	0%
	Espectro Radioeléctrico (Medio de Tx)	0%
REDES AEREAS	Postes y Torres	Baja
	Fibra Optica (Medio de Tx)	0%
	Cobre (Medio de Tx)	0%
REDES SUBTERRANEAS	Canalizaciones / Ductos	Alta
	Fibra Optica (Medio de Tx)	Baja
	Cobre (Medio de Tx)	Alta

NOTA: Los estimativos han sido efectuados tomando en consideración máxima exposición y que el fenomeno ocurre

Fuente: CINTEL

5.4 VULNERABILIDAD FUNCIONAL DE LOS SERVICIOS DE TELECOMUNICACIONES VITALES

Es importante precisar, antes de analizar la vulnerabilidad funcional específica de cada uno de los servicios de telecomunicaciones considerados, dos factores de alta vulnerabilidad de estas redes:

- El suministro de energía eléctrica
- La congestión de redes

Con relación a la energía eléctrica, es importante puntualizar que ésta es a los equipos de telecomunicaciones como el oxígeno al ser humano, es decir que sin este importante fluido los equipos electrónicos de telecomunicaciones no podrán operar. El sector de las telecomunicaciones es totalmente dependiente del sector eléctrico en este sentido.

No obstante lo anterior, las instalaciones del sector de las telecomunicaciones han buscado blindarse al respecto utilizando diferentes sistemas de redundancia, así:

- Doble acometida eléctrica: mediante la doble acometida eléctrica proveniente de diferentes subestaciones se pretende tener una redundancia 1+1 con relación a la acometida, es decir que si un circuito falla el otro entra de manera automática. Esta solución se emplea en instalaciones de misión crítica como pueden ser los datacenters, los telepuertos o algunas instalaciones del core de las redes de telefonía móvil celular y telefonía pública básica conmutada, entre otros.
- Fuentes alternativas de energía: tales como plantas o grupos motogeneradores, los cuales entran en operación tan pronto falla el suministro de energía comercial. Estos grupos tienen previstos sus tanques de combustible, que dependiendo de su

capacidad pueden dar autonomía eléctrica desde unas pocas horas hasta varios días.

- UPS y baterías: La UPS y las baterías se utilizan para dar respaldo entre unos pocos minutos a algunas horas, y su objetivo básico es soportar los equipos de telecomunicaciones ante una falla del suministro de energía eléctrica, entretanto inicia la operación la planta o motogenerador.
- Sistemas de alimentación de energía eólica y solar: Estos sistemas de energías alternativas soportan la operación de las estaciones de telecomunicaciones cuando el suministro comercial presenta falla.

Tomando en consideración las conclusiones del estudio de Townsend &Moss[40] con relación a que una de las tres principales causas para que fallen las telecomunicaciones ante un evento natural desastroso es la disrupción del suministro de energía eléctrica, y que para este estudio no se analiza la vulnerabilidad de las redes eléctricas, se considerará para los efectos de éste que en las zonas bajo análisis habrá una alta probabilidad de disrupción del suministro de energía eléctrica, y que por lo tanto en la cadena de vulnerabilidad funcional de toda las redes se incluirá este factor, el cual se minimizará en función de los sistemas de energía de respaldo y de las horas de autonomía de los mismos.

40TELECOMMUNICATIONS INFRASTRUCTURE IN DISASTERS: Preparing Cities for Crisis Communications - By Anthony M. Townsend & Mitchell L. Moss -Center for Catastrophe Preparedness and Response & Robert F. Wagner Graduate School of Public Service New York University, April 2005

Con relación a la congestión de redes, la experiencia nacional permite claramente y sin lugar a dudas concluir que es altamente probable que ante un evento natural desastroso como los analizados en este estudio, se genere una congestión de las redes de telefonía móvil celular, TPBCL e INTERNET que se soporta sobre ellas, tal como ha ocurrido tradicionalmente en ocasiones como navidad, fin de año, día de la madre y en ocasiones de desastre ocurridas en Colombia.

A nivel internacional el estudio mencionado de Townsend & Moss de los últimos veinte años de eventos desastrosos incluye la congestión de red como uno de los tres factores de falla de los sistemas de telecomunicaciones, situación que claramente se dio en eventos recientes como el terremoto de China del 2008 donde 2.300 celdas de telefonía móvil celular de China Telecom quedaron fuera de servicio, entre otros, por congestión de red, o en el terremoto ocurrido a comienzos de 2010 en Chile, donde en algunas zonas la congestión impactó al 70% de la red.

Por lo tanto, en la cadena de vulnerabilidad funcional de las redes de telefonía móvil celular, telefonía pública básica conmutada e INTERNET, se considerará que en las zonas bajo análisis habrá una alta probabilidad de congestión y se incluirá este factor como factor de vulnerabilidad.

Con las anteriores precisiones, se presenta a continuación el resultado del análisis de vulnerabilidad funcional para cada uno de los servicios considerados. Para un mejor entendimiento de la vulnerabilidad funcional, se establecen los cruces respectivos con el libro de Excel: ***VULNERABILIDAD FÍSICA Y FUNCIONAL DE REDES DE TELECOMUNICACIONES***, que hace parte de este estudio.

5.4.1 Servicio Portador

En Colombia los servicios de telefonía pública básica conmutada, telefonía móvil celular, INTERNET y muchas redes privadas, utilizan dentro de sus redes los servicios de portador prestados por terceros, es decir, que estos servicios son altamente dependientes del servicio portador en sus diferentes niveles, local, regional, nacional e internacional.

Los demás servicios de telecomunicaciones utilizan marginalmente el servicio portador, ya que las capacidades de transporte básicamente están satisfechas con sus propios recursos de red y mediante la utilización de capacidad satelital de proveedores autorizados para este fin, tal como ocurre con los servicios radiodifundidos.

El servicio portador a nivel nacional, está estructurado sobre un gran backbone de fibra óptica, el cual se conecta por un “extremo” al mundo a través de nodos de salida internacional localizados en la costa Caribe y los cables submarinos de diferentes operadores.

Por el otro “extremo”, se conectan los diferentes usuarios del servicio portador, ya sea a nivel local, regional, nacional o internacional, para lo cual se utilizan nodos de agregación local, regional y nacional y diferentes medios de transporte tales como fibra óptica, microondas y/o satélite, según la ubicación del usuario con relación al backbone.

Tomando en consideración lo anterior, se modela la vulnerabilidad funcional del servicio portador para un municipio determinado, como una función de las vulnerabilidades físicas de los elementos de red comprometidos en la prestación del servicio portador al municipio objeto de estudio. La vulnerabilidad funcional del servicio portador para un municipio dado, en ese orden de ideas, será igual a la vulnerabilidad física del elemento con mayor

vulnerabilidad presente en la cadena de prestación del servicio portador al municipio de interés.

La vulnerabilidad funcional del servicio portador para un municipio dado, basado en las vulnerabilidades físicas de cada uno de los componentes es:

5.4.1.1 Nodo de servicio al municipio

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Equipos instalados en el nodo de servicio al municipio **(Fila 8, VFIS PORTADOR, VER Archivo Excel en CD)**
- Vulnerabilidad de la conectividad ante diferentes amenazas naturales:
    - Antenas y espectro radioeléctrico, si la conectividad entre el nodo de servicio municipal y el de agregación nacional es a través de microondas. **(Fila 11 y Fila 12, VFIS PORTADOR)**
    - Fibra óptica aérea[41], si la conectividad entre el nodo de servicio municipal y el nodo de agregación nacional es por fibra óptica. **(Fila 14, VFIS PORTADOR)**
    - Si la conectividad es de fibra óptica con backup de microondas, se toma la menor vulnerabilidad de los dos medios de transporte. **(Menor de (Fila 11 y Fila 12, VFIS PORTADOR) y (Fila 14, VFIS PORTADOR)).**
- La vulnerabilidad del nodo del servicio al municipio ante fallas del suministro de energía:

[41] **Se toma la vulnerabilidad de la fibra óptica aérea ya que esta representa el peor de los casos, ya que es más vulnerable a los eventos naturales tratados.**

- Si el nodo de servicio al municipio posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS PORTADOR)**
- Si el nodo de servicio al municipio posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS PORTADOR)**
- Si el nodo de servicio al municipio NO posee energía de respaldo, se considera de alta vulnerabilidad. **(Celda 8H, VFIS PORTADOR)**

- La vulnerabilidad del nodo del servicio al municipio ante aumento de uso (sobredemanda) causante de congestión, se considera baja. **(Celda 8E, VFIS PORTADOR)**

5.4.1.2 Nodo de agregación nacional

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Equipos instalados en el nodo de agregación nacional **(Fila 8, VFIS PORTADOR, VER Archivo Excel en CD).**
- Vulnerabilidad de la conectividad ante diferentes amenazas naturales:
  - Antenas y espectro radioeléctrico, si la conectividad entre el nodo de servicio municipal y el de agregación nacional es a través de microondas. **(Fila 11 y Fila 12, VFIS PORTADOR)**
  - Fibra óptica aérea[42], si la conectividad entre el nodo de servicio municipal y el nodo de agregación nacional es por fibra óptica. **(Fila 14, VFIS PORTADOR)**

[42] **Se toma la vulnerabilidad de la fibra óptica aérea ya que esta representa el peor de los casos, ya que es más vulnerable a los eventos naturales tratados.**

- Si la conectividad es de fibra óptica con backup de microondas, se toma la menor vulnerabilidad de los dos medios de transporte. **(Menor de (Fila 11 y Fila 12, VFIS PORTADOR) y (Fila 14, VFIS PORTADOR)).**

- La vulnerabilidad del nodo de agregación nacional ante fallas del suministro de energía
  - Si el nodo de agregación nacional posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS PORTADOR)**
  - Si el nodo de agregación nacional posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS PORTADOR)**
  - Si el nodo agregación nacional NO posee energía de respaldo, se considera de alta vulnerabilidad. **(Celda 8H, VFIS PORTADOR)**
- La vulnerabilidad del nodo de agregación nacional ante aumento de uso (sobredemanda) causante de congestión, se considera baja. **(Celda 8E, VFIS PORTADOR)**

5.4.1.3 Nodo de agregación alternativo

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Equipos instalados en el nodo de agregación alternativo **(Fila 8, VFIS PORTADOR, VER Archivo Excel en CD)**
- Vulnerabilidad de la conectividad ante diferentes amenazas naturales:
  - Antenas y espectro radioeléctrico, si la conectividad entre el nodo de servicio municipal y el de agregación alternativo es a través de microondas. **(Fila 11 y Fila 12, VFIS PORTADOR)**

- Fibra óptica aérea[43], si la conectividad entre el nodo de servicio municipal y el nodo de agregación alternativo es por fibra óptica. **(Fila 14, VFIS PORTADOR)**
- Si la conectividad es de fibra óptica con backup de microondas, se toma la menor vulnerabilidad de los dos medios de transporte. **(Menor de (Fila 11 y Fila 12, VFIS PORTADOR) y (Fila 14, VFIS PORTADOR)).**

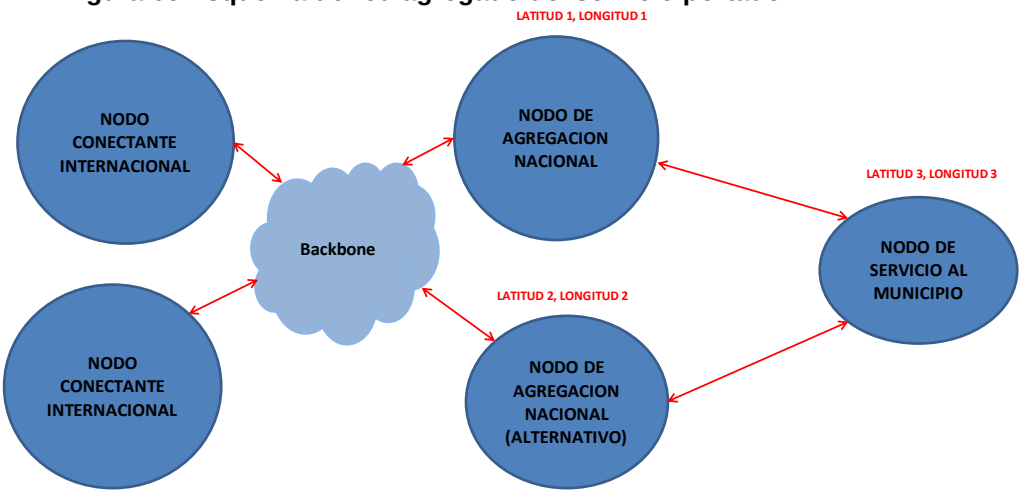
- La vulnerabilidad del nodo de agregación alternativo ante fallas del suministro de energía:
  - Si el nodo de servicio de agregación alternativo posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS PORTADOR)**
  - Si el nodo de agregación alternativo posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS PORTADOR)**
  - Si el nodo de agregación alternativo NO posee energía de respaldo, se considera de alta vulnerabilidad. **(Celda 8H, VFIS PORTADOR)**
- La vulnerabilidad del nodo de agregación alternativo ante aumento de uso (sobredemanda) causante de congestión, se considera baja. **(Celda 8E, VFIS PORTADOR)**

La vulnerabilidad funcional del servicio portador para un municipio determinado es equivalente a la mayor vulnerabilidad funcional de los tres (3) elementos tratados.

[43] **Se toma la vulnerabilidad de la fibra óptica aérea ya que esta representa el peor de los casos, ya que es más vulnerable a los eventos naturales tratados.**

La Figura 65 ilustra los componentes de red básicos considerados en el modelo para la vulnerabilidad funcional del servicio portador y la **Figura 66**permite ver las relaciones funcionales de manera desagregada.

Figura 65 Esquema de red agregado del servicio portador

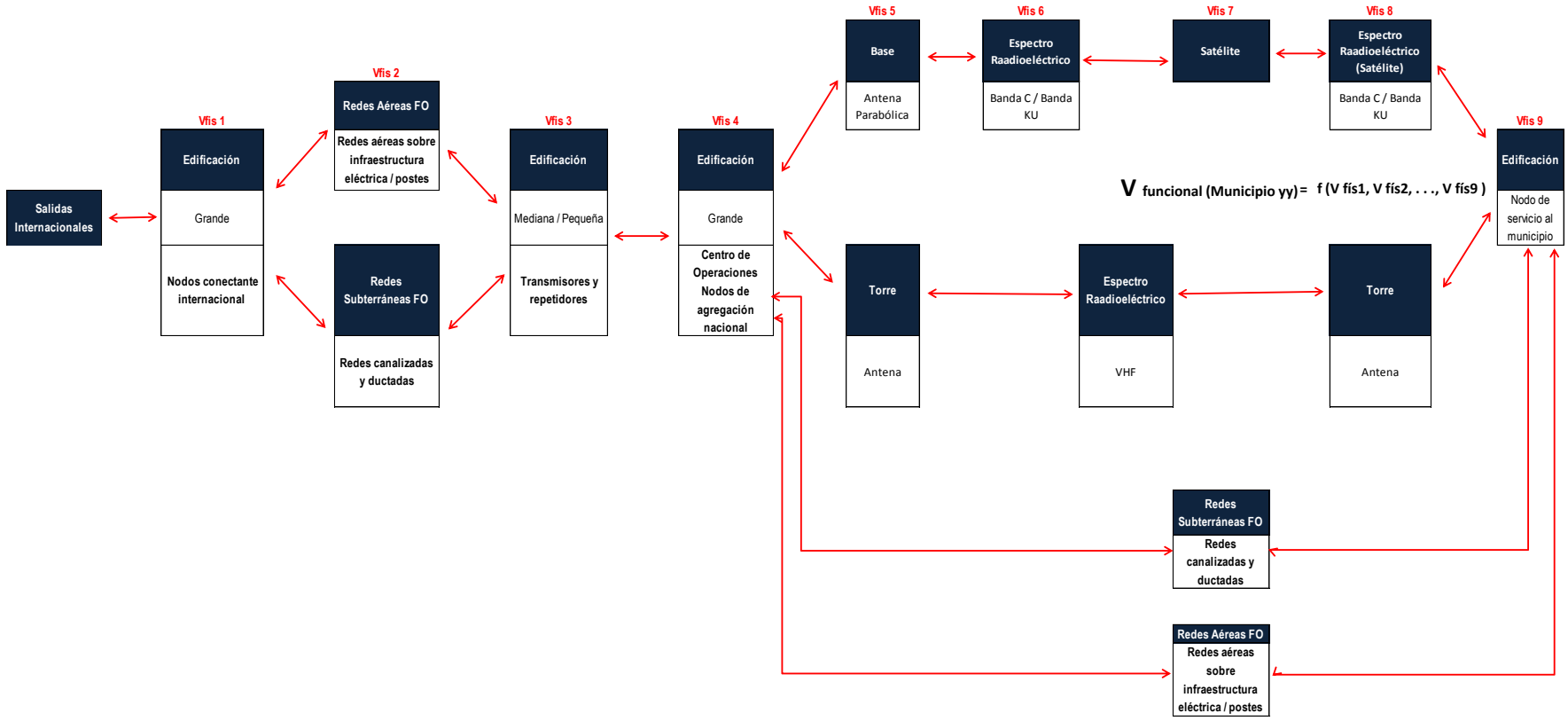


NOTA 1: Ultimas millas y equipos en los sitios de usuarios no cubiertos por este estudio
NOTA 2: Backbone, nodos conectantes internacionales y salidas internacionales no cubiertas por este estudio

Fuente: CINTEL

Figura 66. Esquema funcional general del servicio portador

La vulnerabilidad física (V fís) de cada componente de red se estima con base en la resistencia estimada del componente, la amenaza a la cual está expuesto y en la experiencia de fenómenos similares.



Fuente: CINTEL

5.4.2 Servicio de Telefonía Pública Básica Conmutada e INTERNET fijo xDSL

Es el servicio básico de telecomunicaciones cuyo objeto es la transmisión conmutada de voz a través de la Red Telefónica Pública Conmutada (RTPC)[44], con acceso generalizado al público.

Este servicio basa su prestación en las centrales de conmutación - softswitch y para la prestación de los servicios de acceso a INTERNET fijo xDSL (el de mayor penetración) en los DSLAM, que normalmente se encuentran instalados en una gran edificación y se conectan por un lado a través de la red troncal, primordialmente a través de redes de fibra óptica propias o de operadores de servicio portador, con otras centrales de su red y con otros operadores de telecomunicaciones (TPBCL, telefonía móvil celular e INTERNET).

Las centrales de conmutación, por otro lado se conectan a los armarios a través de la red primaria (normalmente en cobre) y de los armarios a través de red secundaria (normalmente en cobre) y de dispersión se presta el servicio a los abonados. Las redes de cobre son tanto aéreas sobre postes, como subterráneas en ductos; en muchas ciudades de Colombia por políticas de planeación municipal, las redes aéreas se están subterranizando y se está limitando la instalación de nuevas redes aéreas dentro de las ciudades.

---

[44]RTPC es el conjunto de elementos que hacen posible la transmisión conmutada de voz, con acceso generalizado al público, tanto en Colombia como en el exterior. Incluye las redes de los operadores de TPBCL, TPBCLE, TMR y TPBCLD. Fuente: Resolución 87 - CRC

La vulnerabilidad funcional del servicio de telefonía pública básica conmutada e INTERNET fijo para un municipio específico, se modela en función de los elementos básicos utilizados para la prestación de este servicio. La vulnerabilidad funcional de este servicio para un grupo de abonados conectados a un armario específico, será igual a la vulnerabilidad del elemento con mayor vulnerabilidad física presente en la cadena de prestación del servicio de telefonía pública básica conmutada conexa al armario de interés.[45]

La vulnerabilidad funcional del servicio de telefonía pública básica conmutada e INTERNET fijo xDSL para un armario que tiene conectado un número dado de abonados, de un municipio específico, basado en las vulnerabilidades físicas de cada uno de los componentes, es:

5.4.2.1 Sistema de conmutación mediante el cual se presta el servicio al municipio

- Vulnerabilidad de equipos ante diferentes amenazas naturales:
  - Equipos instalados en grandes edificaciones: Centrales de Conmutación, Softswitch, DSLAM **(Fila 8, VFIS TPBCL, VER Archivo Excel en CD).**
  - Equipos instalados en pequeñas edificaciones: Si el servicio se presta a través de concentradores, estaciones base de telefonía inalámbrica (BS WLL wireless local loop), multiacceso alambrado, PCM, VSAT y nodos WI MAX **(Fila 9, VFIS TPBCL)**

[45]**Esta descripción del servicio de TPBCL es típica y sobre esta se desarrolla el modelo; sin embargo en este se prevé el uso de softswitch, concentradores y redes WILL (wireless local loop).**

- Vulnerabilidad de la conectividad (Red Primaria), ante diferentes amenazas naturales:
    - Antenas y espectro radioeléctrico, en el caso soluciones inalámbricas (WLL), en el que se utiliza un enlace de microondas para conectar la central de conmutación con la estación base (BS) de WLL. **(Fila 13 y Fila 14, VFIS TPBCL)**
    - Fibra óptica subterránea, en el caso soluciones inalámbricas (WLL), en el que se utiliza un enlace de fibra óptica para conectar la central de conmutación con la estación base (BS) de WLL. **(Fila 18, VFIS TPBCL)**
    - Si la conectividad con la estación base de WLL es de fibra óptica con backup de microondas, se toma la menor vulnerabilidad de los dos medios de transporte. **(Menor de (Fila 13y Fila 14, VFIS TPBCL) y (Fila 18, VFIS TPBCL).**
    - Si la conectividad es por par trenzado, indicativo de coubicación dela BS de WLL con la central de conmutación, no se considera ninguna vulnerabilidad adicional, ya que esta conectividad se toma en cuenta en la vulnerabilidad de equipos instalados.
    - Redes Subterráneas de Cobre, soluciones alámbricas típicas, correspondiente a la red primaria para conexión de la central de conmutación a los armarios. **(Fila 19, VFIS TPBCL)**
- Vulnerabilidad de la conectividad (Red Troncal) con elemento de orden superior, ante diferentes amenazas naturales:
    - Antenas y espectro radioeléctrico, en el caso de que se utilice un enlace de microondas para conectar el sistema de conmutación mediante el cual se presta el servicio al municipio con el elemento de orden superior

(Normalmente cuando se utilizan concentradores). **(Fila 13 y Fila 14, VFIS TPBCL, VER Archivo Excel en CD)**

- Fibra óptica subterránea, para conectar el sistema de conmutación mediante el cual se presta el servicio al municipio con el elemento de orden superior (Normalmente cuando se utilizan centrales de conmutación). **(Fila 18, VFIS TPBCL)**
- Si la conectividad entre el sistema de conmutación mediante el cual se presta el servicio al municipio con el elemento de orden superior, es de fibra óptica con backup de microondas, se toma la menor vulnerabilidad de los dos medios de transporte. **(Menor de (Fila 13y Fila 14, VFIS TPBCL) y (Fila 18, VFIS TPBCL).**

- La vulnerabilidad del sistema de conmutación ante fallas del suministro de energía
  - Si el sistema de conmutación (central de conmutación, softswitch o concentrador remoto) posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS TPBCL, para centrales de conmutación; Celda 9F, VFIS TPBCL, para concentradores, VER Archivo Excel en CD)**
  - Si el sistema de conmutación (central de conmutación, softswitch o concentrador remoto) posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS TPBCL, para centrales de conmutación; Celda 9G, VFIS TPBCL, para concentradores)**
  - Si el sistema de conmutación (central de conmutación, softswitch o concentrador remoto) NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS TPBCL, para centrales**

de conmutación; Celda 9H, VFIS TPBCL, para concentradores)

- La vulnerabilidad del sistema de conmutación (central de conmutación, softswitch o concentrador remoto) ante aumento de uso (sobredemanda) causante de congestión, se considera alta. **(Celda 8E, VFIS TPBCL)**

5.4.2.2 Elemento de orden superior

- Vulnerabilidad de equipos ante diferentes amenazas naturales:
  - Equipos instalados en grandes edificaciones: Centrales de Conmutación, Softswitch **(Fila 8, VFIS TPBCL).**
- Vulnerabilidad de la conectividad (Red Troncal), ante diferentes amenazas naturales:
  - Antenas y espectro radioeléctrico, en el caso de que se utilice un enlace de microondas para conectar el elemento de orden superior con el sistema de conmutación mediante el cual se presta el servicio al municipio (Normalmente cuando se utilizan concentradores). **(Fila 13 y Fila 14, VFIS TPBCL)**
  - Fibra óptica subterránea, para conectar el elemento de orden superior con el sistema de conmutación mediante el cual se presta el servicio al municipio (Normalmente cuando se utilizan centrales de conmutación). **(Fila 18, VFIS TPBCL)**
  - Si la conectividad entre el elemento de orden superior y el sistema de conmutación mediante el cual se presta el servicio al municipio, es de fibra óptica con backup de microondas, se toma la menor vulnerabilidad de los dos medios de transporte. **(Menor de (Fila 13y Fila 14, VFIS TPBCL) y (Fila 18, VFIS TPBCL).**

- La vulnerabilidad del elemento de orden superior ante fallas del suministro de energía
    - Si el elemento de orden superior posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS TPBCL)**
    - Si el elemento de orden superior posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS TPBCL)**
    - Si el elemento de orden superior NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS TPBCL)**
- La vulnerabilidad del elemento de orden superior ante aumento de uso (sobredemanda) causante de congestión, se considera alta.**(Celda 8E, VFIS TPBCL)**

5.4.2.3 Elemento de orden superior alternativo

- Vulnerabilidad de equipos ante diferentes amenazas naturales:
    - Equipos instalados en grandes edificaciones: Centrales de Conmutación, Softswitch **(Fila 8, VFIS TPBCL).**
- Vulnerabilidad de la conectividad (Red Troncal), ante diferentes amenazas naturales:
    - Antenas y espectro radioeléctrico, en el caso de que se utilice un enlace de microondas para conectar el elemento de orden superior alternativo con el sistema de conmutación mediante el cual se presta el servicio al municipio (Normalmente cuando se utilizan concentradores). **(Fila 13 y Fila 14, VFIS TPBCL)**
    - Fibra óptica subterránea, para conectar el elemento de orden superior alternativo con el sistema de conmutación

mediante el cual se presta el servicio al municipio (Normalmente cuando se utilizan centrales de conmutación). **(Fila 18, VFIS TPBCL)**

- Si la conectividad entre el elemento de orden superior alternativo y el sistema de conmutación mediante el cual se presta el servicio al municipio, es de fibra óptica con backup de microondas, se toma la menor vulnerabilidad de los dos medios de transporte. **(Menor de (Fila 13y Fila 14, VFIS TPBCL) y (Fila 18, VFIS TPBCL).**

- La vulnerabilidad del elemento de orden superior alternativo ante fallas del suministro de energía
  - Si el elemento de orden superior alternativo posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS TPBCL)**
  - Si el elemento de orden superior alternativo posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS TPBCL)**
  - Si el elemento de orden superior alternativo NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS TPBCL)**
- La vulnerabilidad del elemento de orden superior alternativo ante aumento de uso (sobredemanda) causante de congestión, se considera alta.**(Celda 8E, VFIS TPBCL)**

5.4.2.4 Armario

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Armario **(Fila 10, VFIS TPBCL)**
- Vulnerabilidad de la conectividad (Red Primaria), ante diferentes amenazas naturales: Redes Subterráneas de Cobre,

soluciones alámbricas típicas, correspondiente a la red primaria para conexión de la central de conmutación a los armarios. **(Fila 19, VFIS TPBCL)**

- Vulnerabilidad de la conectividad (Red Secundaria), ante diferentes amenazas naturales: Redes Aéreas de Cobre y Redes Subterráneas de Cobre, del armario hacia el abonado. **(Mayor valor entre Fila 16 y Fila 19, VFIS TPBCL).**

5.4.2.5 BS de WLL

- Vulnerabilidad de equipos ante diferentes amenazas naturales:
  - BS instalados en gabinetes /shelters en pequeñas edificaciones **(Fila 9, VFIS TPBCL)**
- Vulnerabilidad de la conectividad ante diferentes amenazas naturales:
  - Antenas y espectro radioeléctrico, en el caso que se utilice un enlace de microondas para conectar la estación base (BS) de WLL con la central de conmutación. **(Fila 13 y Fila 14, VFIS TPBCL)**
  - Fibra óptica subterránea, en el caso que se utilice un enlace de fibra óptica para conectar la estación base (BS) de WLL con la central de conmutación. **(Fila 18, VFIS TPBCL)**
  - Si la conectividad con la estación base de WLL es de fibra óptica con backup de microondas, se toma la menor vulnerabilidad de los dos medios de transporte. **(Menor de (Fila 13y Fila 14, VFIS TPBCL) y (Fila 18, VFIS TPBCL).**
  - Si la conectividad es por par trenzado, indicativo de coubicación dela BS de WLL con la central de conmutación, no se considera ninguna vulnerabilidad

adicional, ya que esta conectividad se toma en cuenta en la vulnerabilidad de equipos instalados.

- La vulnerabilidad de la cobertura de las BS de WLL ante diferentes amenazas naturales. Antenas y espectro radioeléctrico**. (Fila 13 y Fila 14, VFIS TPBCL)**
- La vulnerabilidad de las BS de WLL ante fallas del suministro de energía
    - Si la BS de WLL posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 9F, VFIS TPBCL)**
    - Si la BS de WLL posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 9G, VFIS TPBCL)**
    - Si la BS de WLL NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 9H, VFIS TPBCL)**
- La vulnerabilidad de la BS de WLL ante aumento de uso (sobredemanda) causante de congestión, se considera alta. **(Celda 9E, VFIS TPBCL)**

La vulnerabilidad funcional del servicio de telefonía pública básica conmutada e INTERNET fijo xDSL de un armario dado que presta servicio a un grupo de abonados determinado en un municipio, es equivalente a la mayor vulnerabilidad funcional de los elementos tratados según la tecnología utilizada, así:

Para soluciones alámbricas tradicionales:

- Elemento de orden superior
- Elemento de orden superior alternativo

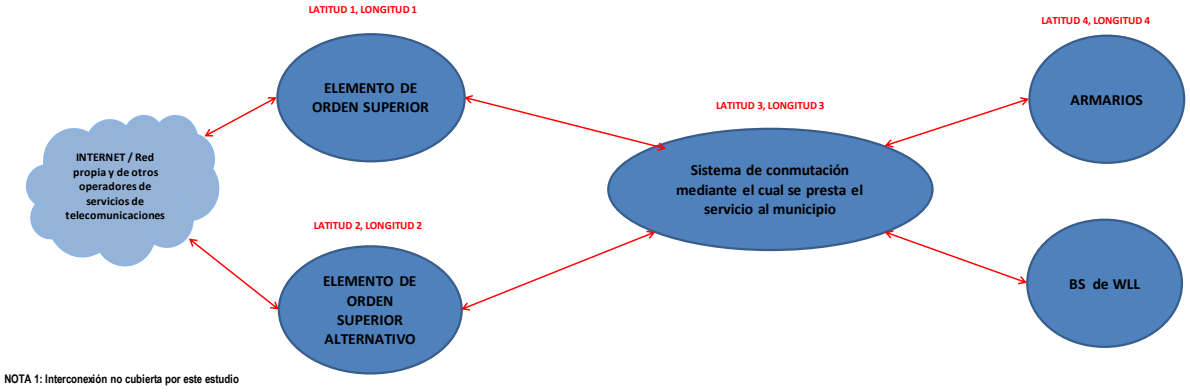
- Sistema de Conmutación mediante el cual se presta el servicio al municipio
- Armario

Para soluciones WLL:

- Elemento de orden superior
- Elemento de orden superior alternativo
- Sistema de Conmutación mediante el cual se presta el servicio al municipio
- BS de WLL

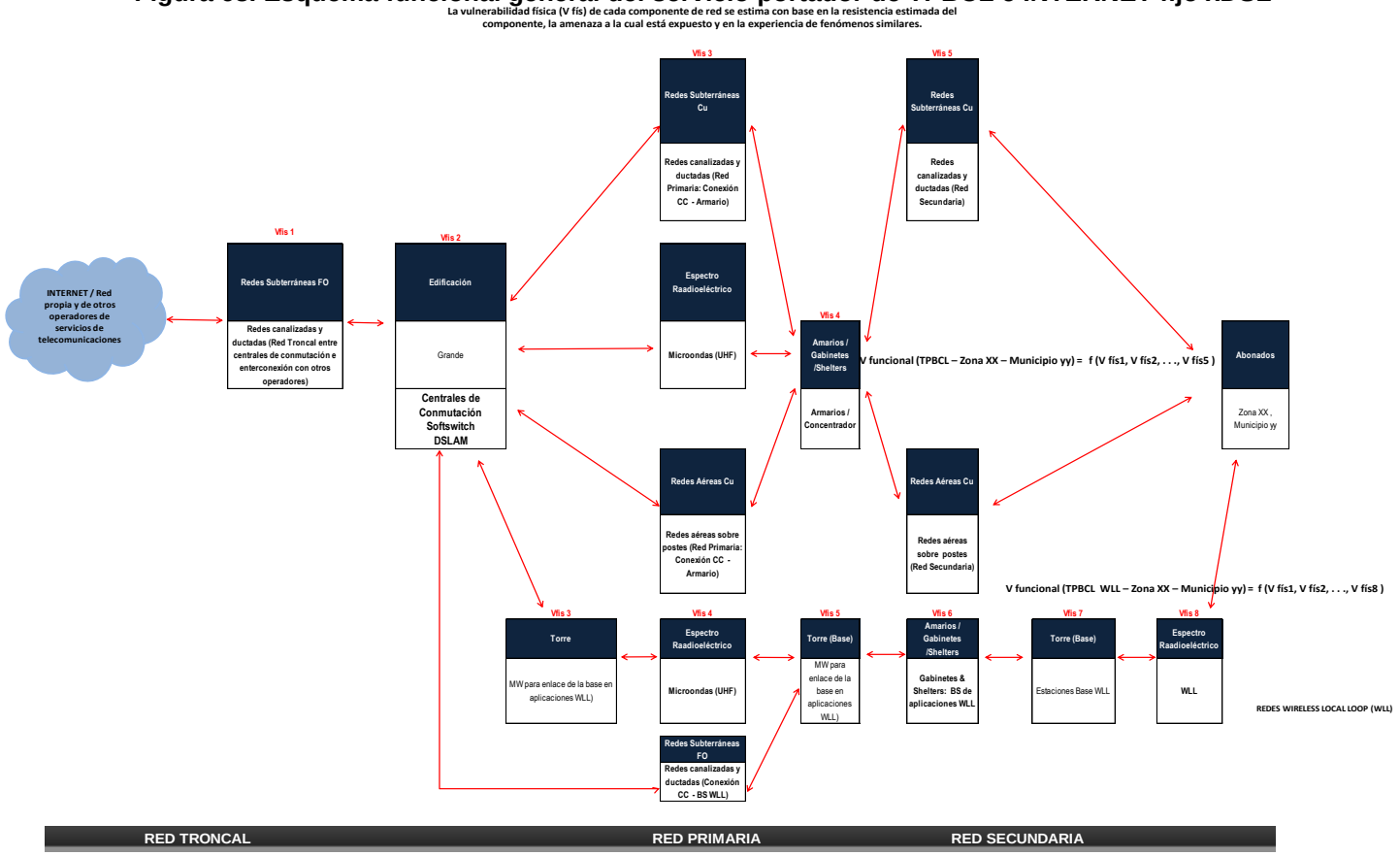
La Figura 67 ilustra los componentes de red básicos considerados en el modelo para la vulnerabilidad funcional del servicio de telefonía pública básica conmutada e INTERNET fijo xDSL y la Figura 68 permite ver las relaciones funcionales de manera desagregada.

Figura 67. Esquema de red agregado del servicio de TPBCL e INTERNET fijo xDSL



Fuente: CINTEL

Figura 68. Esquema funcional general del servicio portador de TPBCL e INTERNET fijo xDSL



Fuente: CINTEL

5.4.3 Servicio de Telefonía Móvil Celular (GSM & UMTS) e INTERNET móvil

El servicio de telefonía móvil celular está definido, como ya se mencionó, como un servicio público de telecomunicaciones, no domiciliario, de ámbito y cubrimiento nacional, que proporciona en sí mismo capacidad completa para la comunicación telefónica entre usuarios móviles y, a través de la interconexión con la red telefónica pública conmutada (RTPC), entre aquellos y usuarios fijos, haciendo uso de una red de telefonía móvil celular, en la que la parte del espectro radioeléctrico asignado constituye su elemento principal.

Este servicio, en la sociedad moderna se destaca como el de mayor penetración, y permite a sus usuarios la ubicuidad y la interacción a través de voz, datos y video.

Este servicio basa su prestación en las centrales de conmutación móvil (MSC) - BSC - softswitch y para la prestación de los servicios de acceso a INTERNET móvil en los nodos SGSN (Service GPRS SupportNode) y GGSN (Gateway GPRS SupportNode), que normalmente se encuentran instalados en una gran edificación. Éstos se conectan por un lado a través de la red troncal, primordialmente a través de redes de fibra óptica propias o de operadores de servicio portador con otros operadores de telecomunicaciones (TPBCL, telefonía móvil celular e INTERNET).

La MSC se conecta al BSC y este a su vez a las estaciones base y nodos B a través de enlaces de microondas o enlaces de fibra óptica o utiliza los dos medios para redundancia y vía el espectro radioeléctrico (banda de 900 MHz y 1900 MHz) entregado en concesión por el Ministerio TIC, se llega desde las estaciones base y los nodos B al abonado.

Con base en lo anterior, la vulnerabilidad funcional del servicio de telefonía móvil celular e INTERNET móvil para una celda dada que presta servicio a un municipio específico, se modela en función de los elementos básicos utilizados para la prestación de este servicio. La vulnerabilidad funcional de este servicio para una celda determinada, será igual a la vulnerabilidad del elemento con mayor vulnerabilidad física presente en la cadena de prestación del servicio de telefonía móvil celular a la celda de interés.

La vulnerabilidad funcional del servicio de telefonía móvil celular para una celda específica de un municipio dado, basado en las vulnerabilidades físicas de cada uno de los componentes, es:

5.4.3.1 MSC

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Equipos instalados en el MSC **(Fila 8, VFIS TELEFONÍA MÓVIL, VER Archivo Excel en CD)**
- Vulnerabilidad de la conectividad ante diferentes amenazas naturales:
    - Antenas y espectro radioeléctrico, si la conectividad entre el MSC y el BSC es a través de microondas. **(Fila 12 y Fila 13, VFIS TELEFONÍA MÓVIL)**
    - Fibra óptica subterránea[46], si la conectividad entre el MSC y BSC es por fibra óptica. **(Fila 15, VFIS TELEFONÍA MÓVIL)**
    - Si la conectividad es de fibra óptica con backup de microondas, se toma la menor vulnerabilidad de los dos

[46] **Se toma la vulnerabilidad de la fibra óptica subterránea ya la MSC y el BSC normalmente están en ambientes urbanos.**

medios de transporte. **(Menor de (Fila 12y Fila 13, VFIS TELEFONÍA MÓVIL) y (Fila 15, VFIS TELEFONÍA MÓVIL).**

- Si la conectividad es por par trenzado, indicativo de coubicación del MSC y BSC, no se considera ninguna vulnerabilidad adicional, ya que esta conectividad se toma en cuenta en la vulnerabilidad de equipos instalados en la MSC.

- La vulnerabilidad del MSC ante fallas del suministro de energía
  - Si el MSC posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS TELEFONÍA MÓVIL)**
  - Si el MSC posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS TELEFONÍA MÓVIL)**
  - Si el MSC NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS TELEFONÍA MÓVIL)**
- La vulnerabilidad del MSC ante aumento de uso (sobredemanda) causante de congestión, se considera baja. **(Celda 8E, VFIS TELEFONÍA MÓVIL)**

5.4.3.2 BSC

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Equipos instalados en el BSC **(Fila 8, VFIS TELEFONÍA MÓVIL, VER Archivo Excel en CD)**
- Vulnerabilidad de la conectividad ante diferentes amenazas naturales:
  - Antenas y espectro radioeléctrico, si la conectividad entre el BSC y el MSC es a través de microondas. **(Fila 12 y Fila 13, VFIS TELEFONÍA MÓVIL)**

- Fibra óptica subterránea[47], si la conectividad entre el BSC y MSC es por fibra óptica. **(Fila 15, VFIS TELEFONÍA MÓVIL)**
- Si la conectividad es de fibra óptica con backup de microondas, se toma la menor vulnerabilidad de los dos medios de transporte. **(Menor de (Fila 12y Fila 13, VFIS TELEFONÍA MÓVIL) y (Fila 15, VFIS TELEFONÍA MÓVIL).**
- Si la conectividad es por par trenzado, indicativo de coubicación del BSC y MSC, no se considera ninguna vulnerabilidad adicional, ya que esta conectividad se toma en cuenta en la vulnerabilidad de equipos instalados en la MSC.

- La vulnerabilidad del BSC ante fallas del suministro de energía
  - Si el BSC posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS TELEFONÍA MÓVIL)**
  - Si el BSC posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS TELEFONÍA MÓVIL)**
  - Si el BSC NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS TELEFONÍA MÓVIL)**
- La vulnerabilidad del BSC ante aumento de uso (sobredemanda) causante de congestión, se considera baja. **(Celda 8E, VFIS TELEFONÍA MÓVIL)**

---

[47] **Se toma la vulnerabilidad de la fibra óptica subterránea ya la MSC y el BSC normalmente están en ambientes urbanos.**

5.4.3.3 BS / NODOS B

- Vulnerabilidad de equipos ante diferentes amenazas naturales:
  - BS instalados en gabinetes /shelters en pequeñas edificaciones[48] **(Fila 9, VFIS TELEFONÍA MÓVIL, VER Archivo Excel en CD)**
  - BS instalados en gabinetes /shelters al aire libre **(Fila 10, VFIS TELEFONÍA MÓVIL)**
- Vulnerabilidad de la conectividad ante diferentes amenazas naturales:
  - Antenas y espectro radioeléctrico, si la conectividad entre la BS/NODO B y el BSC es a través de microondas. **(Fila 12 y Fila 13, VFIS TELEFONÍA MÓVIL)**
  - Fibra óptica subterránea[49], si la conectividad entre la BS/NODO B y el BSC es por fibra óptica. **(Fila 15, VFIS TELEFONÍA MÓVIL)**
  - Si la conectividad es de fibra óptica con backup de microondas, se toma la menor vulnerabilidad de los dos medios de transporte. **(Menor de (Fila 12y Fila 13, VFIS TELEFONÍA MÓVIL) y (Fila 15, VFIS TELEFONÍA MÓVIL).**
- La vulnerabilidad de la cobertura de las BS / NODO B ante diferentes amenazas naturales. Antenas y espectro radioeléctrico**. (Fila 12 y Fila 13, VFIS TELEFONÍA MÓVIL)**

---

[48]Se considera que la vulnerabilidad física de gabinetes y shelters instalados en pequeñas edificaciones construidas sin apego a normas antisísmicas es mayor que la de los instalados al aire libre.

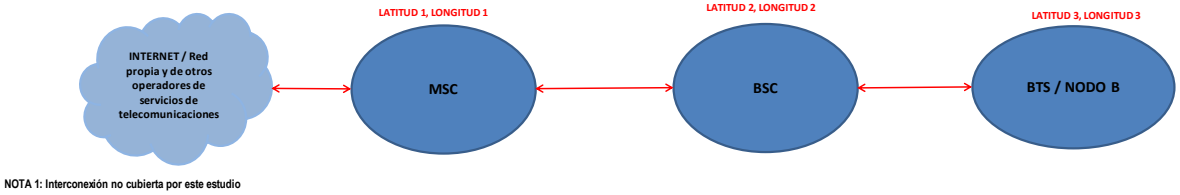
[49] Se toma la vulnerabilidad de la fibra óptica subterránea ya que la conectividad por fibra óptica normalmente es en ambientes urbanos y esta es subterránea.

- La vulnerabilidad de las BS / NODOS B ante fallas del suministro de energía
    - Si la BS / NODO B posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 9F, VFIS TELEFONÍA MÓVIL)**
    - Si la BS / NODO B posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 9G, VFIS TELEFONÍA MÓVIL)**
    - Si la BS / NODO B NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 9H, VFIS TELEFONÍA MÓVIL)**
- La vulnerabilidad de la BS / NODO B ante aumento de uso (sobredemanda) causante de congestión, se considera alta. **(Celda 9E, VFIS TELEFONÍA MÓVIL)**

La vulnerabilidad funcional del servicio de telefonía móvil celular para una celda específica de un municipio dado, que afecta un área (Km^2), es equivalente a la mayor vulnerabilidad funcional de los tres (3) elementos tratados (MSC, BSC y BS/NODO B).

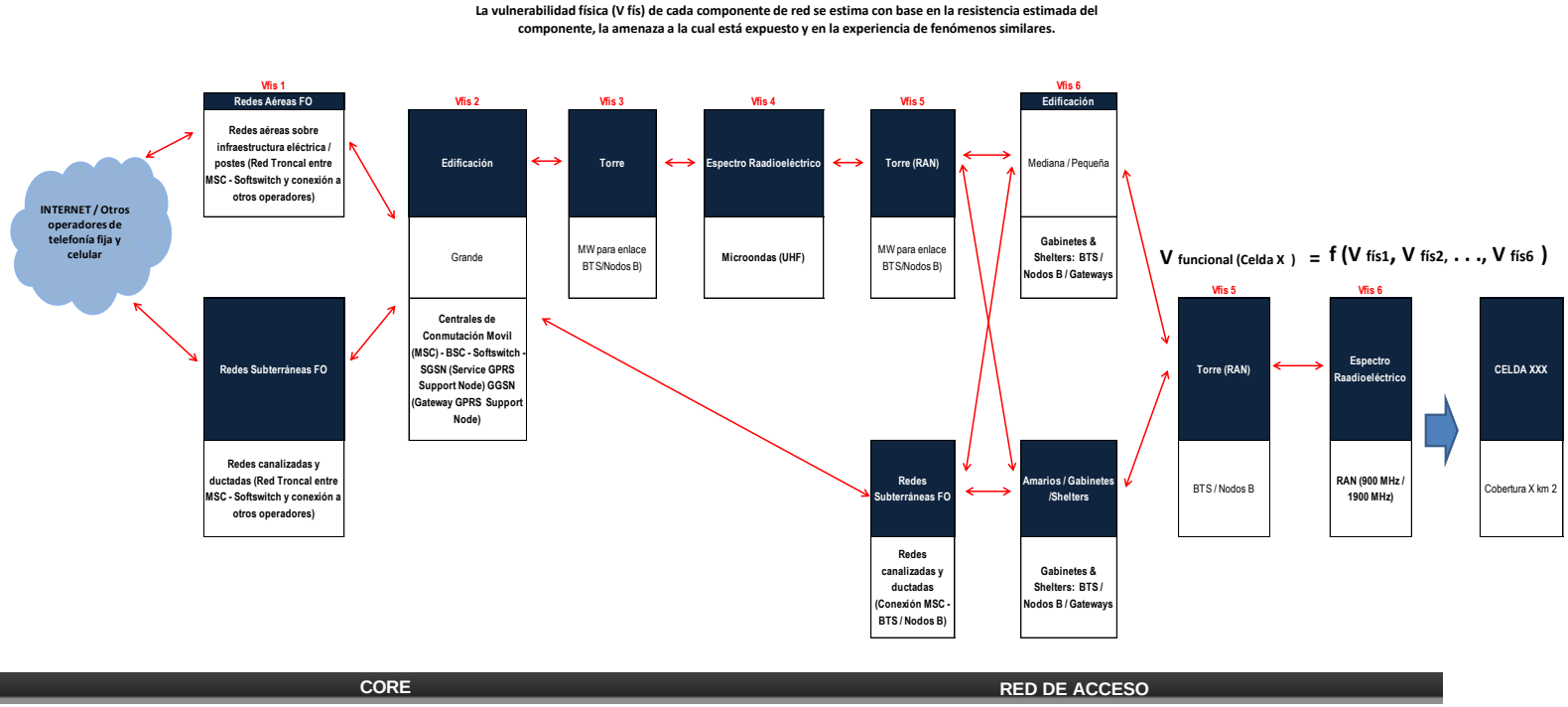
La Figura 69 ilustra los componentes de red básicos considerados en el modelo para la vulnerabilidad funcional del servicio de telefonía móvil celular e INTERNET móvil y la Figura 70 permite ver las relaciones funcionales de manera desagregada.

Figura 69. Esquema de red agregado del servicio de telefonía móvil celular e INTERNET móvil.



Fuente: CINTEL

Figura 70. Esquema funcional general del servicio Telefonía móvil celular (GSM & UMTS) e INTERNET móvil



Fuente: CINTEL

5.4.4 Servicio de radiodifusión sonora AM & FM

Este es un servicio de radiocomunicación cuyas emisiones se destinan a ser recibidas por el público en general. El contenido de las emisiones a radiodifundir a la población en general es producido en los estudios, el cual se lleva al sitio de transmisión vía un enlace de microondas (enlace estudio transmisor), vía satélite, o vía coaxial cuando el estudio está co ubicado con el transmisor. En el sitio de transmisión el contenido es radiodifundido en un área geográfica determinada a través de las frecuencias atribuidas y asignadas para radiodifusión sonora AM y FM.

Para el servicio de radiodifusión sonora se modela la vulnerabilidad funcional de cada emisora como una función de la vulnerabilidad física de cada componente de red y la vulnerabilidad funcional del servicio de radiodifusión sonora en una población determinada como una función de las vulnerabilidades de las emisoras que cubren la población bajo estudio, sin importar si son AM o FM.

La vulnerabilidad funcional de una emisora específica, se modela en función de los elementos básicos utilizados para la prestación de este servicio. La vulnerabilidad funcional de este servicio para un municipio dado, será igual a la vulnerabilidad del elemento con mayor vulnerabilidad presente en la cadena de prestación del servicio de radiodifusión sonora al municipio de interés.

La vulnerabilidad funcional de una emisora específica, basada en las vulnerabilidades físicas de cada uno de sus componentes es:

5.4.4.1 Estudio

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Equipos de estudio (se incluyen los de telepuerto cuando este

se encuentra en las misma ubicación del estudio) **(Fila 8, VFIS RADIODIFUSIÓN SONORA)**

- Vulnerabilidad de la conectividad ante diferentes amenazas naturales:
    - Antenas y espectro radioeléctrico, si la conectividad entre el estudio y el transmisor se realiza a través de microondas o satélite. **(Fila 11 y Fila 12, VFIS RADIODIFUSIÓN SONORA, VER Archivo Excel en CD)**
    - Si la conectividad es a través de coaxial, indicativo de coubicación del estudio y el transmisor, no se considera ninguna vulnerabilidad adicional, ya que esta conectividad se toma en cuenta en la vulnerabilidad de equipos instalados en el estudio.
- La vulnerabilidad del estudio ante fallas del suministro de energía
    - Si el estudio posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS RADIODIFUSIÓN SONORA)**
    - Si el estudio posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS RADIODIFUSIÓN SONORA)**
    - Si el estudio NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS RADIODIFUSIÓN SONORA)**

5.4.4.2 Transmisor

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Transmisores y equipo periférico **(Fila 9, VFIS RADIODIFUSIÓN SONORA, VER Archivo Excel en CD)**

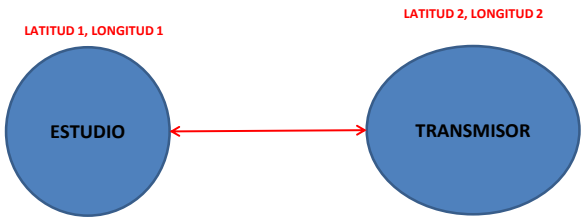
- Vulnerabilidad de la conectividad ante diferentes amenazas naturales:
    - Antenas y espectro radioeléctrico, si la conectividad entre el transmisor y el estudio se realiza a través de microondas o satélite. **(Fila 11 y Fila 12, VFIS RADIODIFUSIÓN SONORA)**
    - Si la conectividad es a través de coaxial, indicativo de co ubicación del estudio y el transmisor, no se considera ninguna vulnerabilidad adicional, ya que esta conectividad se toma en cuenta en la vulnerabilidad de equipos instalados en el estudio.
- La vulnerabilidad de la emisión radiodifundida. Antenas y espectro radioeléctrico de radiodifusión sonora. **(Fila 11 y Fila 12, VFIS RADIODIFUSIÓN SONORA, VER Archivo Excel en CD)**
- La vulnerabilidad del transmisor ante fallas del suministro de energía :
    - Si el transmisor posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 9F, VFIS RADIODIFUSIÓN SONORA)**
    - Si el transmisor posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 9G, VFIS RADIODIFUSIÓN SONORA)**
    - Si el transmisor NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 9H, VFIS RADIODIFUSIÓN SONORA)**

La vulnerabilidad funcional del servicio de radiodifusión sonora de una emisora específica, es equivalente a la mayor vulnerabilidad funcional de los dos elementos tratados (Estudio y Transmisor).

La vulnerabilidad funcional del servicio de radiodifusión sonora para un municipio determinado, se calcula como el promedio de las vulnerabilidades funcionales de todas las emisoras AM y FM, que prestan el servicio al municipio.

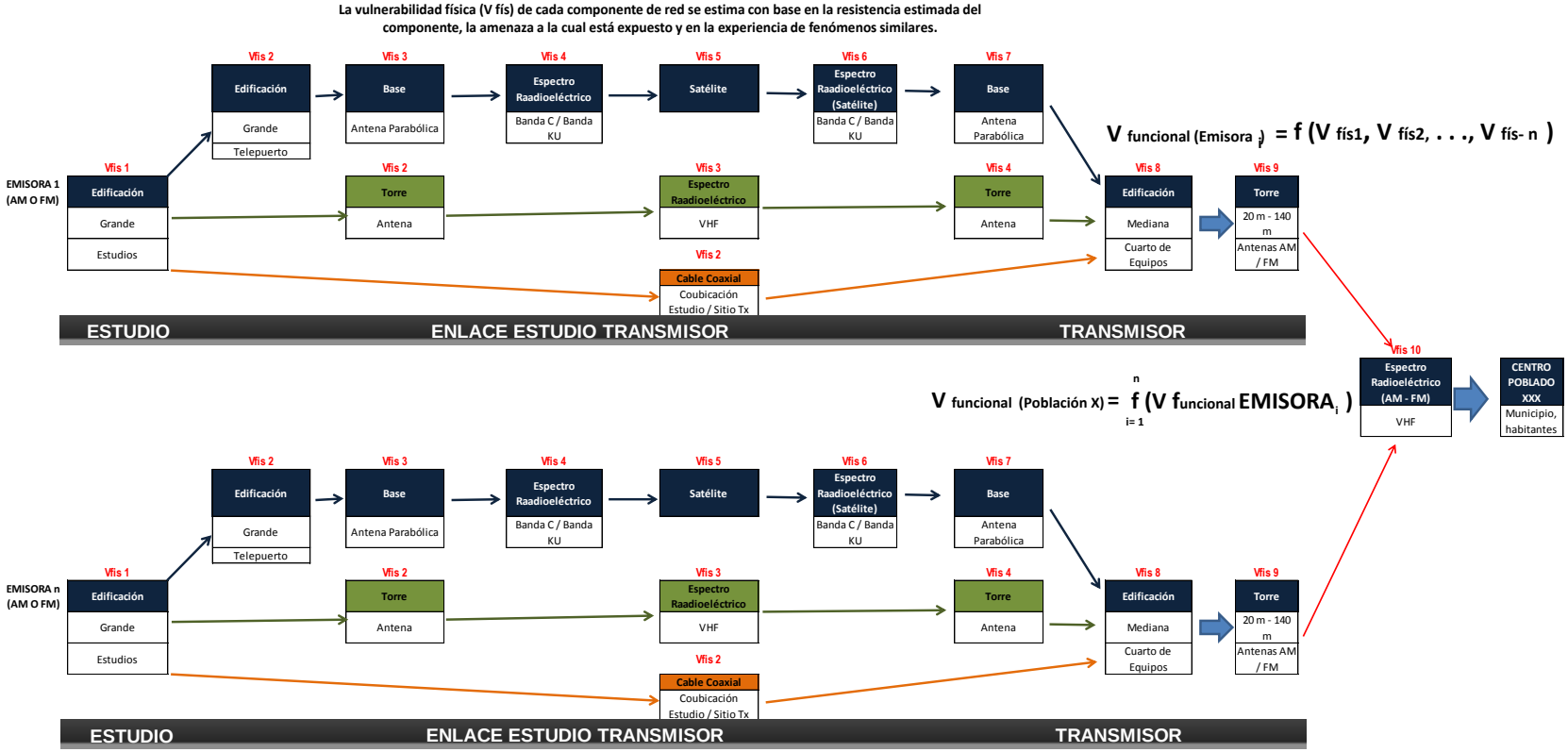
La Figura 71 ilustra los componentes de red básicos considerados en el modelo para la vulnerabilidad funcional del servicio radiodifusión sonora AM y FM y la Figura 72 permite ver las relaciones funcionales de manera desagregada.

Figura 71. Esquema de red agregado del servicio de radiodifusión sonora AM & FM.



Fuente: CINTEL

Figura 72. Esquema funcional general del servicio de radiodifusión sonora AM & FM



Fuente: CINTEL

5.4.5 Servicio de televisión radiodifundida

Este es un servicio público dirigido al público sin excepción, consistente en la emisión, transmisión, difusión, distribución, radiación y recepción de señales de audio y video en forma simultánea, distribuido a través del espectro radioeléctrico previsto para tal fin en las bandas de VHF y UHF, sin guía artificial.

En el centro de emisión se produce, integra y programa el contenido de las emisiones a radiodifundir, las cuales a través de la red de transporte (normalmente satelital) son llevadas a los sitios de transmisión (red de radiodifusión).

En el sitio de transmisión, el contenido es radiodifundido en un área geográfica determinada a través de las frecuencias atribuidas y asignadas para televisión radiodifundida de acuerdo con el Plan de Utilización de Frecuencias de la Comisión Nacional de Televisión.

Para el servicio de televisión radiodifundida, se modela la vulnerabilidad funcional de cada canal como una función de la vulnerabilidad física de cada componente de red y la vulnerabilidad funcional del servicio de televisión radiodifundida en una población determinada como una función de las vulnerabilidades de los canales radiodifundidos que cubren la población bajo estudio, sin importar si son públicos o privados.

La vulnerabilidad funcional de un canal específico, se modela en función de los elementos básicos utilizados para la prestación de este servicio. La vulnerabilidad funcional de este servicio para un municipio dado, será igual a la vulnerabilidad del elemento con mayor vulnerabilidad presente en la cadena de prestación del servicio de televisión radiodifundida al municipio de interés.

La vulnerabilidad funcional de un canal específico, basado en las vulnerabilidades físicas de cada uno de sus componentes es:

5.4.5.1 Centro de Emisión

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Equipos del centro de emisión (se incluyen los de telepuerto cuando este se encuentra en las misma ubicación del centro de emisión) **(Fila 8, VFIS TV RADIODIFUNDIDA, VER Archivo Excel en CD)**
- Vulnerabilidad de la conectividad ante diferentes amenazas naturales: Antenas y espectro radioeléctrico de la red satelital de transporte entre el centro de emisión y el transmisor. **(Fila 11 y Fila 12, VFIS TV RADIODIFUNDIDA)**
- La vulnerabilidad del centro de emisión ante fallas del suministro de energía.
    - Si el centro de emisión posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS TV RADIODIFUNDIDA)**
    - Si el centro de emisión posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS TV RADIODIFUNDIDA)**
    - Si el centro de emisión NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS TV RADIODIFUNDIDA)**

5.4.5.2 Transmisor

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Transmisores y equipo periférico **(Fila 9, VFIS TV RADIODIFUNDIDA, VER Archivo Excel en CD)**

- Vulnerabilidad de la conectividad ante diferentes amenazas naturales: Antenas y espectro radioeléctrico de la red satelital de transporte entre el transmisor y el centro de emisión. **(Fila 11 y Fila 12, VFIS TV RADIODIFUNDIDA)**
- La vulnerabilidad de la emisión de televisión radiodifundida. Antenas y espectro radioeléctrico de televisión radiodifundida. **(Fila 11 y Fila 12, VFIS TV RADIODIFUNDIDA)**
- La vulnerabilidad del transmisor ante fallas del suministro de energía :
    - Si el transmisor posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 9F, VFIS TV RADIODIFUNDIDA)**
    - Si el transmisor posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 9G, VFIS TV RADIODIFUNDIDA)**
    - Si el transmisor NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 9H, VFIS TV RADIODIFUNDIDA)**

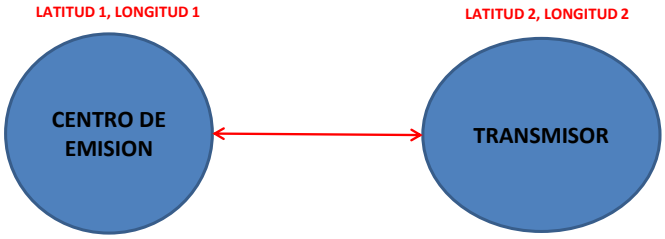
La vulnerabilidad funcional del servicio de televisión radiodifundida de un canal específico, es equivalente a la mayor vulnerabilidad funcional de los dos (2) elementos tratados (centro de emisión y transmisor).

La vulnerabilidad funcional del servicio de televisión radiodifundida para un municipio determinado se calcula como el promedio de las vulnerabilidades funcionales de todos los canales radiodifundidos que prestan el servicio al municipio.

La siguiente figura ilustra los componentes de red básicos considerados en el modelo para la vulnerabilidad funcional del servicio de televisión

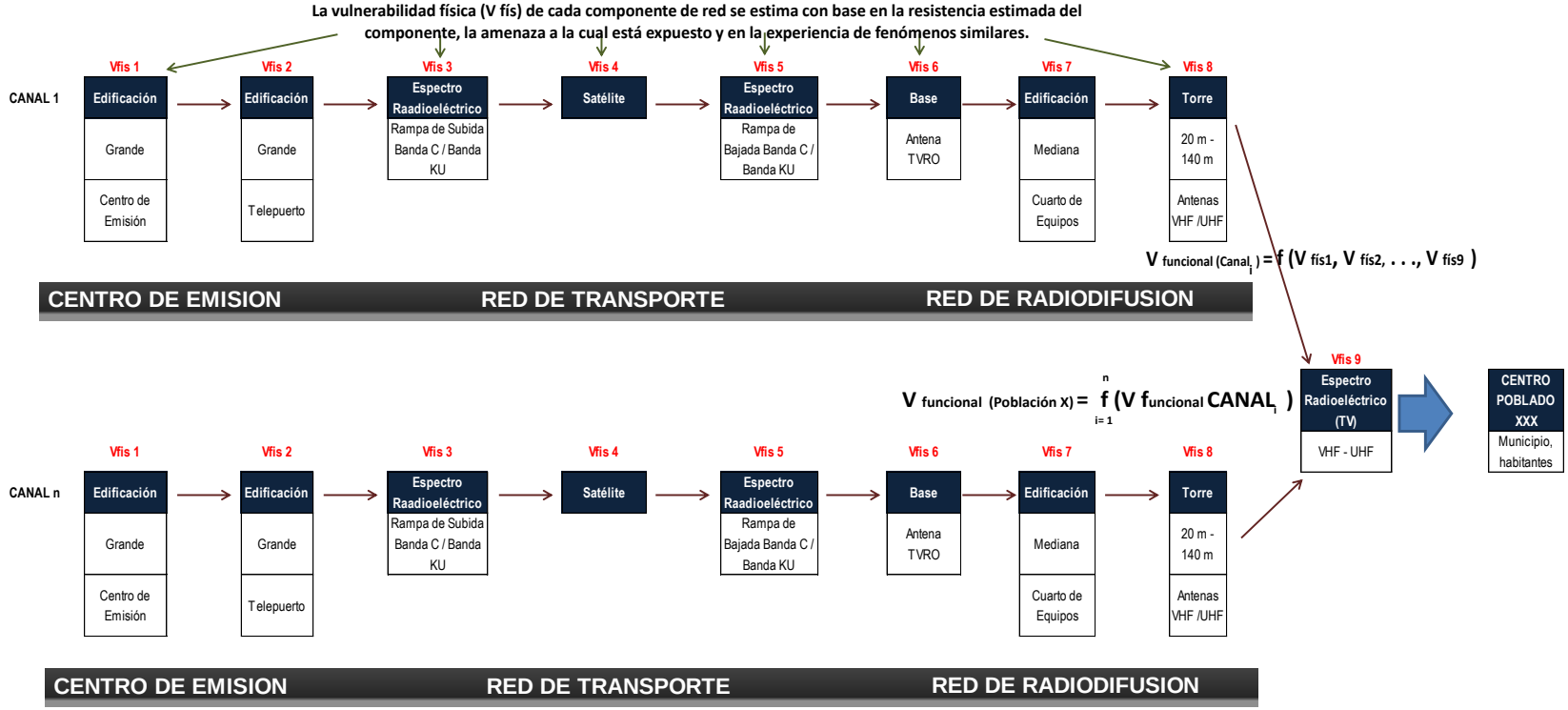
radiodifundida y la Figura 74 permite ver las relaciones funcionales de manera desagregada.

Figura 73. Esquema de red agregado del servicio de televisión radiodifundida.



Fuente: CINTEL

Figura 74. Esquema funcional general del servicio de televisión radiodifundida



Fuente: CINTEL

5.4.6 Servicio de televisión por cable

Este servicio es un servicio público dirigido al público sin excepción, consistente en la recepción, adaptación, transmisión y distribución de señales de televisión a través de un medio físico de manera exclusiva o compartida con otros servicios de telecomunicaciones.

La cabecera adapta señales de televisión tanto terrestres como satelitales y luego a través de sus redes de transporte y acceso, las cuales son redes aéreas y subterráneas de fibra óptica (normalmente fibra óptica subterránea), entrega estas señales a la red de distribución, la cual normalmente es una red aérea o subterránea de cable coaxial que llega hasta el hogar del usuario.

Para el servicio de televisión por cable se modela la vulnerabilidad funcional de cada concesionario como una función de la vulnerabilidad física de cada componente de red y la vulnerabilidad funcional del servicio de televisión por cable en una población determinada como una función de las vulnerabilidades de los concesionarios que prestan el servicio de televisión por cablea un municipio dado.

La vulnerabilidad funcional de un concesionario específico, se modela en función de los elementos básicos utilizados para la prestación de este servicio. La vulnerabilidad funcional de este servicio para un municipio dado, será igual a la vulnerabilidad del elemento con mayor vulnerabilidad presente en la cadena de prestación del servicio de televisión por cable al municipio de interés.

La vulnerabilidad funcional de un concesionario específico, basado en las vulnerabilidades físicas de cada uno de sus componentes es:

5.4.6.1 Cabecera

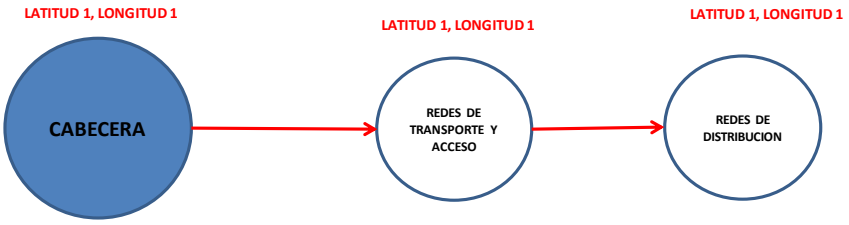
- Vulnerabilidad de equipos ante diferentes amenazas naturales: Equipos de Cabecera **(Fila 8, VFIS TV POR CABLE, VER Archivo Excel en CD)**
- Vulnerabilidad de la conectividad (recepción de señales) ante diferentes amenazas naturales: Antenas y espectro radioeléctrico que reciben señales de televisión satelitales y vía microondas.**(Fila 10 y Fila 11, VFIS TV POR CABLE)**
- Vulnerabilidad de la conectividad (Red de Transporte), ante diferentes amenazas naturales: Fibra óptica subterránea y aérea. **(Mayor valor entre Fila 13 y Fila 16 de VFIS TV POR CABLE).**
- Vulnerabilidad de la conectividad (Red de Acceso), ante diferentes amenazas naturales: Fibra óptica subterránea y aérea. **(Mayor valor entre Fila 13 y Fila 16 de VFIS TV POR CABLE).**
- Vulnerabilidad de la conectividad (Red de Distribución), ante diferentes amenazas naturales: Redes aéreas y subterráneas de cobre (COAXIAL). **(Mayor valor entre Fila 14 y Fila 17 de VFIS TV POR CABLE).**
- La vulnerabilidad de la Cabecera ante fallas del suministro de energía:
    - Si la cabecera posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS TV POR CABLE)**
    - Si la cabecera posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS TV POR CABLE)**
    - Si la cabecera NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS TV POR CABLE)**

La vulnerabilidad funcional del servicio por cable de un concesionario específico, es equivalente a la mayor vulnerabilidad física de los elementos básicos analizados en la cabecera.

La vulnerabilidad funcional del servicio de televisión por cable para un municipio determinado se calcula como el promedio de las vulnerabilidades funcionales de todos los concesionarios que prestan el servicio al municipio.

La Figura 75 ilustra los componentes de red básicos considerados en el modelo para la vulnerabilidad funcional del servicio de televisión por cable y la Figura 76 permite ver las relaciones funcionales de manera desagregada.

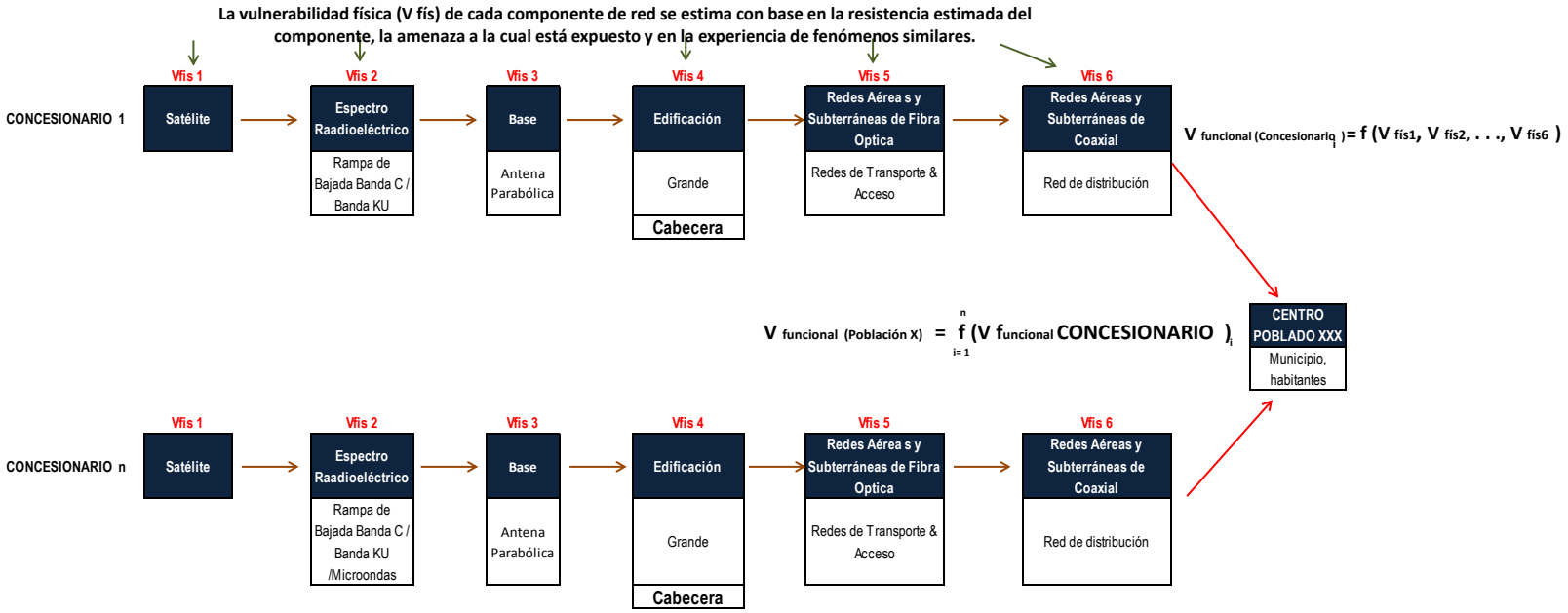
Figura 75. Esquema de red agregado del servicio de televisión por cable.



NOTA 1: En este estudio se toman las redes de transporte, acceso y distribución como un elemento de la cabecera y con sus mismas coordenadas geográficas.

Fuente: CINTEL

Figura 76. Esquema funcional general del servicio de televisión por cable



Fuente: CINTEL

5.4.7 Servicio de Móvil Marítimo

El servicio de móvil marítimo comprende las comunicaciones al interior de la embarcación y con su botes, aspecto no cubierto en este estudio y, las comunicaciones desde la embarcación con la (s) estación (es) costera (s), tanto terrestres como satelitales.

La vulnerabilidad funcional de una estación costera o un gabinete de ayuda a la navegación, se modela en función de los elementos básicos utilizados para la prestación de este servicio. La vulnerabilidad funcional de este servicio para una estación costera o un gabinete de ayuda a la navegación, será igual a la vulnerabilidad del elemento con mayor vulnerabilidad presente en la cadena de prestación del servicio de móvil marítimo conexo a la estación costera o al gabinete de ayuda a la navegación.

La vulnerabilidad funcional de las comunicaciones de móvil marítimo, basado en las vulnerabilidades físicas de cada uno de sus componentes es:

5.4.7.1 Estación costera

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Estación costera **(Fila 8, VFIS MÓVIL MARÍTIMO, VER Archivo Excel en CD)**
- Vulnerabilidad de la conectividad con el elemento de orden superior ante diferentes amenazas naturales:
    - Antenas y espectro radioeléctrico, si la conectividad entre la estación costera y el elemento de orden superior es a través de microondas. **(Fila 12y Fila 13, VFIS MÓVIL MARÍTIMO)**

- Fibra óptica subterránea[50], si la conectividad entre la estación costera y el elemento de orden superior es por fibra óptica. **(Fila 15, VFIS MÓVIL MARÍTIMO)**
- Si la conectividad es de fibra óptica con backup de microondas, se toma la menor vulnerabilidad de los dos medios de transporte. **(Menor de (Fila 12y Fila 13, VFIS MÓVIL MARÍTIMO) y (Fila 15, VFIS MÓVIL MARÍTIMO)).**

- Vulnerabilidad de la conectividad con los gabinetes de navegación ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 12 y Fila 13, VFIS MÓVIL MARÍTIMO).**
- Vulnerabilidad de la conectividad con las embarcaciones ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 12 y Fila 13, VFIS MÓVIL MARÍTIMO).**
- La vulnerabilidad de la estación costera ante fallas del suministro de energía:
  - Si la estación costera posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS MÓVIL MARÍTIMO)**
  - Si la estación costera posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS MÓVIL MARÍTIMO)**

---

[50] Se toma la vulnerabilidad de la fibra óptica subterránea ya que esta conectividad se realizaría en un ambiente urbano, que utiliza normalmente fibra subterránea.

- Si la estación costera NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS MÓVIL MARÍTIMO)**

5.4.7.2 Elemento de orden superior

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Elemento de Orden Superior **(Fila 8, VFIS MÓVIL MARÍTIMO, VER Archivo Excel en CD)**
- Vulnerabilidad de la conectividad con la estación costera ante diferentes amenazas naturales:
  - Antenas y espectro radioeléctrico, si la conectividad entre el elemento de orden superior y la estación costera es a través de microondas. **(Fila 12y Fila 13, VFIS MÓVIL MARÍTIMO)**
  - Fibra óptica subterránea[51], si la conectividad entre el elemento de orden superior y la estación costera es por fibra óptica. **(Fila 15, VFIS MÓVIL MARÍTIMO)**
  - Si la conectividad es de fibra óptica con backup de microondas, se toma la menor vulnerabilidad de los dos medios de transporte. **(Menor de (Fila 12y Fila 13, VFIS MÓVIL MARÍTIMO) y (Fila 15, VFIS MÓVIL MARÍTIMO)).**
- Vulnerabilidad de la conectividad con los gabinetes de navegación ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 12 y Fila 13, VFIS MÓVIL MARÍTIMO).**

---

[51] Se toma la vulnerabilidad de la fibra óptica subterránea ya que esta conectividad se realizaría en un ambiente urbano, que utiliza normalmente fibra subterránea.

- La vulnerabilidad del elemento de orden superior ante fallas del suministro de energía:
    - Si el elemento de orden superior posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS MÓVIL MARÍTIMO)**
    - Si el elemento de orden superior posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS MÓVIL MARÍTIMO)**
    - Si el elemento de orden superior NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS MÓVIL MARÍTIMO)**

5.4.7.3 Gabinete de ayuda a la navegación

- Vulnerabilidad de equipos ante diferentes amenazas naturales:
    - Equipos de ayuda a la navegación instalados en gabinetes en pequeñas edificaciones[52] **(Fila 9, VFIS MÓVIL MARÍTIMO, VER Archivo Excel en CD)**
    - Equipos de ayuda a la navegación instalados en gabinetes al aire libre **(Fila 10, VFIS MÓVIL MARÍTIMO)**
- Vulnerabilidad de la conectividad con la estación costera ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres **(Fila 12 y Fila 13, VFIS MÓVIL MARÍTIMO)**

---

[52] **Se considera que la vulnerabilidad física de gabinetes y shelters instalados en pequeñas edificaciones construidas sin apego a normas antisísmicas es mayor que la de los instalados al aire libre.**

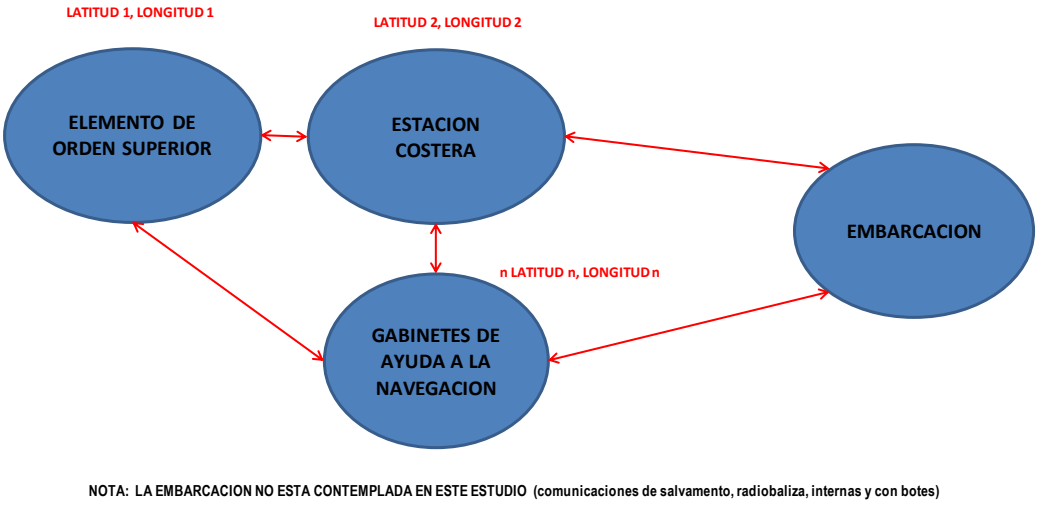
- Vulnerabilidad de la conectividad con el elemento de orden superior ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres **(Fila 12 y Fila 13, VFIS MÓVIL MARÍTIMO)**
- Vulnerabilidad de la conectividad con la embarcación ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres **(Fila 12 y Fila 13, VFIS MÓVIL MARÍTIMO)**
- La vulnerabilidad del gabinete ante fallas del suministro de energía:
    - Si el gabinete posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 9F, VFIS MÓVIL MARÍTIMO)**
    - Si el gabinete posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 9G, VFIS MÓVIL MARÍTIMO)**
    - Si el gabinete NO posee energía de respaldo, se considera de alta vulnerabilidad. **(Celda 9H, VFIS MÓVIL MARÍTIMO)**

La vulnerabilidad funcional del servicio de móvil marítimo, para una estación costera determinada con todas sus funcionalidades, se calcula como el valor de la mayor vulnerabilidad de los componentes básicos del servicio: estación costera, elemento de orden superior y gabinetes de ayuda a la navegación (promedio de vulnerabilidad de gabinetes).

La vulnerabilidad funcional del servicio de móvil marítimo, para una estación costera determinada solamente con la funcionalidad de las comunicaciones con la embarcación, se calcula como el valor de la mayor vulnerabilidad de los componentes básicos de esta cadena: estación costera.

La Figura 77 ilustra los componentes de red básicos considerados en el modelo para la vulnerabilidad funcional del servicio de móvil marítimo y la Figura 78 permite ver las relaciones funcionales de manera desagregada.

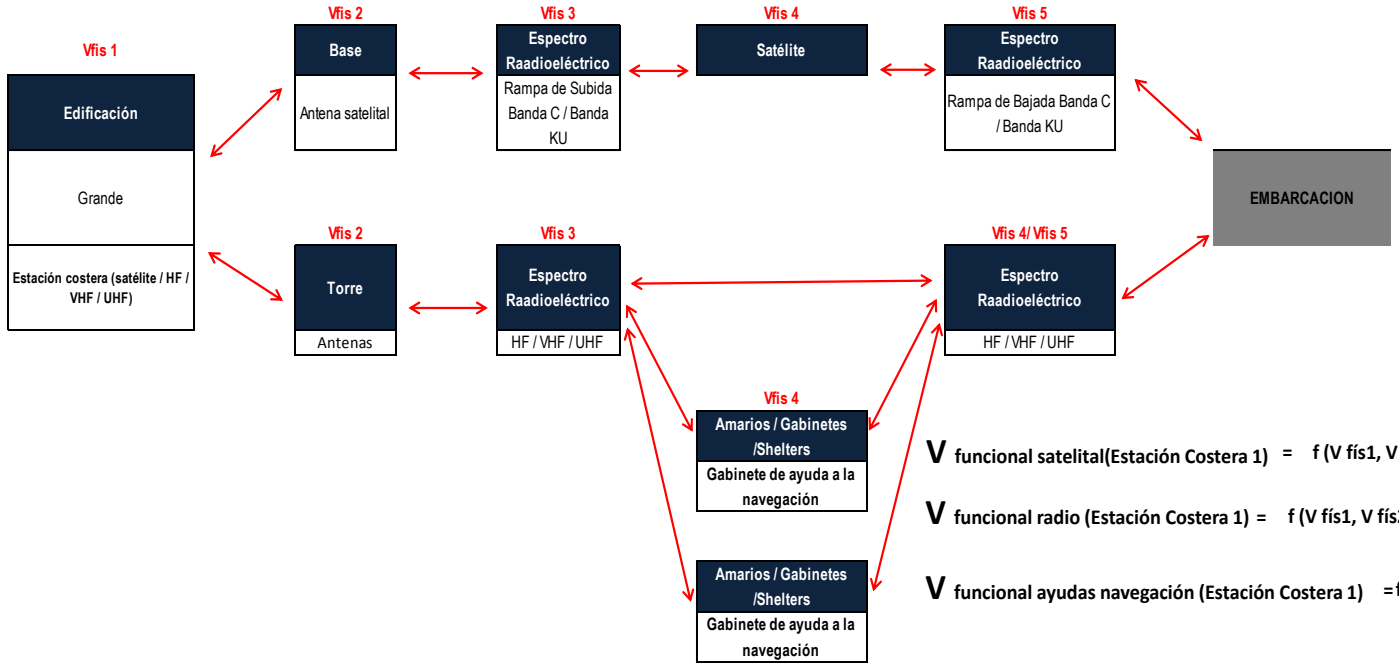
Figura 77. Esquema de red agregado del servicio de móvil marítimo



Fuente: CINTEL

Figura 78. Esquema funcional general del servicio de móvil marítimo

La vulnerabilidad física (V fís) de cada componente de red se estima con base en la resistencia estimada del componente, la amenaza a la cual está expuesto y en la experiencia de fenómenos similares.



V funcional satelital(Estación Costera 1) = f (V fís1, V fís2, . . ., V fís5)

V funcional radio (Estación Costera 1) = f (V fís1, V fís2, . . ., V fís4)

V funcional ayudas navegación (Estación Costera 1) =f (V fís1, V fís2, . . ., V fís5)

Fuente: CINTEL

5.4.8 Servicio de Móvil Aeronáutico

El servicio de móvil aeronáutico comprende las comunicaciones desde la aeronave con la (s) estación (es) aeronáuticas (s), tanto terrestres como satelitales.

La vulnerabilidad funcional de una estación aeronáutica o un gabinete de ayuda a la navegación, se modela en función de los elementos básicos utilizados para la prestación de este servicio. La vulnerabilidad funcional de este servicio para una estación aeronáutica o un gabinete de ayuda a la navegación, será igual a la vulnerabilidad del elemento con mayor vulnerabilidad presente en la cadena de prestación del servicio de móvil aeronáutico conexo a la estación aeronáutica o al gabinete de ayuda a la navegación.

La vulnerabilidad funcional de las comunicaciones de móvil aeronáutico, basado en las vulnerabilidades físicas de cada uno de sus componentes es:

5.4.8.1 Estación Aeronáutica

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Estación aeronáutica **(Fila 8, VFIS MÓVIL AERONÁUTICO, VER Archivo Excel en CD)**
- Vulnerabilidad de la conectividad con el elemento de orden superior ante diferentes amenazas naturales:
    - Antenas y espectro radioeléctrico, si la conectividad entre la estación aeronáutica y el elemento de orden superior es a través de microondas. **(Fila 12 y Fila 13, VFIS MÓVIL AERONÁUTICO)**

- Fibra óptica subterránea[53], si la conectividad entre la estación aeronáutica y el elemento de orden superior es por fibra óptica. **(Fila 15, VFIS MÓVIL AERONÁUTICO)**
- Si la conectividad es de fibra óptica con backup de microondas, se toma la menor vulnerabilidad de los dos medios de transporte. **(Menor de (Fila 12y Fila 13, VFIS MÓVIL AERONÁUTICO) y (Fila 15, VFIS MÓVIL AERONÁUTICO)).**

- Vulnerabilidad de la conectividad con los gabinetes de navegación ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 12 y Fila 13, VFIS MÓVIL AERONÁUTICO).**
- Vulnerabilidad de la conectividad con las aeronaves ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 12 y Fila 13, VFIS MÓVIL AERONÁUTICO).**
- La vulnerabilidad de la estación aeronáutica ante fallas del suministro de energía:
  - Si la estación aeronáutica posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS MÓVIL AERONÁUTICO)**
  - Si la estación aeronáutica posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS MÓVIL AERONÁUTICO)**

---

[53] Se toma la vulnerabilidad de la fibra óptica subterránea ya que esta conectividad se realizaría en un ambiente urbano, que utiliza normalmente fibra subterránea.

- Si la estación aeronáutica NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS MÓVIL AERONÁUTICO)**

5.4.8.2 Elemento de orden superior

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Elemento de Orden Superior **(Fila 8, VFIS MÓVIL AERONÁUTICO, VER Archivo Excel en CD)**
- Vulnerabilidad de la conectividad con la estación aeronáutica ante diferentes amenazas naturales:
- Antenas y espectro radioeléctrico, si la conectividad entre el elemento de orden superior y la estación aeronáutica es a través de microondas. **(Fila 12y Fila 13, VFIS MÓVIL AERONÁUTICO)**
  - Fibra óptica subterránea[54], si la conectividad entre el elemento de orden superior y la estación aeronáutica es por fibra óptica. **(Fila 15, VFIS MÓVIL AERONÁUTICO)**
  - Si la conectividad es de fibra óptica con backup de microondas, se toma la menor vulnerabilidad de los dos medios de transporte. **(Menor de (Fila 12y Fila 13, VFIS MÓVIL AERONÁUTICO) y (Fila 15, VFIS MÓVIL AERONÁUTICO)).**
- Vulnerabilidad de la conectividad con los gabinetes de navegación ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 12 y Fila 13, VFIS MÓVIL AERONÁUTICO).**

[54] **Se toma la vulnerabilidad de la fibra óptica subterránea ya que esta conectividad se realizaría en un ambiente urbano, que utiliza normalmente fibra subterránea.**

- La vulnerabilidad del elemento de orden superior ante fallas del suministro de energía:
    - Si el elemento de orden superior posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS MÓVIL AERONÁUTICO)**
    - Si el elemento de orden superior posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS MÓVIL AERONÁUTICO)**
    - Si el elemento de orden superior NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS MÓVIL AERONÁUTICO)**

5.4.8.3 Gabinete de ayuda a la navegación

- Vulnerabilidad de equipos ante diferentes amenazas naturales:
    - Equipos de ayuda a la navegación instalados en gabinetes en pequeñas edificaciones[55] **(Fila 9, VFIS MÓVIL AERONÁUTICO, VER Archivo Excel en CD)**
    - Equipos de ayuda a la navegación instalados en gabinetes al aire libre **(Fila 10, VFIS MÓVIL AERONÁUTICO)**
- Vulnerabilidad de la conectividad con la estación aeronáutica ante diferentes amenazas naturales: Antenas y espectro

[55]Se considera que la vulnerabilidad física de gabinetes y shelters instalados en pequeñas edificaciones construidas sin apego a normas antisísmicas es mayor que la de los instalados al aire libre.

radioeléctrico satelitales y terrestres **(Fila 12 y Fila 13, VFIS MÓVIL AERONÁUTICO)**

- Vulnerabilidad de la conectividad con el elemento de orden superior ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres **(Fila 12 y Fila 13, VFIS MÓVIL AERONÁUTICO)**
- Vulnerabilidad de la conectividad con la aeronave ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres **(Fila 12 y Fila 13, VFIS MÓVIL AERONÁUTICO)**
- La vulnerabilidad del gabinete ante fallas del suministro de energía:
    - Si el gabinete posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 9F, VFIS MÓVIL AERONÁUTICO)**
    - Si el gabinete posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 9G, VFIS MÓVIL AERONÁUTICO)**
    - Si el gabinete NO posee energía de respaldo, se considera de alta vulnerabilidad. **(Celda 9H, VFIS MÓVIL AERONÁUTICO)**

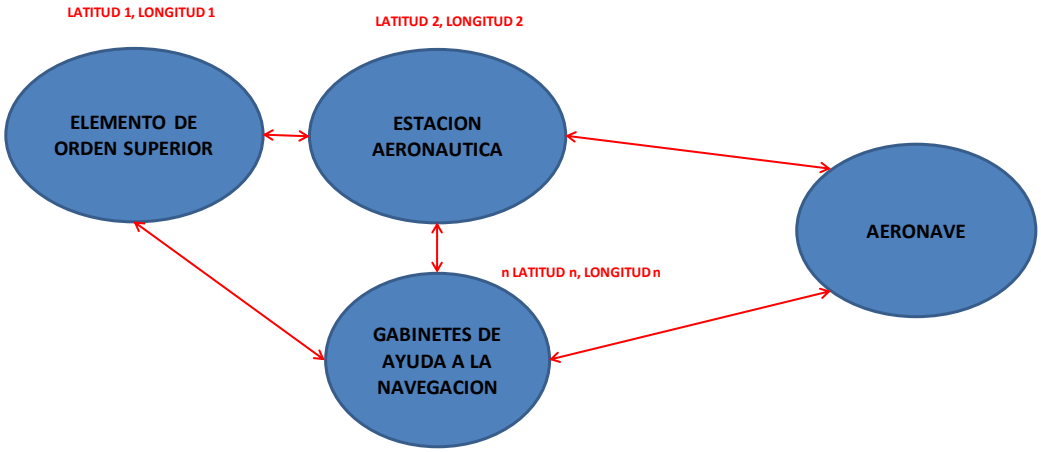
La vulnerabilidad funcional del servicio de móvil aeronáutico, para una estación aeronáutica determinada con todas sus funcionalidades, se calcula como el valor de la mayor vulnerabilidad de los componentes básicos del servicio: estación aeronáutica, elemento de orden superior y gabinetes de ayuda a la navegación (promedio de vulnerabilidad de gabinetes).

La vulnerabilidad funcional del servicio de móvil aeronáutico, para una estación aeronáutica determinada solamente con la funcionalidad de las

comunicaciones con la aeronave, se calcula como el valor de la mayor vulnerabilidad de los componentes básicos de esta cadena: estación aeronáutica.

La Figura 79 ilustra los componentes de red básicos considerados en el modelo para la vulnerabilidad funcional del servicio de móvil aeronáutico y la Figura 80 permite ver las relaciones funcionales de manera desagregada.

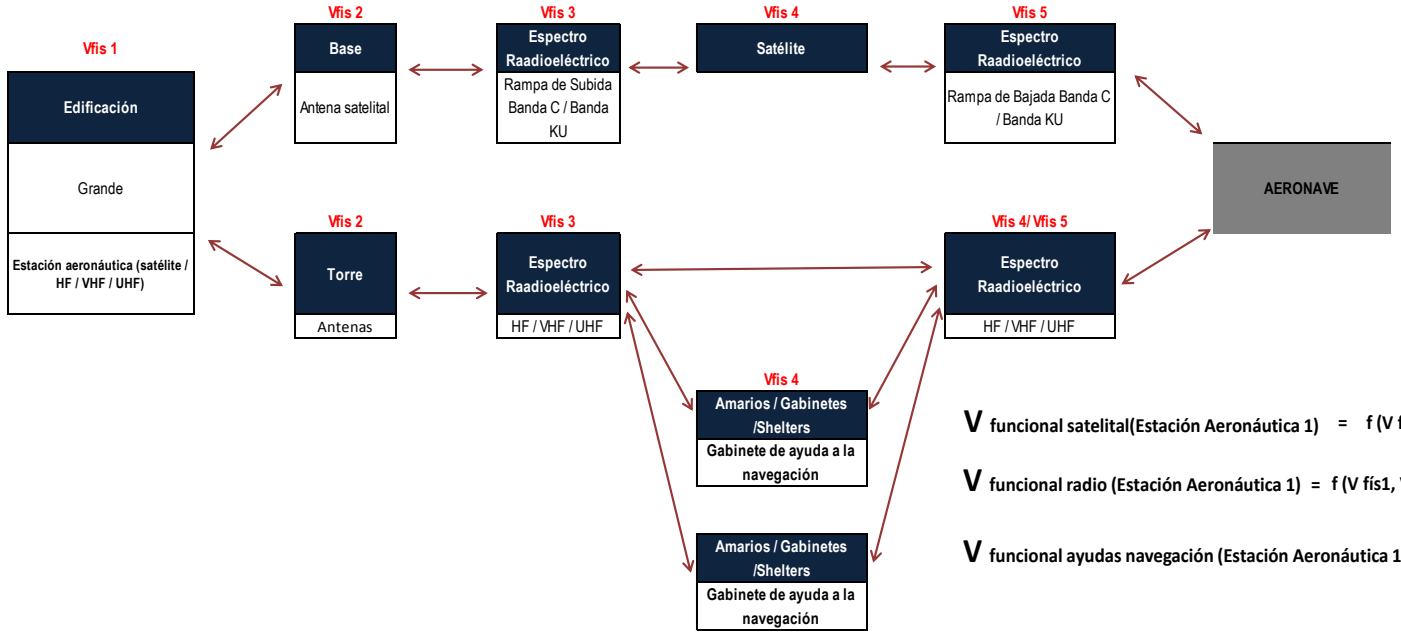
Figura 79. Esquema de red agregado del servicio de móvil aeronáutico



Fuente: CINTEL

Figura 80. Esquema funcional general del servicio de móvil aeronáutico

La vulnerabilidad física (V fís) de cada componente de red se estima con base en la resistencia estimada del componente, la amenaza a la cual está expuesto y en la experiencia de fenómenos similares.



Fuente: CINTEL

5.4.9 Servicio de radioaficionados

La red de radioaficionados basa su operación en el interés social y comunitario de radioaficionados y técnicamente la operación de un radioaficionado no depende de ninguno otro, por lo cual la vulnerabilidad funcional de un radioaficionado es:

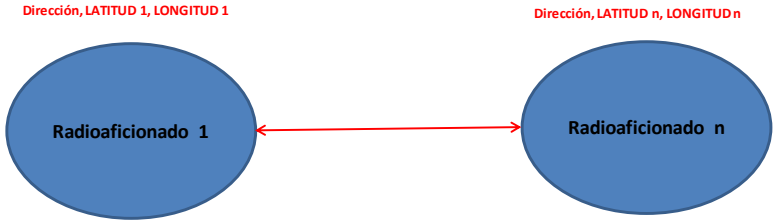
5.4.9.1 Estación de radioaficionado (Tiene sus coordenadas geográficas o dirección)

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Estación de radioaficionado (Normalmente en casas de habitación) **(Fila 8, VFIS RADIOAFICIONADOS, VER Archivo Excel en CD)**
- Vulnerabilidad de la conectividad con otros radioaficionados ante diferentes amenazas naturales: Antenas y espectro radioeléctrico de HF, VHF y UHF. **(Fila 10 y Fila 11, VFIS RADIOAFICIONADOS)**
- La vulnerabilidad de la estación de radioaficionado ante fallas del suministro de energía:
    - Si la estación de radioaficionado posee energía de respaldo con autonomía mayor a 24 horas (NO ES LO NORMAL), se considera de baja vulnerabilidad. **(Celda 8F, VFIS RADIOAFICIONADOS)**
    - Si la estación de radioaficionado posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS RADIOAFICIONADOS)**
    - Si la estación de radioaficionado NO posee energía de respaldo, se considera de alta vulnerabilidad. **(Celda 8H, VFIS RADIOAFICIONADOS)**

La vulnerabilidad funcional de una estación de radioaficionado, es equivalente a la mayor vulnerabilidad física de los elementos básicos que la componen.

La Figura 81 ilustra los componentes básicos considerados en el modelo para la vulnerabilidad funcional del servicio de radioaficionados y la **Figura 82** permite ver las relaciones funcionales de manera desagregada.

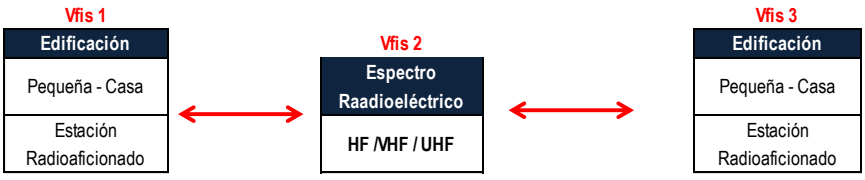
Figura 81. Esquema de red agregado del servicio de radioaficionados



Fuente: CINTEL

Figura 82 Esquema funcional general del servicio de móvil aeronáutico

La vulnerabilidad física (V fís) de cada componente de red se estima con base en la resistencia estimada del componente, la amenaza a la cual está expuesto y en la experiencia de fenómenos similares.



Fuente: CINTEL

5.4.10 COMPARTEL

La vulnerabilidad funcional de las redes COMPARTEL, la cuales son básicamente satelitales, se modela en función de los elementos específicos básicos utilizados para la prestación de este servicio en un punto COMPARTEL determinado, de un municipio específico. La vulnerabilidad funcional de este servicio para un punto COMPARTEL dado, será igual a la vulnerabilidad del elemento con mayor vulnerabilidad presente en la cadena de prestación del servicio.

La vulnerabilidad funcional del servicio de COMPARTEL en un punto dado, basado en las vulnerabilidades físicas de cada uno de sus componentes es:

5.4.10.1 HUB

- Vulnerabilidad de equipos ante diferentes amenazas naturales: HUB **(Fila 8, VFIS COMPARTEL, VER Archivo Excel en CD)**
- Vulnerabilidad de la conectividad con los puntos COMPARTEL ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 11 y Fila 12, VFIS COMPARTEL).**
- La vulnerabilidad del HUB ante fallas del suministro de energía:
    - Si el HUB posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS COMPARTEL)**
    - Si el HUB posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS COMPARTEL)**
    - Si el HUB NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS COMPARTEL)**

5.4.10.2 Elemento de orden superior alternativo

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Elemento de orden superior **(Fila 8, VFIS COMPARTEL, VER Archivo Excel en CD)**
- Vulnerabilidad de la conectividad con los puntos COMPARTEL ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 11 y Fila 12, VFIS COMPARTEL).**
- La vulnerabilidad del elemento de orden superior alternativo ante fallas del suministro de energía:
    - Si el elemento de orden superior alternativo posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS COMPARTEL)**
    - Si el elemento de orden superior alternativo posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS COMPARTEL)**
    - Si el elemento de orden superior alternativo NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS COMPARTEL)**

5.4.10.3 Punto COMPARTEL

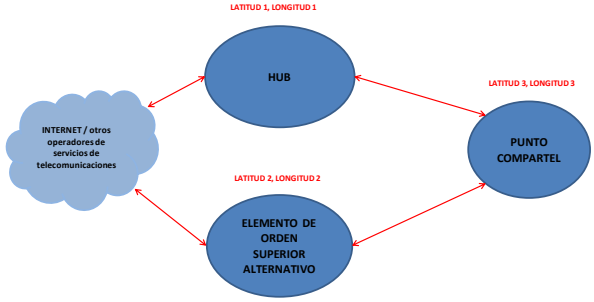
- Vulnerabilidad de equipos ante diferentes amenazas naturales: Punto COMPARTEL instalado normalmente en pequeñas edificaciones**(Fila 9, VFIS COMPARTEL)**
- Vulnerabilidad de la conectividad con el HUB ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 11 y Fila 12, VFIS COMPARTEL).**
- Vulnerabilidad de la conectividad con el elemento de orden superior alternativo ante diferentes amenazas naturales:

Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 11 y Fila 12, VFIS COMPARTEL).**

- La vulnerabilidad del punto COMPARTEL ante fallas del suministro de energía:
  - Si el punto COMPARTEL posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 9F, VFIS COMPARTEL)**
  - Si el punto COMPARTEL posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 9G, VFIS COMPARTEL)**
  - Si el punto COMPARTEL NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 9H, VFIS COMPARTEL)**

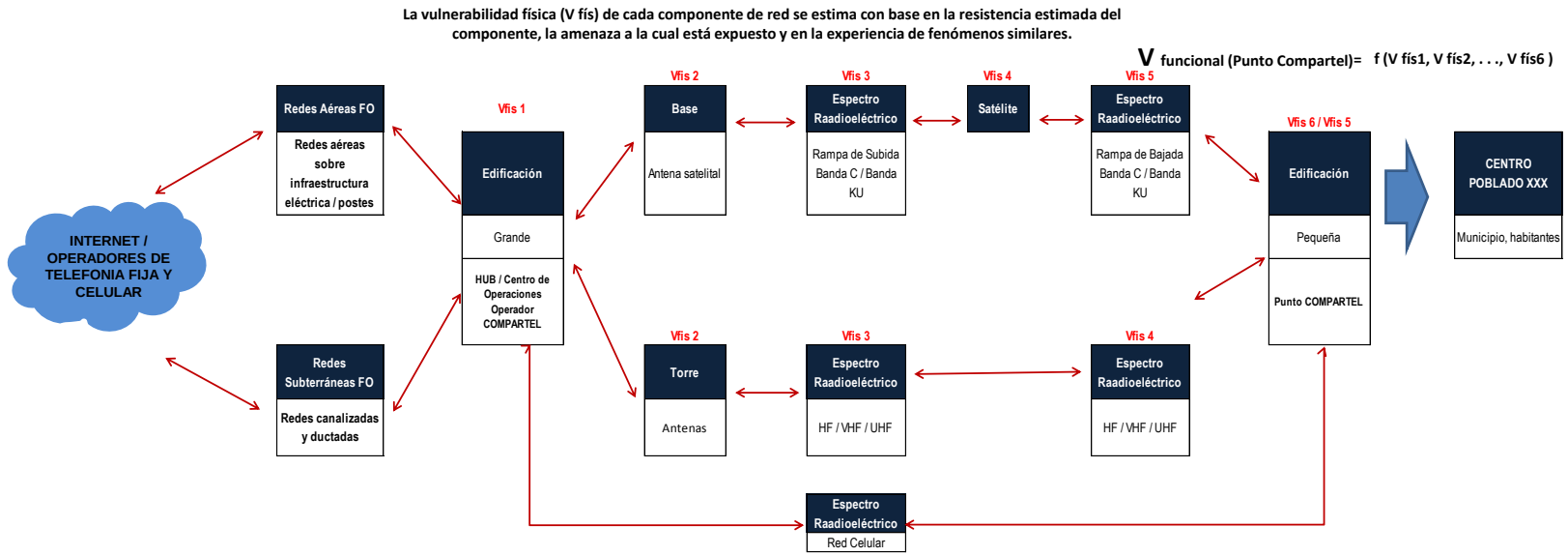
La vulnerabilidad funcional de un punto COMPARTEL específico, se calcula como el valor de la mayor vulnerabilidad funcional de los componentes básicos del servicio, esto es: HUB, elemento de orden superior alternativo y punto COMPARTEL. La Figura 83 ilustra los componentes de red básicos considerados en el modelo para la vulnerabilidad funcional del servicio COMPARTEL y la Figura 84 permite ver las relaciones funcionales de manera desagregada.

Figura 83. Esquema de red agregado de COMPARTEL



Fuente: CINTEL

Figura 84. Esquema funcional general de COMPARTEL



Fuente: CINTEL

5.4.11 Redes de comunicaciones de emergencia

Las redes de emergencia, como ya se ha establecido, operan sobre redes de radio que utilizan sistemas de monocanales de voz o radio convencional, en las bandas de VHF.

La vulnerabilidad funcional de estas redes para una BASE de radio dada, será igual a la vulnerabilidad del elemento con mayor vulnerabilidad presente en la cadena de operación de la red de emergencia.

La vulnerabilidad funcional de las redes de emergencia para una BASE de radio dada, basado en las vulnerabilidades físicas de cada uno de sus componentes es:

5.4.11.1 Repetidora

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Repetidora **(Fila 8, VFIS REDES DE EMERGENCIA, VER Archivo Excel en CD).**
- Vulnerabilidad de la conectividad con las BASES de radio ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 10 y Fila 11, VFIS REDES DE EMERGENCIA).**
- La vulnerabilidad de la repetidora ante fallas del suministro de energía:
    - Si la repetidora posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS REDES DE EMERGENCIA)**
    - Si la repetidora posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS REDES DE EMERGENCIA)**

- Si la repetidora NO posee energía de respaldo, se considera de alta vulnerabilidad. **(Celda 8H, VFIS REDES DE EMERGENCIA)**

5.4.11.2 Elemento de orden superior alternativo

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Elemento de orden superior alternativo **(Fila 8, VFIS REDES DE EMERGENCIA)**
- Vulnerabilidad de la conectividad con las BASES de radio ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 10 y Fila 11, VFIS REDES DE EMERGENCIA).**
- La vulnerabilidad del elemento de orden superior alternativo ante fallas del suministro de energía:
  - Si el elemento de orden superior alternativo posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS REDES DE EMERGENCIA)**
  - Si el elemento de orden superior alternativo posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS REDES DE EMERGENCIA)**
  - Si el elemento de orden superior alternativo NO posee energía de respaldo, se considera de alta vulnerabilidad. **(Celda 8H, VFIS REDES DE EMERGENCIA)**

5.4.11.3 Base

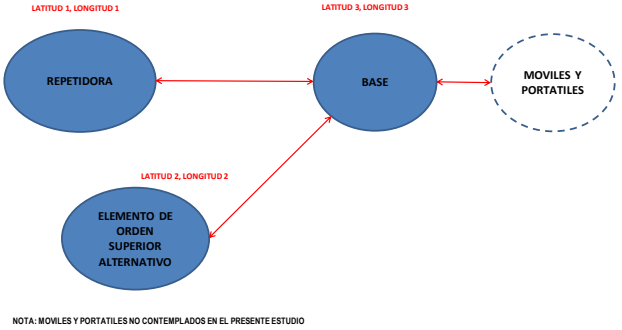
- Vulnerabilidad de equipos ante diferentes amenazas naturales: BASE de radio**(Fila 8, VFIS REDES DE EMERGENCIA)**

- Vulnerabilidad de la conectividad con repetidora de radio ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 10 y Fila 11, VFIS REDES DE EMERGENCIA).**
- Vulnerabilidad de la conectividad con el elemento de orden superior ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 10 y Fila 11, VFIS REDES DE EMERGENCIA).**
- La vulnerabilidad de la BASE ante fallas del suministro de energía:
    - Si la BASE posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS REDES DE EMERGENCIA)**
    - Si la BASE posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS REDES DE EMERGENCIA)**
    - Si la BASE NO posee energía de respaldo, se considera de alta vulnerabilidad. **(Celda 8H, VFIS REDES DE EMERGENCIA)**

La vulnerabilidad funcional de una BASE de radio específica, se calcula como el valor de la mayor vulnerabilidad funcional de los componentes básicos conexos, esto es: Repetidora, elemento de orden superior alternativo y BASE.

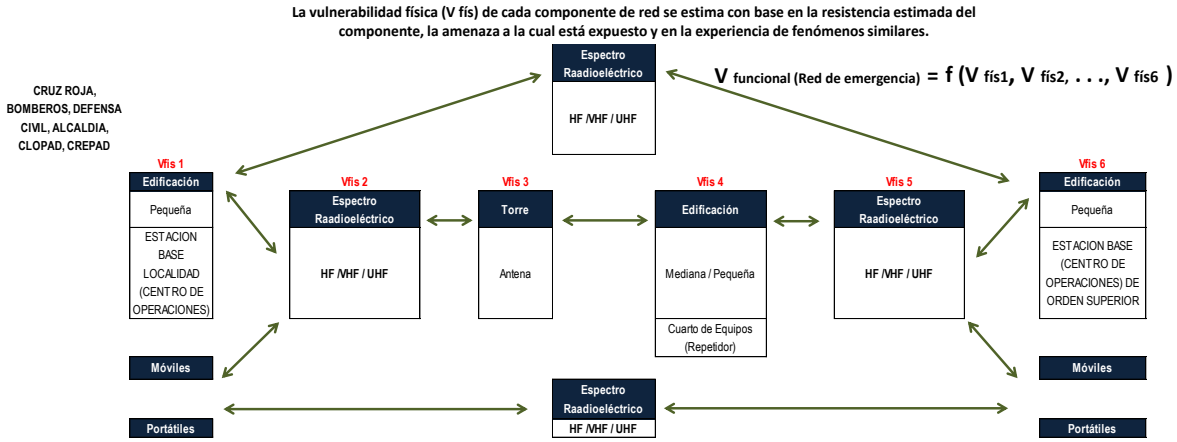
La Figura 85 ilustra los componentes de red básicos considerados en el modelo para la vulnerabilidad funcional de las redes de emergencia y la Figura 86 permite ver las relaciones funcionales de manera desagregada.

Figura 85. Esquema de red agregado de las redes de emergencia



Fuente: CINTEL

Figura 86. Esquema funcional general de las redes de emergencia



Fuente: CINTEL

5.4.12 Redes de Telemetría

Las redes de telemetría como ya se ha mencionado son utilizadas para monitorear de manera permanente y en tiempo real los diferentes fenómenos asociados con los eventos naturales desastrosos; estas redes

son inalámbricas y la gran mayoría se soporta en redes satelitales (algunas hacen uso de redes de radio o de redes celulares).

La vulnerabilidad funcional, se modela en función de los elementos específicos básicos utilizados para la obtención de datos en un punto de medida determinado de un municipio específico. La vulnerabilidad funcional de este servicio para un punto de medida dado, será igual a la vulnerabilidad del elemento con mayor vulnerabilidad presente en la cadena de telemetría. La vulnerabilidad funcional de un punto de medida, basado en las vulnerabilidades físicas de cada uno de sus componentes es:

5.4.12.1 HUB

- Vulnerabilidad de equipos ante diferentes amenazas naturales: HUB **(Fila 8, VFIS TELEMETRÍA, VER Archivo Excel en CD)**
- Vulnerabilidad de la conectividad con los gabinetes de medición ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 12 y Fila 13, VFIS TELEMETRÍA).**
- Vulnerabilidad de la conectividad con el elemento de orden superior alternativo ante diferentes amenazas naturales: Redes subterráneas de fibra óptica[56]. **(Fila 15, VFIS TELEMETRÍA).**
- La vulnerabilidad del HUB ante fallas del suministro de energía:
    - Si el HUB posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS TELEMETRÍA)**

[56]Se toma la vulnerabilidad de la fibra óptica subterránea ya que esta conectividad se realizaría en un ambiente urbano, que utiliza normalmente fibra subterránea.

- Si el HUB posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 8G, VFIS TELEMETRÍA)**
- Si el HUB NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS TELEMETRÍA)**

5.4.12.2 Elemento de orden superior alternativo

- Vulnerabilidad de equipos ante diferentes amenazas naturales: Elemento de orden superior **(Fila 8, VFIS TELEMETRÍA, VER Archivo Excel en CD)**
- Vulnerabilidad de la conectividad con los gabinetes de medición ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 12 y Fila 13, VFIS TELEMETRÍA).**
- Vulnerabilidad de la conectividad con el HUB ante diferentes amenazas naturales: Redes subterráneas de fibra óptica[57]. **(Fila 15, VFIS TELEMETRÍA).**
- La vulnerabilidad del elemento de orden superior alternativo ante fallas del suministro de energía:
  - Si el elemento de orden superior alternativo posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 8F, VFIS TELEMETRÍA)**
  - Si el elemento de orden superior alternativo posee energía de respaldo con autonomía menor a 24 horas,

[57]Se toma la vulnerabilidad de la fibra óptica subterránea ya que esta conectividad se realizaría en un ambiente urbano, que utiliza normalmente fibra subterránea.

se considera de media vulnerabilidad. **(Celda 8G, VFIS TELEMETRÍA)**

- Si el elemento de orden superior alternativo NO posee energía de respaldo (NO ES LO NORMAL), se considera de alta vulnerabilidad. **(Celda 8H, VFIS TELEMETRÍA)**

5.4.12.3 Gabinete de medición

- Vulnerabilidad de equipos ante diferentes amenazas naturales:
  - Gabinetes de medición en pequeñas edificaciones[58] **(Fila 9, VFIS TELEMETRÍA)**
  - Gabinetes de medición al aire libre **(Fila 10, VFIS TELEMETRÍA)**
- Vulnerabilidad de la conectividad con el HUB ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 12 y Fila 13, VFIS TELEMETRÍA).**
- Vulnerabilidad de la conectividad con el elemento de orden superior ante diferentes amenazas naturales: Antenas y espectro radioeléctrico satelitales y terrestres. **(Fila 12 y Fila 13, VFIS TELEMETRÍA).**
- La vulnerabilidad del gabinete de medición ante fallas del suministro de energía:
  - Si el gabinete de medición posee energía de respaldo con autonomía mayor a 24 horas, se considera de baja vulnerabilidad. **(Celda 9F, VFIS TELEMETRÍA)**

---

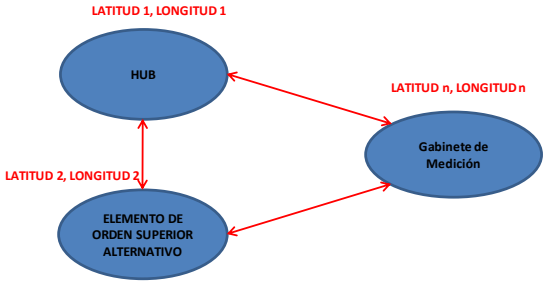
[58]Se considera que la vulnerabilidad física de gabinetes y shelters instalados en pequeñas edificaciones construidas sin apego a normas antisísmicas es mayor que la de los instalados al aire libre.

- Si el gabinete de medición posee energía de respaldo con autonomía menor a 24 horas, se considera de media vulnerabilidad. **(Celda 9G, VFIS TELEMETRÍA)**
- Si el gabinete de medición NO posee energía de respaldo, se considera de alta vulnerabilidad. **(Celda 9H, VFIS TELEMETRÍA)**

La vulnerabilidad funcional de un punto de medición específico, se calcula como el valor de la mayor vulnerabilidad funcional de los componentes básicos de la cadena de telemetría, esto es: HUB, elemento de orden superior alternativo y gabinete de medición.

La Figura 87 ilustra los componentes de red básicos considerados en el modelo para la vulnerabilidad funcional de las redes de telemetría y la **Figura 88** permite ver las relaciones funcionales de manera desagregada.

Figura 87. Esquema de red agregado de TELEMETRÍA

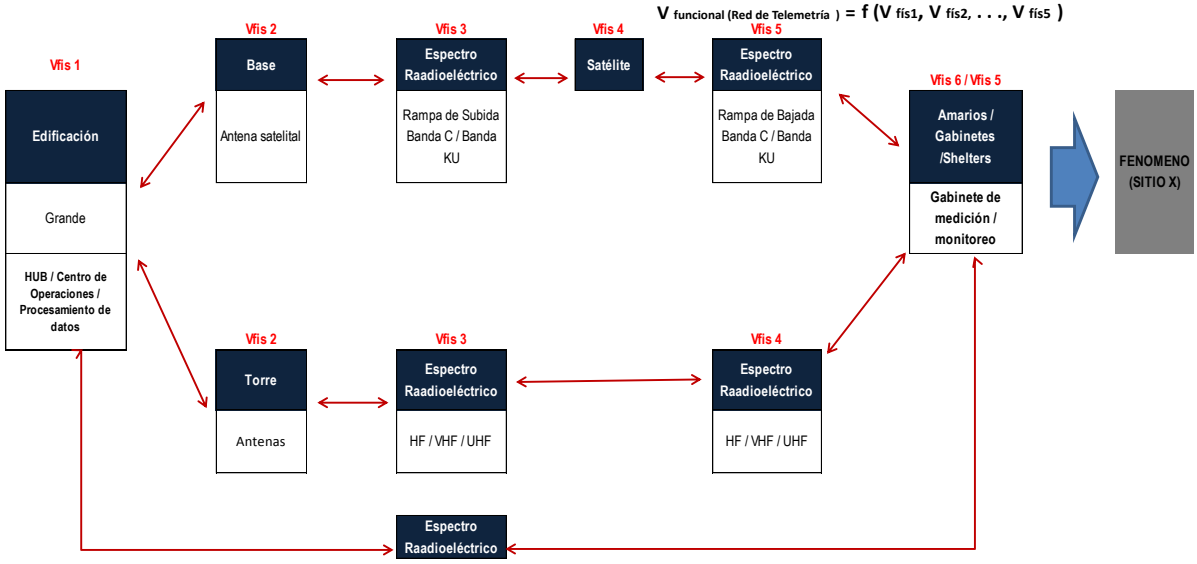


Fuente: CINTEL

Figura 88. Esquema funcional general de las redes de telemetría

La vulnerabilidad física (V fís) de cada componente de red se estima con base en la resistencia estimada del componente, la amenaza a la cual está expuesto y en la experiencia de fenómenos similares.

$$V_{\text{funcional (Red de Telemetría)}} = f(V_{\text{fís1}}, V_{\text{fís2}}, \ldots, V_{\text{fís5}})$$



Fuente: CINTEL

PÁGINA EN BLANCO

6 APLICACIÓN DEL MODELO EN LAS ZONAS Y PARA LAS AMENAZAS DEFINIDAS

De acuerdo con el modelo descrito en el numeral 0, en este capítulo se abordan los resultados obtenidos, y a partir de éstos se presentan las conclusiones y recomendaciones específicas para las zonas objeto de este estudio. Con relación a lo anterior, se aclara que dichos resultados fueron obtenidos bajo el supuesto que el evento desastroso se materializó:

- Sismo: Evento desastroso de magnitud 7 en la escala de Richter.
- Volcán: Evento desastroso de fase 5 (erupción principal).
- Tsunami: Evento desastroso de fase 6 en la escala modificada SIEBERG de intensidades de Tsunamis.
- Inundación: Evento desastroso de fase 3 (Régimen de Lluvias igual o superior al Máximo anual para el departamento).

A nivel general, se concluye que actualmente no se posee la información completa requerida sobre elementos de red ubicados en las zonas de estudio, por lo cual el modelo se corrió solo con la información disponible a la fecha. Para efectos de planeación sectorial y para llevar a cabo estudios similares al presente, se recomienda que el Ministerio de TIC, materialice y ejecute las iniciativas relacionadas con el suministro de información por parte de los proveedores de redes y servicios, de tal manera que le permitan tener y mantener la información completa y actualizada sobre redes y elementos de red de telecomunicaciones en bases de datos espaciales enmarcados en las normas nacionales de metadatos e interoperabilidad y con el sistema de referencia MAGNA-SIRGAS definida por el IGAC.

6.1 EVENTO ANALIZADO: SISMO

6.1.1 Generalidades caso de estudio

- Municipio: Armenia
- Municipios y población de la zona de influencia: Armenia, capital del Quindío, cuenta con una extensión de 250 Km^2 y 272.574 habitantes[59].

6.1.2 Infraestructura de telecomunicaciones en riesgo

En las zonas de estudio solo se registró infraestructura de los servicios de radiodifusión sonora AM y FM, COMPARTEL, telefonía móvil celular y TPBCL, portador y radioaficionados.

Tabla 76. Elementos de Infraestructura en riesgo por amenaza de sismo.

SERVICIO	ELEMENTO DE RED	ARMENIA									
		Población: 272,574 Habitantes									
		TOTAL ELEMENTOS		ELEMENTOS EN RIESGO		RIESGO BAJO		RIESGO MEDIO		RIESGO ALTO	
		No.	%	No.	%	No.	%	No.	%	No.	%
RADIODIFUSION AM	Estudios	7	100%	7	100%	0	0%	6	86%	1	14%
	Transmisores	1	100%	1	100%	0	0%	0	0%	1	100%
RADIODIFUSION FM	Estudios	6	100%	6	100%	0	0%	5	83%	1	17%
	Transmisores	3	100%	2	67%	0	0%	0	0%	2	67%
COMPARTEL	Puntos	8	100%	8	100%	0	0%	1	13%	7	88%
TMC E	CELDAS	76	100%	69	91%	0	0%	9	12%	60	79%
TPBCL E INTERNET FIJO xDSL	Sistema de Conmutación de Servicio al Municipio	10	100%	10	100%	0	0%	0	0%	10	100%
	Elemento de Orden Superior	3	100%	3	100%	0	0%	3	100%	0	0%
PORTADOR	Nodo de servicio al Municipio	1	100%	1	100%	0	0%	0	0%	1	100%
RADIOAFICIONADOS	Radioaficionados	30	100%	30	100%	0	0%	0	0%	30	100%

Fuente: CINTEL

59 Fuente DANE y portal de la alcaldía de Armenia.

6.1.2.1 Radiodifusión Sonora

La aplicación del modelo arrojó como resultado que 6 estudios de radiodifusión sonora equivalentes al 86% presentan riesgo medio y 1 correspondiente al 14% presenta riesgo alto; en el caso de los estudios de radiodifusión sonora en FM, 5 de ellos correspondientes al 83% presentan riesgo medio y 1 estudio presenta alto riesgo. En relación con los transmisores, en AM 1 de estos presenta alto riesgo al igual que dos transmisores de FM.

Por lo anterior, se recomienda que se lleve a cabo un estudio específico de vulnerabilidad de estos elementos y se tomen las medidas de mitigación pertinentes, las cuales pueden ser la disminución de la exposición reubicándolos en zonas seguras o el empleo de técnicas de construcción pertinentes y buenas prácticas mencionadas en el 7. La reubicación de transmisores y estudios está sujeta a los planes técnicos de AM y FM, a las coberturas esperadas y al rediseño de los sitios de transmisión con relación a los equipos de transmisión y a los sistemas radiantes.

6.1.2.2 COMPARTEL

En la zona de estudio, se encuentran instalados 8 puntos COMPARTEL, de los cuales 7 se encuentran alto riesgo y 1 en riesgo medio, dada la alta vulnerabilidad de las edificaciones ante sismos de esta magnitud. Por esta razón, se recomienda que se acometa un estudio específico de vulnerabilidad de estos elementos y se tomen las medidas de mitigación pertinentes, las cuales pueden ser la disminución de la exposición, reubicándolos en zonas seguras o el empleo de técnicas de construcción pertinentes y buenas prácticas mencionadas en el numeral 7. En este caso, es importante mencionar que los puntos COMPARTEL cumplen una función de conectividad para los habitantes vecinos de las zonas donde se

encuentran instalados, es decir que la reubicación tiene la limitante de seguir prestando los servicios de conectividad en las zonas donde actualmente se encuentran instalados y la reubicación tendría que darse dentro de la misma zona, la cual probablemente en muchos de los casos esté sometida a los mismos grados de amenaza por sismo. Es prudente entonces, que las soluciones finales consulten las decisiones de reasentamiento de la población estructuradas para enfrentar de manera general estas amenazas, tanto por el Gobierno central como por las municipalidades.

6.1.2.3 Telefonía Móvil

Para la zona de estudio, se encuentran instaladas 76 celdas de las cuales el 79% se encuentran en alto riesgo y el 12% se encuentran en riesgo medio, dada la alta vulnerabilidad de las edificaciones ante sismos de esta magnitud. De acuerdo con lo anterior, se recomienda que se acometa un estudio específico de vulnerabilidad de estos elementos y se tomen las medidas de mitigación pertinentes, las cuales pueden incluir la disminución de la exposición, reubicándolos en zonas seguras o el empleo de técnicas de construcción pertinentes y buenas prácticas mencionadas en el numeral 7.

En este caso, es importante mencionar que la red de acceso de celular se instala para cubrir las necesidades específicas de una población dentro del área de cobertura de cada una de las celdas, es decir, que la reubicación tiene la limitante de seguir prestando los servicios de telefonía móvil celular en las zonas donde actualmente se encuentran instaladas las celdas y su reubicación tendría que darse garantizando la cobertura de la misma zona, la cual probablemente en muchos de los casos esté sometida a los mismos grados de amenaza por sismo.

Es prudente, entonces, que las soluciones finales consulten las decisiones de reasentamiento de la población estructuradas para enfrentar de manera

general estas amenazas, tanto por el gobierno central como por las municipalidades.

6.1.2.4 Telefonía Pública Básica Conmutada e INTERNET fijo xDSL

En la zona de estudio se presta el servicio a través de 10 sistemas de conmutación (centrales de conmutación, concentradores, entre otros), de los cuales el 100% presentan alto riesgo, y tres elementos de orden superior al cual están conectados, presentan riesgo medio, dada la alta vulnerabilidad de las edificaciones ante sismos de esta magnitud, así como las altas probabilidades de daño de las redes subterráneas ante un sismo de esta magnitud. Por esta razón, se recomienda que se acometa un estudio específico de vulnerabilidad de estos elementos y se tomen las medidas de mitigación pertinentes, las cuales pueden ser la disminución de la exposición reubicándolos en zonas seguras o el empleo de técnicas de construcción pertinentes y buenas prácticas mencionadas en el numeral 7. En este caso, es importante mencionar que los sistemas de conmutación y las redes externas se instalan para cubrir las necesidades específicas de una población dentro de su área de cobertura, es decir, que la reubicación tiene la limitante de seguir prestando los servicios de TPBC en las zonas donde actualmente se encuentran instalados los sistemas de conmutación, y el rediseño para disminuir la vulnerabilidad ante sismos implicaría cambios relevantes en la infraestructura. Es prudente, entonces, que las soluciones finales consulten las decisiones de reasentamiento de la población estructuradas para enfrentar de manera general estas amenazas, tanto por el Gobierno central como por las municipalidades.

6.1.2.5 Servicio Portador

En la zona de estudio se presta el servicio portador y un elemento se encuentra en alto riesgo dada la alta vulnerabilidad de las edificaciones, así como las altas probabilidades de daño de las redes ante un sismo de esta magnitud. Por esta razón, se recomienda acometer un estudio específico de vulnerabilidad de estos elementos y tomar las medidas de mitigación pertinentes, las cuales pueden ser la disminución de la exposición reubicándolos en zonas seguras o el empleo de técnicas de construcción pertinentes y buenas prácticas mencionadas en el numeral 7.

En este caso, es importante mencionar que los elementos de infraestructura, incluyendo las redes externas, se instalan para cubrir las necesidades específicas de una población dentro del área, es decir, que la reubicación tiene la limitante de seguir prestando los servicios en las zonas donde actualmente se encuentran instalados dichos elementos, y el rediseño para disminuir la vulnerabilidad ante sismos implicaría cambios relevantes en la infraestructura.

Es prudente, entonces, que las soluciones finales consulten las decisiones de reasentamiento de la población estructuradas para enfrentar de manera general estas amenazas, tanto por el Gobierno central como por las municipalidades.

6.1.2.6 Radioaficionados

Para la zona de estudio se encuentran registrados 30 radioaficionados, de los cuales dieciséis, el 100%, están en alto riesgo. Tomando en consideración que los radioaficionados, como ya se ha mencionado, tienen su estación instalada en sus casas de habitación, las medidas de mitigación del riesgo de estas instalaciones están enmarcadas dentro de las decisiones

de reasentamiento de la población o cualquiera otra que se estructure para enfrentar de manera general estas amenazas, tanto por el Gobierno central como por las municipalidades.

6.2 EVENTO ANALIZADO: VOLCÁN MACHÍN

6.2.1 Generalidades caso de estudio

- Municipio: Cajamarca
- Población de la zona de influencia:

Tabla 77. Zona de Influencia del estudio para volcán

Departamento	Municipio	Población (núm. de hab)	Extensión (km^2)
Quindío	Armenia	272.574	250
Quindío	Calarcá	71.605	219.23
Tolima	Cajamarca	19501	520

Fuente: DANE y portal de los municipios

6.2.2 Infraestructura de telecomunicaciones en riesgo

Se registró en las zonas de estudio infraestructura de los servicios de radiodifusión sonora AM y FM, COMPARTEL, telefonía móvil celular, televisión radiodifundida, TPBCL, portador, radioaficionados y telemetría.

Tabla 78. Elementos de Infraestructura en riesgo por amenaza de volcán.

SERVICIO	ELEMENTO DE RED	TOTAL									
		TOTAL ELEMENTOS		ELEMENTOS EN RIESGO		RIESGO BAJO		RIESGO MEDIO		RIESGO ALTO	
		No.	%	No.	%	No.	%	No.	%	No.	%
RADIODIFUSION AM	Estudios	9	100%	9	100%	9	100%	0	0%	0	0%
	Transmisores	9	100%	9	100%	6	67%	3	33%	0	0%
RADIODIFUSION FM	Estudios	16	100%	16	100%	13	81%	1	6%	2	13%
	Transmisores	14	100%	14	100%	11	79%	3	21%	0	0%
COMPARTEL	Puntos	269	100%	269	100%	105	39%	13	5%	151	56%
TMC E INTERNET MOVIL	CELDAS	215	100%	215	100%	147	68%	45	21%	23	11%
TPBCL E INTERNET FIJO xDSL	Sistema de Conmutación de Servicio al Municipio	34	100%	34	100%	27	79%	0	0%	7	21%
	Elemento de Orden Superior	11	100%	11	100%	9	82%	0	0%	2	18%
TELEVISION RADIODIFUNDIDA	Transmisores	65	100%	65	100%	57	88%	5	8%	3	5%
PORTADOR	Nodo Alternativo de Agregación Nacional	1	100%	1	100%	1	100%	0	0%	0	0%
RADIOAFICIONADOS	Radioaficionados	75	100%	40	53%	40	53%	0	0%	0	0%
TELEMETRIA	Gabinetes de Medición	3	100%	3	100%	2	67%	1	33%	0	0%

Fuente: CINTEL

6.2.2.1 Radiodifusión sonora

Para el caso de radiodifusión sonora (AM & FM), el modelo arrojó como resultado que en la zona de influencia del Volcán Machín se reportaron en total 25 estudios y 23 transmisores. De estos elementos, solo 2 estudios de FM se encuentran sometidos a un riesgo alto principalmente por la ubicación los mismos en una zona de amenaza por proyectiles balísticos del volcán ante la cual estos elementos son altamente vulnerables.

Adicional a esto, los elementos ubicados en riesgo medio y bajo se encuentran principalmente amenazados por ceniza, en donde dependiendo su cercanía al volcán, la vulnerabilidad está dada por la afectación que el peso de la misma puede ocasionar sobre la infraestructura. En este sentido, se recomienda realizar un estudio específico de vulnerabilidad de los elementos y tomar las medidas de mitigación pertinentes, las cuales pueden ser la disminución de la exposición de los elementos en áreas donde no exista amenaza o la misma se presente en un grado menor, teniendo en cuenta que ella debe estar en capacidad de enfrentar la amenaza a la que se encuentre sometida.

Así mismo, es necesario tener en cuenta que la reubicación de transmisores y estudios está sujeta a los planes técnicos de AM y FM, a las coberturas esperadas y al rediseño de los sitios de transmisión con relación a los equipos de transmisión y a los sistemas radiantes.

6.2.2.2 COMPARTEL

Para el caso de los puntos COMPARTEL, se encontró que en el área de influencia del Volcán Machín hay un total de 269 puntos en riesgo, de los cuales el 57%, es decir 151, se encuentran en riesgo alto. Analizando este grupo de 151 puntos COMPARTEL, es posible identificar que todos ellos se

encuentran sometidos a la amenaza de lahar ante la cual toda la infraestructura de telecomunicaciones es altamente vulnerable. Aunque también se encontraron elementos sometidos a amenaza por ceniza, piroclásto y balístico, dicha amenaza fue baja, permitiendo catalogar a esos puntos COMPARTEL en un nivel de riesgo entre bajo y medio.

A partir de este análisis, se propone realizar un estudio de vulnerabilidad específico para cada punto COMPARTEL que permita tomar las medidas de mitigación pertinentes. Dado que los puntos COMPARTEL cumplen una función de conectividad para los habitantes vecinos de las zonas donde se encuentran instalados, una medida de mitigación asociada a la reubicación tiene la limitante de seguir prestando los servicios de conectividad en las zonas donde actualmente se encuentran instalados por lo cual la reubicación tendría que darse dentro de la misma zona, la cual en muchos de los casos está sometida a las mismas amenazas del volcán.

En este caso es prudente, entonces, que las soluciones finales consulten las decisiones de reasentamiento de la población estructuradas para enfrentar de manera general estas amenazas, tanto por el Gobierno central como por las municipalidades.

6.2.2.3 Telefonía Móvil

En cuanto a la telefonía móvil, se encontraron dentro de la zona de influencia del Volcán Machín 215 celdas en riesgo, de las cuales el 11% (23 celdas) se encuentran en riesgo alto. Respecto a estas 23 celdas, cabe mencionar que 9 de ellas están sometidas a todas las amenazas analizadas para el caso de volcán (ceniza, lahar, piroclastos y balísticos). En todas las celdas ubicadas en riesgo alto la principal amenaza es lahar, ante la cual la infraestructura de telecomunicaciones es altamente vulnerable.

En cuanto al resto de las celdas, aquellas ubicadas zonas de riesgo medio se encuentran afectadas principalmente por la afectación por peso de ceniza y aquellas en riesgo bajo por afectación en funcionamiento que causa la nube de ceniza. De acuerdo con los resultados encontrados, se recomienda realizar un estudio específico de vulnerabilidad de estos elementos que permita tomar las medidas de mitigación pertinentes, llamando sobretodo la atención en aquellas celdas que se encuentran sometidas a las cuatro a amenazas de volcán consideradas en este estudio.

Una alternativa, es la disminución de la exposición a las distintas amenazas del volcán por medio de la reubicación en zonas más seguras. En este caso es importante mencionar que la red de acceso de celular se instala para cubrir las necesidades específicas de una población dentro del área de cobertura de cada una de las celdas, es decir que la reubicación tiene la limitante de seguir prestando los servicios de telefonía móvil celular en las zonas donde actualmente se encuentran instaladas las celdas y su reubicación tendría que darse garantizando la cobertura de la misma zona, la cual probablemente en muchos de los casos este sometida a las mismas amenazas del volcán.

Es prudente, entonces, que las soluciones finales consulten las decisiones de reasentamiento de la población estructuradas para enfrentar de manera general estas amenazas, tanto por el Gobierno central como por las municipalidades.

6.2.2.4 Telefonía Pública Básica Conmutada e INTERNET fijo xDSL

En cuanto a TPBCL, en la zona de estudio se lograron identificar 34 sistemas de conmutación y 11 elementos de orden superior sometidos a riesgo, de los cuales 7 (21%) sistemas de conmutación y 2 (18%) elementos de orden superior se encuentran en riesgo alto.

En el caso de los sistemas de conmutación, la principal amenaza a 6 de los elementos es el lahar y para uno, los proyectiles balísticos, amenazas ante las cuales los sistemas de conmutación son altamente vulnerables. Por su parte, de los elementos de orden superior, el que se encuentra ubicado en el municipio de Cajamarca se encuentra sometido a las 4 amenazas y el ubicado en el municipio de Espinal se encuentra sometido a lahar. Al igual que para los sistemas de conmutación, los elementos de orden superior son altamente vulnerables ante el lahar.

El resto de elementos sometidos a riesgo bajo están amenazados por ceniza sin embargo su vulnerabilidad en este caso es baja. En el caso de TPBCL dada la alta vulnerabilidad de los equipos electrónicos de telecomunicaciones a amenazas como lahar y piroclastos, se recomienda desarrollar un estudio específico de vulnerabilidad de estos elementos y tomar las medidas de mitigación pertinentes, las cuales pueden ser la disminución de la exposición a cada una de las amenazas reubicándolos en zonas seguras, el rediseño de las redes externas o el empleo de técnicas de construcción menos vulnerables.

En este caso, es importante mencionar que los sistemas de conmutación y las redes externas se instalan para cubrir las necesidades específicas de una población dentro del área de cobertura de estos, es decir que la reubicación tiene la limitante de seguir prestando los servicios de TPBC en las zonas donde actualmente se encuentran instalados los sistemas de conmutación, y el rediseño para disminuir la exposición a la amenaza volcánica implicaría cambios en tecnología, ya que lo recomendable sería la utilización de accesos inalámbricos (WLL).

Es prudente, entonces, que las soluciones finales consulten las decisiones de reasentamiento de la población estructuradas para enfrentar de manera

general estas amenazas, tanto por el Gobierno central como por las municipalidades.

6.2.2.5 Servicio Portador

Para el caso de portador, se encontró un único elemento sometido a amenaza volcánica en riesgo bajo. En este caso es importante mencionar que los elementos de infraestructura incluyendo las redes externas se instalan para cubrir las necesidades específicas de una población dentro del área, es decir que la reubicación tiene la limitante de seguir prestando los servicios en las zonas donde actualmente se encuentran instalados dichos elementos, y el rediseño para disminuir la vulnerabilidad implicaría cambios relevantes en la infraestructura.

Es prudente, entonces, que las soluciones finales consulten las decisiones de reasentamiento de la población estructuradas para enfrentar de manera general estas amenazas, tanto por el Gobierno central como por las municipalidades.

6.2.2.6 Radioaficionados

En la zona de estudio se encuentran registrados 75 radioaficionados, de los cuales 40, equivalentes al 53%, se encuentran en riesgo bajo. Tomando en consideración que los radioaficionados, como ya se ha mencionado, tienen su estación instalada en sus casas de habitación, las medidas de mitigación del riesgo de estas instalaciones, están enmarcadas dentro de las decisiones de reasentamiento de la población o cualquiera otra que se estructure para enfrentar de manera general estas amenazas, tanto por el Gobierno central como por las municipalidades

6.2.2.7 Telemetría

En telemetría se encuentra en total 3 gabinetes de medición sujetos a amenaza por volcán, sin embargo ninguno de ellos está sometido a riesgo alto.

6.3 EVENTO ANALIZADO: TSUNAMI

6.3.1 Generalidades caso de estudio

- Municipio: Tumaco
- Población de la zona de influencia[60]: Tumaco es un municipio de Nariño con una extensión de 3.800 Km^2 y 161.490 habitantes.

6.3.2 Infraestructura de telecomunicaciones en riesgo

Se registró en las zonas de estudio, infraestructura de los servicios de radiodifusión sonora AM y FM, COMPARTEL, telefonía móvil celular y TPBCL, televisión radiodifundida y radioaficionados.

Tabla 79. Elementos de Infraestructura en riesgo por amenaza de tsunami.

SERVICIO	ELEMENTO DE RED	TOTAL									
		TOTAL ELEMENTOS		ELEMENTOS EN RIESGO		RIESGO BAJO		RIESGO MEDIO		RIESGO ALTO	
		No.	%	No.	%	No.	%	No.	%	No.	%
RADIODIFUSION AM	Estudios	1	100%	1	100%	0	0%	0	0%	1	100%
	Transmisores	1	100%	1	100%	0	0%	0	0%	1	100%
RADIODIFUSION FM	Estudios	1	100%	1	100%	0	0%	0	0%	1	100%
	Transmisores	1	100%	1	100%	0	0%	0	0%	1	100%
COMPARTEL	Puntos	44	100%	28	64%	0	0%	0	0%	28	64%
TMC E INTERNET MOVIL	CELDAS	22	100%	20	91%	0	0%	0	0%	20	91%
TPBCL E INTERNET FIJO xDSL	Sistema de Conmutación de Servicio al Municipio	12	100%	2	17%	0	0%	0	0%	2	17%
	Elemento de Orden Superior	3	100%	1	33%	0	0%	0	0%	1	33%
TELEMETRIA	Gabinetes de Medición	3	100%	1	33%	0	0%	0	0%	1	33%

Fuente: CINTEL

6.3.2.1 Radiodifusión Sonora

Para el caso de radiodifusión sonora (AM & FM) el modelo arrojó como resultado que en la zona de estudio se reportaron en total 2 estudios y 2

[60] **Fuente DANE y portal de la alcaldía de Tumaco.**

transmisores, los cuales se encuentran en riego alto debido a los tres factores, golpe de ola, fuerzas laterales e inundación. En este sentido, se recomienda realizar un estudio específico de vulnerabilidad de los elementos y tomar las medidas de mitigación pertinentes, las cuales pueden ser la disminución de la exposición de los elementos en áreas donde no exista amenaza o la misma se presente en un grado menor teniendo en cuenta que ella debe estar en capacidad de enfrentar la amenaza a la que se encuentre sometida.

Así mismo, es necesario tener en cuenta que la reubicación de transmisores y estudios está sujeta a los planes técnicos de AM y FM, a las coberturas esperadas y al rediseño de los sitios de transmisión con relación a los equipos de transmisión y a los sistemas radiantes.

6.3.2.2 COMPARTEL

Para el caso de los puntos COMPARTEL, se encontró que en el área hay un total de 44 puntos, de los cuales 28 se encuentran en riesgo alto. Analizando este grupo, es posible identificar que todos ellos se encuentran sometidos a la amenaza debido a golpe de ola, fuerzas laterales e inundación. A partir de este análisis, se recomienda realizar un estudio de vulnerabilidad específico para los puntos COMPARTEL que permita tomar las medidas de mitigación pertinentes.

Dado que los puntos COMPARTEL cumplen una función de conectividad para los habitantes vecinos de las zonas donde se encuentran instalados, una medida de mitigación asociada a la reubicación tiene la limitante de seguir prestando los servicios de conectividad en las zonas donde actualmente se encuentran instalados, por lo cual, la reubicación tendría que darse dentro de la misma zona, que en muchos de los casos está sometida a las mismas amenazas por tsunami.

En este caso es prudente, entonces, que las soluciones finales consulten las decisiones de reasentamiento de la población estructuradas para enfrentar de manera general estas amenazas, tanto por el Gobierno central como por el municipio.

6.3.2.3 Telefonía Móvil

En cuanto a la telefonía móvil, se encontraron dentro de la zona 22 celdas en riesgo, de las cuales el 91% (20 celdas), se encuentran en riesgo alto. Respecto a estas 20 celdas, se menciona que están sometidas a todas las amenazas analizadas: golpe de ola, fuerzas laterales e inundación. De acuerdo con los resultados encontrados, se recomienda realizar un estudio específico de vulnerabilidad de estos elementos que permita tomar las medidas de mitigación pertinentes, llamando sobretodo la atención en aquellas celdas que se encuentran sometidas a las tres amenazas consideradas en este estudio.

Una alternativa es la disminución de la exposición a las distintas amenazas por medio de la reubicación en zonas más seguras. En este caso es importante mencionar que la red de acceso de celular se instala para cubrir las necesidades específicas de una población dentro del área de cobertura de cada una de las celdas, es decir que la reubicación tiene la limitante de seguir prestando los servicios de telefonía móvil celular en las zonas donde actualmente se encuentran instaladas las celdas y su reubicación tendría que darse garantizando la cobertura de la misma zona, la cual probablemente en muchos de los casos este sometida a las mismas amenazas.

En este sentido, es prudente que las soluciones finales consulten las decisiones de reasentamiento de la población estructuradas para enfrentar de manera general estas amenazas, tanto por el Gobierno central como por el municipio.

6.3.2.4 Telefonía Pública Básica Conmutada e INTERNET fijo xDSL

En cuanto a TPBCL, en la zona de estudio se lograron identificar 12 sistemas de conmutación y 3 elementos de orden superior sometidos a riesgo, de los cuales 2 (17%) sistemas de conmutación y 1 (33%) elemento de orden superior se encuentran en riesgo alto debido a la amenaza por inundación y fuerzas laterales.

En este caso, dada la alta vulnerabilidad de los equipos electrónicos de telecomunicaciones a las inundaciones y de las edificaciones ante fuerzas laterales, así como de las redes subterráneas y las altas probabilidades de inundación de las zonas, se recomienda llevar a cabo un estudio específico de vulnerabilidad de estos elementos y tomar las medidas de mitigación pertinentes, las cuales pueden ser la disminución de la exposición a la amenaza reubicándolos en zonas seguras.

Es importante mencionar, que los sistemas de conmutación y las redes externas se instalan para cubrir las necesidades específicas de una población dentro del área de cobertura de estos, es decir, que la reubicación tiene la limitante de seguir prestando los servicios de TPBC en las zonas donde actualmente se encuentran instalados los sistemas de conmutación, y el rediseño para disminuir la exposición a inundaciones implicaría cambios en tecnología, ya que lo recomendable sería la utilización de accesos inalámbricos (WLL).

Es prudente, entonces, que las soluciones finales consulten las decisiones de reasentamiento de la población estructuradas para enfrentar de manera general estas amenazas, tanto por el Gobierno central como por el municipio.

6.3.2.5 Telemetría

En telemetría se encuentran en la zona de estudio en total 3 gabinetes de medición. De éstos, 1 está sujeto a riesgo alto por fuerza lateral e inundación. A partir de este análisis, se recomienda realizar un estudio de vulnerabilidad específico de forma que permita tomar las medidas de mitigación pertinentes para garantizar la continua operación ante un evento de tsunami en la zona.

6.4 EVENTO ANALIZADO: INUNDACIÓN

6.4.1 Generalidades caso de estudio

- Zona: Mojana Sucreña

- Municipios y población de la zona de influencia:

Tabla 80. Municipio de la zona de estudio de inundación.

DEPARTAMENTO	MUNICIPIO	POBLACIÓN (núm. hab)	EXTENSIÓN (km^2)
BOLÍVAR	ACHI	19.629	1.471
BOLÍVAR	MAGANGUE	121.085	1.382
BOLÍVAR	MOMPOS	41.326	645,37
BOLÍVAR	MONTECRISTO	11.212	2.089
BOLÍVAR	PINILLOS	22.714	75.346,8
BOLÍVAR	SAN JACINTO DEL CAUCA	7.204	549
BOLÍVAR	TIQUISIO (Puerto Rico)	18.714	758
CÓRDOBA	AYAPEL	42.629	2.098
CÓRDOBA	BUENAVISTA	19.076	847
CÓRDOBA	CHINÚ	43.331	624
CÓRDOBA	PLANETA RICA	61.570	1.148,4
CÓRDOBA	PUEBLO NUEVO	31.754	715
CÓRDOBA	SAHAGÚN	86.189	992
SUCRE	CAIMITO	10.960	406,6
SUCRE	EL ROBLE	8.469	206.095
SUCRE	GUARANDÁ	15.080	373,4
SUCRE	LA UNIÓN	10.279	234,39
SUCRE	MAJAGUAL	31.213	826
SUCRE	SAN BENITO ABAD	22.579	1592
SUCRE	SAN MARCOS	50.336	534,54
SUCRE	SUCRE	21.716	1139

Fuente DANE y portal de las alcaldías municipales.

6.4.2 Infraestructura de telecomunicaciones en riesgo

Se registró en la zona de estudio, infraestructura de los servicios de radiodifusión sonora AM y FM, COMPARTEL, telefonía móvil celular y TPBCL, televisión radiodifundida y radioaficionados.

Tabla 81. Elementos de Infraestructura en riesgo por amenaza de inundación

SERVICIO	ELEMENTO DE RED	TOTAL									
		TOTAL ELEMENTOS		ELEMENTOS EN RIESGO		RIESGO BAJO		RIESGO MEDIO		RIESGO ALTO	
		No.	%	No.	%	No.	%	No.	%	No.	%
RADIODIFUSION AM	Estudios	2	100%	2	100%	0	0%	0	0%	2	100%
	Transmisores	3	100%	3	100%	0	0%	0	0%	3	100%
RADIODIFUSION FM	Estudios	17	100%	11	65%	0	0%	0	0%	11	65%
	Transmisores	17	100%	11	65%	0	0%	0	0%	11	65%
COMPARTEL	Puntos	1068	100%	585	55%	0	0%	0	0%	585	55%
TMC E INTERNET MOVIL	CELDAS	272	100%	272	100%	0	0%	0	0%	272	100%
TPBCL E INTERNET FIJO xDSL	Sistema de Conmutación de Servicio al Municipio	51	100%	34	67%	0	0%	0	0%	34	67%
	Elemento de Orden Superior	6	100%	4	67%	0	0%	0	0%	4	67%
TELEVISION RADIODIFUNDIDA	Transmisores	20	100%	8	40%	0	0%	0	0%	8	40%
RADIOAFICIONADOS	Radioaficionados	20	100%	16	80%	0	0%	0	0%	16	80%

Fuente: CINTEL

6.4.2.1 Radiodifusión sonora

El modelo arrojó como resultado que trece (13) estudios de radiodifusión sonora (AM & FM) de los diecinueve (19) estudios instalados en los departamentos de Sucre, Bolívar y Córdoba, equivalentes al 69%, presentan alto riesgo y que catorce (14) de los veinte (20) transmisores de radiodifusión sonora (AM y FM) ubicados en la zona, equivalentes al 70%, tienen igualmente un alto riesgo, dada la alta vulnerabilidad de los equipos electrónicos de telecomunicaciones a las inundaciones y las altas probabilidades de inundación de las zonas.

Por esta razón, se recomienda acometer un estudio específico de vulnerabilidad de estos elementos y tomar las medidas de mitigación pertinentes, las cuales pueden ser la disminución de la exposición a la inundación reubicándolos en zonas seguras no sujetas a inundación o el empleo de técnicas de construcción de tipo flotante. La reubicación de

transmisores y estudios está sujeta a los planes técnicos de AM y FM, a las coberturas esperadas y al rediseño de los sitios de transmisión con relación a los equipos de transmisión y a los sistemas radiantes.

6.4.2.2 COMPARTEL

En las zonas de estudio de los departamentos de Sucre, Bolívar y Córdoba, se encuentran instalados 1.068 puntos COMPARTEL, de los cuales 585 equivalentes a un 55% presentan alto riesgo, dada la alta vulnerabilidad de los equipos electrónicos de telecomunicaciones a las inundaciones y las altas probabilidades de inundación de las zonas.

Por esta razón, se recomienda que se acometa un estudio específico de vulnerabilidad de estos elementos y se tomen las medidas de mitigación pertinentes, las cuales pueden ser la disminución de la exposición a la inundación reubicándolos en zonas seguras no sujetas a inundación o el empleo de técnicas de construcción de tipo flotante. En este caso, es importante mencionar que los puntos COMPARTEL cumplen una función de conectividad para los habitantes vecinos de las zonas donde se encuentran instalados, es decir que la reubicación tiene la limitante de seguir prestando los servicios de conectividad en las zonas donde actualmente se encuentran instalados y la reubicación tendría que darse dentro de la misma zona, la cual probablemente en muchos de los casos este sometida a los mismos grados de amenaza por inundación.

Es prudente, entonces, que las soluciones finales consulten las decisiones de reasentamiento de la población estructuradas para enfrentar de manera general estas amenazas, tanto por el gobierno central como por las municipalidades.

6.4.2.3 Telefonía Móvil Celular e INTERNET móvil

En las zonas de estudio de los departamentos de Sucre, Bolívar y Córdoba, se encuentran instaladas 129 celdas y la totalidad (100%) presentan alto riesgo, dada la alta vulnerabilidad de los equipos electrónicos de telecomunicaciones a las inundaciones y las altas probabilidades de inundación de las zonas.

Por esta razón, se recomienda acometer un estudio específico de vulnerabilidad de estos elementos y tomar las medidas de mitigación pertinentes, las cuales pueden ser la disminución de la exposición a la inundación reubicándolos en zonas seguras no sujetas a inundación o el empleo de técnicas de construcción de tipo flotante. En este caso es importante mencionar que la red de acceso de celular se instala para cubrir las necesidades específicas de una población dentro del área de cobertura de cada una de las celdas, es decir que la reubicación tiene la limitante de seguir prestando los servicios de telefonía móvil celular en las zonas donde actualmente se encuentran instaladas las celdas y su reubicación tendría que darse garantizando la cobertura de la misma zona, la cual probablemente en muchos de los casos este sometida a los mismos grados de amenaza por inundación.

Es prudente, entonces, que las soluciones finales consulten las decisiones de reasentamiento de la población estructuradas para enfrentar de manera general estas amenazas, tanto por el Gobierno central como por las municipalidades.

6.4.2.4 Telefonía Pública Básica Conmutada e INTERNET fijo xDSL

El servicio en las zonas de estudio de los departamentos de Sucre, Bolívar y Córdoba, se presta a través de 51 sistemas de conmutación (centrales de

conmutación, concentradores, entre otros), de los cuales 34 presentan alto riesgo, y a través de tres elementos de orden superior al cual están conectados, los cuales (100%) presentan igualmente alto riesgo, dada la alta vulnerabilidad de los equipos electrónicos de telecomunicaciones a las inundaciones, así como de las redes subterráneas y las altas probabilidades de inundación de las zonas.

Por esta razón, se recomienda acometer un estudio específico de vulnerabilidad de estos elementos y tomar las medidas de mitigación pertinentes, las cuales pueden ser la disminución de la exposición a la inundación reubicándolos en zonas seguras no sujetas a inundación, el rediseño de las redes externas o el empleo de técnicas de construcción de tipo flotante. En este caso, es importante mencionar que los sistemas de conmutación y las redes externas se instalan para cubrir las necesidades específicas de una población dentro del área de cobertura de estos, es decir, que la reubicación tiene la limitante de seguir prestando los servicios de TPBC en las zonas donde actualmente se encuentran instalados los sistemas de conmutación, y el rediseño de las para disminuir la exposición a inundaciones implicaría cambios muy probablemente en tecnología, ya que lo recomendable sería la utilización de accesos inalámbricos (WLL).

Es prudente, entonces, que las soluciones finales consulten las decisiones de reasentamiento de la población estructuradas para enfrentar de manera general estas amenazas, tanto por el Gobierno central como por las municipalidades.

6.4.2.5 Televisión Radiodifundida

El modelo arrojó como resultado, que ocho (8) de los veinte (20) transmisores de televisión radiodifundida, instalados en los departamentos de Sucre, Bolívar y Córdoba, equivalentes al 40%, presentan alto riesgo,

dada la alta vulnerabilidad de los equipos electrónicos de telecomunicaciones a las inundaciones y las altas probabilidades de inundación de las zonas.

Por esta razón, se recomienda realizar un estudio específico de vulnerabilidad de estos elementos y tomar las medidas de mitigación pertinentes, las cuales pueden ser la disminución de la exposición a la inundación reubicándolos en zonas seguras no sujetas a inundación o el empleo de técnicas de construcción de tipo flotante. La reubicación de transmisores está sujeta al Plan de Utilización (PUF) de frecuencias de la Comisión Nacional de Televisión, a las coberturas esperadas y al rediseño de los sitios de transmisión con relación a los equipos de transmisión y a los sistemas radiantes.

6.4.2.6 Radioaficionados

En la zona de estudio en los departamentos de Sucre, Bolívar y Córdoba, se encuentran registrados veinte (20) radioaficionados, de los cuales dieciséis (16), equivalentes al 80%, se encuentran en alto riesgo. Tomando en consideración que los radioaficionados, como ya se ha mencionado, tienen su estación instalada en sus casas de habitación, las medidas de mitigación del riesgo de estas instalaciones están enmarcadas en de las decisiones de reasentamiento de la población o cualquiera otra que se estructure para enfrentar de manera general estas amenazas, tanto por el Gobierno central como por las municipalidades.

7 CONCLUSIONES Y RECOMENDACIONES PARA LA PROTECCIÓN DE LA INFRAESTRUCTURA, MEDIDAS DE MITIGACIÓN Y BUENAS PRÁCTICAS

Una vez desarrollado el modelo de análisis de vulnerabilidad y riesgo de la infraestructura de telecomunicaciones en el país ante las amenazas naturales definidas, y teniendo en cuenta los resultados presentados en este documento, se procede a recomendar algunas medidas de mitigación y a enunciar algunas de las buenas prácticas más reconocidas en este aspecto como son las aplicadas los en Estados Unidos de América y la Unión Europea.

7.1 MEDIDAS DE MITIGACIÓN

El riesgo de la infraestructura física de telecomunicaciones es una función de vulnerabilidad de los diferentes elementos que la componen y de su exposición a las amenazas, en el caso de este estudio a las amenazas naturales de sismo, volcán, tsunami e inundación.

Tomando en cuenta lo anterior, las medidas de mitigación del riesgo de la infraestructura de telecomunicaciones ante cualquier amenaza y en particular a las consideradas en este documento se deben enfocar a:

- Disminución del grado de exposición de la infraestructura, reubicándola fuera de las zonas de amenazas, en este caso de las naturales consideradas, cuando sea posible en razón de la naturaleza del servicio.
- Disminución de la vulnerabilidad de los elementos de la infraestructura de telecomunicaciones, aumentando su resistencia ante los diferentes eventos a los que pueda estar expuesta, mediante el estudio, análisis, adopción y utilización de las buenas prácticas que se recomiendan y utilizan a nivel internacional.

Por lo anterior se recomienda:

- La creación de un Comité Sectorial que acometa, de manera similar a lo que se ha realizado en Estados Unidos de América por FCC y por la Unión Europea, el estudio, análisis y adopción de las buenas prácticas para la gestión de la infraestructura de telecomunicaciones en Colombia.
- La elaboración, por parte de los prestadores de redes y servicios de comunicaciones en Colombia, de planes de mitigación y contingencia tomando en consideración las leyes y

reglamentos nacionales, las buenas prácticas aceptadas a nivel nacional e internacional, los estudios y mapas de amenazas naturales y antrópicas elaborados por las autoridades colombianas en la materia, por las entidades especializadas a nivel internacional para fenómenos específicos o desarrollados al interior de las empresas cuando éstos no estén disponibles o exista una amenaza específica.

- La identificación por parte de los prestadores de redes y servicios de comunicaciones, de los elementos de red instalados en zonas de amenaza, la cuantificación de vulnerabilidad y riesgo de su infraestructura y la reubicación de los mismos si el riesgo lo aconseja y el servicio lo permite, disminuyendo así su exposición o aumentando su resistencia a las amenazas a las que están expuestos.
- La utilización por parte de los prestadores de redes y servicios de comunicaciones, de sistemas de energía de respaldo, con la confiabilidad y autonomía necesarias para garantizar que los servicios de telecomunicaciones, ante la ocurrencia de un evento desastroso, continúen prestándose en ausencia del suministro de energía comercial por un período de tiempo suficiente, ya sea para que el suministro de energía comercial se restablezca o para que el prestador de redes y servicios de comunicaciones tome las medidas para garantizar que el sistema de respaldo de energía continúe operando mediante el adecuado abastecimiento de combustible[61].
- El diseño e implementación de una red de emergencia de amplio cubrimiento nacional, que consulte las zonas de mayores amenazas naturales y antrópicas, con tecnología

[61]Tomando en consideración desastres en la red de transporte y en la infraestructura de abastecimiento de combustible.

requerida para garantizar la interoperabilidad entre las diferentes entidades encargadas de administrar los desastres en sus diferentes fases.

- El diseño y construcción de nuevas edificaciones que albergan infraestructura de telecomunicaciones, de forma que apliquen la norma sismo resistente **NSR 10** o la que la actualice y que las existentes sean reforzadas estructuralmente de acuerdo con esta normativa.
- El establecimiento de planes de acción para la disminución de la vulnerabilidad de la infraestructura:
    - Aumentando la resistencia de las edificaciones utilizando para las nuevas construcciones la norma sismo resistente NSR 10 y realizando reforzamiento estructural para las edificaciones que ya están en funcionamiento.
    - Utilizando sistemas de respaldo de energía con la autonomía adecuada al servicio, al elemento de red específico y a su ubicación.
    - Diseñando las redes de telecomunicaciones con la redundancia y diversidad adecuada al servicio, al elemento de red específico y a su ubicación.
    - Utilizando las ventajas y facilidades tecnológicas que brindan las nuevas redes, con el fin de disminuir las probabilidades de congestión y priorizar el acceso a organismos de administración de desastres.
- La utilización por parte de los prestadores de redes y servicios de comunicaciones, de sistemas de información geográfica que sirvan para mantener actualizada la georeferenciación mediante la utilización de coordenadas WGS 84 de toda su infraestructura y que el Ministerio de las Tecnologías de la

Información y las Comunicaciones disponga del acceso cifrado a estos sistemas.

- La estructuración por parte de los prestadores de redes y servicios de comunicaciones, de bases de datos espaciales bajo estándares de interoperabilidad y estructuras de metadatos geográficos que permitan la interacción con otros sistemas internos así como con aquellos del Gobierno, con el fin de establecer planes de prevención y atención de desastres unificados.
- La utilización por parte de los prestadores de redes y servicios de comunicaciones, de la normativa nacional[62] o internacional[63] para el diseño y construcción de postes y torres de telecomunicaciones, mientras no se desarrolle una normativa propia.
- La toma de medidas tecnológicas necesarias por parte de los prestadores de redes y servicios de comunicaciones, para priorizar el acceso a entidades a cargo de la administración de desastres, utilizando las ventajas de UMTS.
- La expedición por parte del Ministerio de Tecnologías de la Información y las Comunicaciones[64], de la reglamentación dirigida a la disminución de la vulnerabilidad de la

---

62Norma NTC 1329 (Prefabricados en concreto. Postes de concreto armado para líneas aéreas de energía y telecomunicaciones).

63Normas AISC última edición, ASCE report 52, EIA/TIA 222 F (1996), ANSI/ASCE 10-90 (1991), ACI 318 última edición y la nacional NSR10 aunque no es obligatoria.

64 El Gobierno de Chile, Ministerio de Transporte y Telecomunicaciones, en noviembre de 2010, después del terremoto del 27 de febrero impulsó la promulgación de una nueva Ley que apunta a corregir las debilidades de las redes de telecomunicaciones ante catástrofes, que se revelaron en el terremoto del 27 de febrero pasado.

http://www.mtt.cl/prontus_mtt/site/artic/20101118/pags/20101118132336.html

infraestructura de telecomunicaciones ante amenazas de origen natural y antrópicas, incorporando la obligación de los prestadores de redes y servicios de comunicaciones, de adoptar buenas prácticas de aceptación internacional, tales como la implementación de sistemas de administración del riesgo, dentro de los cuales se elaboren, actualicen, se pongan en práctica y difundan al interior de los proveedores de servicios de telecomunicaciones, planes de mitigación y contingencia, con metas e indicadores que permitan su seguimiento.

- La realización de simulacros por parte de los prestadores de redes y servicios de comunicaciones, con modelos de análisis del riesgo, incorporando metodologías de árboles de decisión, con el fin de contar con planes de acción ante escenarios simulados frente a desastres naturales. Dichos simulacros deben realizarse incluso desde la planeación en el montaje o ampliación de una red, analizando cómo impactaría en el negocio ubicar un elemento de red en una zona de amenaza natural.
- La disminución de la vulnerabilidad de la infraestructura de telecomunicaciones, utilizando para la ubicación de la infraestructura no sólo criterios técnicos y de mercado en materia de telecomunicaciones, sino además información relacionada con amenazas antrópicas y naturales, mediante la utilización de estudios y mapas de amenazas desarrollados por las autoridades en la materia o en ausencia de ellos, estudios propios realizados con esta finalidad.
- La ejecución por parte de los prestadores de redes y servicios de comunicaciones, de una gestión integrada del riesgo, incorporando análisis de amenaza natural y de vulnerabilidad de los elementos de la red ante dichas amenazas, en sus programas de continuidad del negocio y recuperación ante desastres.

7.2 BUENAS PRÁCTICAS

En los anexos No. 2 y No. 3 de este documento, se relacionan algunas de las buenas prácticas voluntarias adoptadas por el Network Reliability and Interoperability Council (NRIC) de la FCC en los Estados Unidos de América y algunas otras adoptadas por la Unión Europea.

7.2.1 Buenas prácticas aplicadas en los Estados Unidos de América

Las buenas prácticas adoptadas voluntariamente en los Estados Unidos por el NRIC contemplan los aspectos básicos de las redes de telecomunicaciones. En el anexo No. 2, se incluyen algunas buenas prácticas a manera ilustrativa, relacionadas con:

- Diseño de red
- Continuidad del negocio
- Recuperación de desastres
- Edificaciones
- Suministro de energía eléctrica
- Incendios

Adicionalmente, existe un gran acervo de buenas prácticas de NCIR que se pueden consultar en:

https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm

El informe final del Network Reliability and Interoperability Council V Focus Group 2 Subcommittee 2.A de Enero de 2002, contiene la evaluación de la industria de telecomunicaciones de Estados Unidos con relación a las buenas prácticas, la cual se presenta en la tabla siguiente, de la cual se concluye que existe una gran acogida de estas prácticas en esa industria.

Tabla 82. Evaluación de las buenas prácticas por la industria americana de telecomunicaciones

ASPECTO EVALUADO	EVALUADOR	RESULTADO DE LA EVALUACIÓN
Implementación de las buenas prácticas	Proveedores de servicios (Conmutación de circuitos)	**Más del 70%** de los que respondieron han implementado el **98%** de las buenas prácticas en todo lado o en áreas críticas. **Más del 90%** de los que respondieron han implementado el 68% de las buenas prácticas en todo lado o en áreas críticas.
	Proveedores de servicios (Conmutación de paquetes)	**Más del 50%** de los que respondieron han implementado el **100%** de las buenas prácticas en todo lado o en áreas críticas. **Más del 90%** de los que respondieron han implementado el **66%** de las buenas prácticas en todo lado o en áreas críticas.
	Proveedores de equipos (Conmutación de circuitos)	**Más del 60%** de los que respondieron han implementado el **100%** de las buenas prácticas en todo lado o en áreas críticas. **Más del 90%** de los que respondieron han implementado el **74%** de las buenas prácticas en todo lado o en áreas críticas.
	Proveedores de equipos (Conmutación de paquetes)	**Más del 70%** de los que respondieron han implementado el **98%** de las buenas prácticas en todo lado o en áreas críticas. **Más del 90%** de los que respondieron han implementado el **67%** de las buenas prácticas en todo lado o en áreas críticas.
Efectividad de las	Proveedores de servicios	**Más del 60%** de los que respondieron opinan que el

ASPECTO EVALUADO	EVALUADOR	RESULTADO DE LA EVALUACIÓN
buenas prácticas	(Conmutación de circuitos)	**100%** de las buenas prácticas son efectivas. **Más del 90%** de los que respondieron opinan que el **84%** de las buenas prácticas son efectivas.
	Proveedores de servicios (Conmutación de paquetes)	**Más del 60%** de los que respondieron opinan que el **100%** de las buenas prácticas son efectivas. **Más del 90%** de los que respondieron opinan que el **89%** de las buenas prácticas son efectivas.
	Proveedores de equipos (Conmutación de circuitos)	**Más del 70%** de los que respondieron opinan que el **100%** de las buenas prácticas son efectivas. **Más del 90%** de los que respondieron opinan que el **84%** de las buenas prácticas son efectivas...
	Proveedores de equipos (Conmutación de paquetes)	**Más del 70%** de los que respondieron opinan que el **100%** de las buenas prácticas son efectivas. **Más del 90%** de los que respondieron opinan que el **82%** de las buenas prácticas son efectivas.
Costo de implementación de las buenas prácticas	Proveedores de servicios (Conmutación de circuitos)	**Más del 50%** de los que respondieron consideran que sólo el **12%** de las buenas prácticas tienen alto costo de implementación. **Más del 90%** de los que respondieron consideran que sólo el **1%** de las buenas prácticas tienen alto costo de implementación.
	Proveedores de servicios (Conmutación de paquetes)	**Más del 50%** de los que respondieron consideran que sólo el **13%** de las buenas prácticas tienen alto costo de implementación. **Más del 90%** de los que respondieron consideran que sólo el **2%** de las buenas prácticas tienen alto costo de

ASPECTO EVALUADO	EVALUADOR	RESULTADO DE LA EVALUACIÓN
		implementación.
	Proveedores de equipos (Conmutación de circuitos)	**Más del 50%** de los que respondieron consideran el **54%** de las buenas prácticas tienen alto costo de implementación. **Más del 90%** de los que respondieron consideran que sólo el **12%** de las buenas prácticas tienen alto costo de implementación.
	Proveedores de equipos (Conmutación de paquetes)	**Más del 50%** de los que respondieron consideran que sólo el **24%** de las buenas prácticas tienen alto costo de implementación. **Más del 90%** de los que respondieron consideran que **NINGUNA** de las buenas prácticas tiene alto costo de implementación
Riesgo de NO implementación de las buenas prácticas	Proveedores de servicios (Conmutación de circuitos)	**Más del 50%** de los que respondieron consideran que el **97%** de las buenas prácticas tienen alto o moderado riesgo al NO implementarse. **Más del 90%** de los que respondieron consideran que el **48%** de las buenas prácticas tienen alto o moderado riesgo al NO implementarse.
	Proveedores de servicios (Conmutación de paquetes)	**Más del 50%** de los que respondieron consideran que el **94%** de las buenas prácticas tienen alto o moderado riesgo al NO implementarse. **Más del 90%** de los que respondieron consideran que el **63%** de las buenas prácticas tienen alto o moderado riesgo al NO implementarse.
	Proveedores de equipos (Conmutación	**Más del 50%** de los que respondieron consideran que el **98%** de las buenas prácticas tienen alto o moderado riesgo al NO implementarse.

ASPECTO EVALUADO	EVALUADOR	RESULTADO DE LA EVALUACIÓN
	de circuitos)	**Más del 90%** de los que respondieron consideran que el **60%** de las buenas prácticas tienen alto o moderado riesgo al NO implementarse.
	Proveedores de equipos (Conmutación de paquetes)	**Más del 50%** de los que respondieron consideran que el **96%** de las buenas prácticas tienen alto o moderado riesgo al NO implementarse. **Más del 90%** de los que respondieron consideran que el **55%** de las buenas prácticas tienen alto o moderado riesgo al NO implementarse.

Fuente: Network reliability and interoperability Council V Focus Group 2 Subcommittee 2.A, 2002

7.2.2 Buenas prácticas en la Unión Europea

Las buenas prácticas adoptadas voluntariamente en la Unión Europea contemplan los aspectos fundamentales de las redes de telecomunicaciones. En el anexo No. 3, se incluyen algunas buenas prácticas a manera ilustrativa, relacionadas con:

- Suministro de energía eléctrica
- Hardware
- Software
- Red
- Tráfico (Payload)
- Políticas

En el estudio de Availability and Robustness of Electronic Communications Infrastructures (ARECI) realizado por Alcatel Lucent para la Unión Europea, se registra la opinión de 900 expertos sectoriales europeos, así:

- 90% estimaron que las buenas prácticas incluidas en el Anexo No. 3 son eficaces.
- 71 % indican que el costo de implementar las buenas prácticas es bajo o moderado.
- La implementación voluntaria de las buenas prácticas es factible, aunque no gratuita.
- 91% indican que el riesgo de no implementar las buenas prácticas es alto o moderado.
- 94% de las respuestas indican que el total de las Buenas prácticas específicas se aplican "En todas partes" o "en todas las partes críticas" en las redes o productos de los expertos.

PÁGINA EN BLANCO

8 ANEXO 1 INFORMACIÓN SOLICITADA A OPERADORES

Información solicitada a los operadores de servicios de telecomunicaciones y entidades que hacen uso de ellas, con el fin de aplicar el modelo de vulnerabilidad de las redes de telecomunicaciones ante amenazas naturales y su aplicación en las zonas definidas.

Tabla 83. Información de redes vitales de telecomunicaciones para la elaboración del modelo de vulnerabilidad

INFORMACION PARA LA APLICACIÓN DEL MODELO EN LAS ZONAS DE AMENAZA (67 MUNICIPIOS - 308 CENTROS POBLADOS)

PENETRACION TPBCL E INTERNET - CINTEL

Población	OPERADORES DE TPBCL	NUMERO DE LINEAS TPBCL EN SERVICIO	PENETRACION TPBCL	USUARIOS INTERNET	PENETRACION INTERNET	USUARIOS BANDA ANCHA	OTROS USUARIOS INTERNET

USUARIOS DEL ESPECTRO RADIOELECTRICO - MINTIC

Nombre del Concesionario	SERVICIO	UBICACIÓN ESTACION A UTILICE COORDENADAS GEOGRAFICAS WGS 84	FRECUENCIA (MHz)	UBICACIÓN ESTACION B PARA EL CASO DE ENLACES PUNTO A PUNTO UTILICE COORDENADAS GEOGRAFICAS WGS 84

SERVICIO PORTADOR - OPERADORES

Cantidad de nodos en el MUNICIPIO (Por favor diligenciar información solicitada para cada nodo). INSERTE TANTAS FILAS PARA CADA MUNICIPIO COMO SEA NECESARIO EN FUNCION DE LOS NODOS INSTALADOS	UBICACIÓN NODOS UTILICE COORDENADAS GEOGRAFICAS WGS 84	MEDIO UTILIZADO PARA PRESTAR EL SERVICIO PORATDOR EN EL MUNICIPIO	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS	TIPO DE ELEMENTO DE ORDEN SUPERIOR	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE LOS NODOS EN EL MUNICIPIO CON EL ELEMENTO DE ORDEN SUPERIOR	MEDIO DE CONECTIVIDAD DE BACKUP DESDE LOS NODOS EN EL MUNICIPIO CON EL ELEMENTO DE ORDEN SUPERIOR	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR AL CUAL SE CONECTA LA ESTACION UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS
EXISTE UN PUNTO ALTERNATIVO O MAS DE ORDEN SUPERIOR AL CUAL SE CONECTARIA EL NODO DEL MUNICIPIO EN CASO DE FALLA DEL ELEMENTO DE ORDEN SUPERIOR PRINCIPAL (DIVERSIDAD DE INTERCONEXON); EN CASO DE QUE EXISTAN MAS DE UNO POR FAVOR DILIGENCIE LA INFORMACION DE AL MENOS UNO	TIPO DE ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE LOS NODOS EN EL MUNICIPIO CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	MEDIO DE CONECTIVIDAD DE BACK UP DESDE EL NODO DEL MUNICIPIO CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO AL CUAL SE CONECTA EL NODO DEL MUNICIPIO UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS				

SERVICIO DE TMC - OPERADORES

Cantidad de estaciones base mediante las cuales se presta el servicio al MUNICIPIO (Por favor diligenciar información solicitada para cada estación base). INSERTE TANTAS FILAS PARA CADA MUNICIPIO COMO SEA NECESARIO EN FUNCION DE LAS ESTACIONES BASE INSTALADAS)	UBICACIÓN ESTACIONES BASE / NODOS B (WGS 84)	TECNOLOGIA	MEDIO DE CONECTIVIDAD PRINICIPAL DE LAS ESTACIONES BASE AL BSC /RNC	MEDIO DE CONECTIVIDAD DE BACKUP DE LAS ESTACIONES BASE AL BSC / RNC	RADIO DE COBERTURA ESTIMADA DE LA CELDA (km)	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR (BSC / RNC) AL CUAL SE CONECTA LA CELDA (WGS 84)
TECNOLOGIA	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS	MEDIO DE CONECTIVIDAD PRINICIPAL DE LAS BSC/RNC CON MSC / MEDIA GATEWAY	MEDIO DE CONECTIVIDAD DE BACKUP DE LAS LAS BSC/RNC CON MSC /MEDIA GATEWAY	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR (MEDIA GATEWAY / MSC) (WGS 84)	TIPO DE ELEMENTO DE ORDEN SUPERIOR (MEDIA GATEWAY / MSC)	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS

INFORMACION PARA LA APLICACIÓN DEL MODELO EN LAS ZONAS DE AMENAZA (67 MUNICIPIOS - 308 CENTROS POBLADOS)

SERVICIO DE TPBCL E INTERNET - OPERADORES

Lineas de TPBCL en servicio en el MUNICIPIO	Usuarios de Internet Banda Ancha en el MUNICIPIO	Usuarios de Internet Banda Angosta en el MUNICIPIO	TIPO DE ELEMENTO DE ORDEN SUPERIOR (CENTRAL DE CONMUTACION, SOFTSWITCH, MEDIAGATEWAY)	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE EL MUNICIPIO CON EL ELEMENTO DE ORDEN SUPERIOR	MEDIO DE CONECTIVIDAD DE BACKUPDESDE EL MUNICIPIO CON EL ELEMENTO DE ORDEN SUPERIOR	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR AL CUAL SE CONECTA EL MUNICIPIO UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS
EXISTE UN PUNTO ALTERNATIVO O MAS DE ORDEN SUPERIOR AL CUAL SE CONECTARIA EL MUNICIPIO EN CASO DE FALLA DEL ELEMENTO DE ORDEN SUPERIOR PRINCIPAL (DIVERSIDAD DE INTERCONEXON); EN CASO DE QUE EXISTAN MAS DE UNO POR FAVOR DILIGENCIE LA INFORMACION DE AL MENOS UNO	TIPO DE ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO (CENTRAL DE CONMUTACION, SOFTSWITCH, MEDIA GATEWAY)	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE EL MUNICIPIO CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	MEDIO DE CONECTIVIDAD DE BACKUP DESDE EL MUNICIPIO CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO AL CUAL SE CONECTA EL MUNICIPIO UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS		

	Centrales de conmutación y/o Media Gateway mediante los cuales presta el servicio de TPBCL al munciipio (inserte tantas filas como sea necesario en función del número de centrales y/o media gateways)	Número de líneas en servicio por central	UBICACIÓN CENTRALES DE CONMUTACION y/o MEDIA GATEWAY (WGS 84)	TIPO DE ELEMENTO DE ORDEN SUPERIOR (CENTRAL LARGA DISTANCIA / SOFT SWITCH) AL CUAL SE CONECTA LA CENTRAL DE CONMUTACION O LA MEDIA GATEWAY	MEDIO DE CONECTIVIDAD PRINCIPAL AL ELEMENTO DE ORDEN SUPERIOR	MEDIO DE CONECTIVIDAD DE BACKUP AL ELEMENTO DE ORDEN SUPERIOR	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR (CENTRAL DE LARGA DISTANCIA /SOFT SWITCH) (WGS 84)
ARMENIA, CAJAMARCA & TUMACO	EXISTE UN PUNTO ALTERNATIVO O MAS DE ORDEN SUPERIOR AL CUAL SE CONECTARIA LA CENTRAL DE CONMUTACION O LA MEDIA GATEWAY EN CASO DE FALLA DEL ELEMENTO DE ORDEN SUPERIOR PRINCIPAL (DIVERSIDAD DE INTERCONEXON); EN CASO DE QUE EXISTAN MAS DE UNO POR FAVOR DILIGENCIE LA INFORMACION DE AL MENOS UNO	TIPO DE ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE LA CENTRAL DE CONMUTACION O LA MEDIA GATEWAY EN EL MUNICIPIO CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	MEDIO DE CONECTIVIDAD DE BACKUP DESDE LA CENTRAL DE CONMUTACION O LA MEDIA GATEWAY EN EL MUNICIPIO CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO AL CUAL SE CONECTA LA CENTRAL DE CONMUTACION O LA MEDIA GATEWAY DEL MUNICIPIO UTILICE COORDENADAS GEOGRAFICAS WGS 84	MEDIO DE CONECTIVIDAD DE BACKUP AL ELEMENTO DE ORDEN SUPERIOR	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS	

	Armarios mediante los cuales presta el servicio de TPBCL al munciipio (inserte tantas filas como sea necesario en función del número de armarios)	Número de líneas en servicio por armario	UBICACIÓN ARMARIOS (WGS 84)	TIPO DE ELEMENTO DE ORDEN SUPERIOR (CENTRAL DE CONMUTACION / MEDIAGATEWAY) AL CUAL SE CONECTA EL ARMARIO	MEDIO DE CONECTIVIDAD PRINCIPAL AL ELEMENTO DE ORDEN SUPERIOR	MEDIO DE CONECTIVIDAD DE BACKUP AL ELEMENTO DE ORDEN SUPERIOR	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR (CENTRAL DE CONMUTACION / MEDIA GATEWAY) AL CUAL SE CONECTA EL ARMARIO (WGS 84)	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS
	EXISTE UN PUNTO ALTERNATIVO O MAS DE ORDEN SUPERIOR AL CUAL SE CONECTARIA EL ARMARIO EN CASO DE FALLA DEL ELEMENTO DE ORDEN SUPERIOR PRINCIPAL (DIVERSIDAD DE INTERCONEXON); EN CASO DE QUE EXISTAN MAS DE UNO POR FAVOR DILIGENCIE LA INFORMACION DE AL MENOS UNO	TIPO DE ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE LOS NODOS EN EL MUNICIPIO CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	MEDIO DE CONECTIVIDAD DE BACK UP DESDE EL NODO DEL MUNICIPIO CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO AL CUAL SE CONECTA EL NODO DEL MUNICIPIO UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS	

INFORMACION PARA LA APLICACIÓN DEL MODELO EN LAS ZONAS DE AMENAZA (67 MUNICIPIOS - 308 CENTROS POBLADOS)

SERVICIO DE TELEVISION RADIODIFUNDIDA - CNTV

Cantidad de estaciones de TV radiodifundida mediante las cuales se presta el servicio al MUNICIPIO (Por favor diligenciar información solicitada para cada estación). INSERTE TANTAS FILAS PARA CADA MUNICIPIO COMO SEA NECESARIO EN FUNCION DE LAS ESTACIONES INSTALADAS)	Nombre del Concesionario	UBICACIÓN DEL CENTRO DE EMISION UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE EL CENTRO DE EMISION HASTA EL TRANSMISOR	MEDIO DE CONECTIVIDAD DE BACKUP DESDE EL CENTRO DE EMISION HASTA EL TRANSMISOR	UBICACIÓN DEL TRANSMISOR DE TV UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS

SERVICIO DE TELEVISION POR SUSCRIPCION - CNTV

Cantidad de concesionarios que prestan el servicio al MUNICIPIO (Por favor diligenciar información solicitada para cada cabecera). INSERTE TANTAS FILAS PARA CADA MUNICIPIO COMO SEA NECESARIO EN FUNCION DE LOS CONCESIONARIOS QUE PRESTAN EL SERVICIO	Nombre del Concesionario	UBICACIÓN DE LA CABECERA UTILICE COORDENADAS GEOGRAFICAS WGS 84	NUMERO DE HOGARES PASADOS	UTILIZA EN LA CABECERA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS

SERVICIO DE RADIODIFUSION AM & FM (MINTIC - CARACOL / RCN)

Cantidad de estaciones AM mediante las cuales se presta el servicio al MUNICIPIO (Por favor diligenciar información solicitada para cada estación). INSERTE TANTAS FILAS PARA CADA MUNICIPIO COMO SEA NECESARIO EN FUNCION DE LAS ESTACIONES INSTALADAS)	Nombre del Concesionario	UBICACIÓN DE LOS ESTUDIOS UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE LOS ESTUDIOS HASTA EL TRANSMISOR	MEDIO DE CONECTIVIDAD DE BACKUP DESDE LOS ESTUDIOS HASTA EL TRANSMISOR	UBICACIÓN DEL TRANSMISOR UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS

TELEMETRIA EN LAS ZONAS DE AMENAZA - IDEAM & INGEOMINAS

Cantidad de estaciones en este MUNICIPIO (Por favor diligenciar información solicitada para cada estación). INSERTE TANTAS FILAS PARA CADA MUNICIPIO COMO SEA NECESARIO EN FUNCION DE LAS ESTACIONES INSTALADAS)	UBICACIÓN ESTACIONES UTILICE COORDENADAS GEOGRAFICAS WGS 84	BANDA DE FRECUENCIA UTILIZADA (MHz)	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS	TIPO DE ELEMENTO DE ORDEN SUPERIOR (ESTACION BASE, CENTRO DE OPERACIONES, ETC)	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE LAS ESTACIONES CON EL ELEMENTO DE ORDEN SUPERIOR	MEDIO DE CONECTIVIDAD DE BACK UP DESDE LAS ESTACIONES CON EL ELEMENTO DE ORDEN SUPERIOR	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR AL CUAL SE CONECTA LA ESTACION UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS
EXISTE UN PUNTO ALTERNATIVO O MAS DE ORDEN SUPERIOR AL CUAL SE CONECTARIA EN CASO DE FALLA DEL ELEMENTO DE ORDEN SUPERIOR PRINCIPAL (DIVERSIDAD DE INTERCONEXON); EN CASO DE QUE EXISTAN MAS DE UNO POR FAVOR DILIGENCIE LA INFORMACION DE AL MENOS UNO	TIPO DE ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO (ESTACION BASE, CENTRO DE OPERACIONES, ETC)	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE LAS ESTACIONES CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	MEDIO DE CONECTIVIDAD DE BACK UP DESDE LAS ESTACIONES CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO AL CUAL SE CONECTA LA ESTACION UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS				

INFORMACION PARA LA APLICACIÓN DEL MODELO EN LAS ZONAS DE AMENAZA (67 MUNICIPIOS - 308 CENTROS POBLADOS)

SERVICIO MOVIL AERONAUTICO / MARITIMO EN ZONAS DE AMENAZA - AERONAUTICA / DIMAR

Cantidad de estaciones mediante las cuales se presta el servicio de móvil aeronautico desde este MUNICIPIO (Por favor diligenciar información solicitada para cada estación). INSERTE TANTAS FILAS PARA CADA MUNICIPIO COMO SEA NECESARIO EN FUNCION DE LAS ESTACIONES INSTALADAS)	UBICACIÓN ESTACIONES DE MOVIL AERONAUTICO UTILICE COORDENADAS GEOGRAFICAS WGS 84	BANDA DE FRECUENCIA UTILIZADA	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS	TIPO DE ELEMENTO DE ORDEN SUPERIOR (ESTACION BASE, CENTRO DE OPERACIONES, ETC)	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE LAS ESTACIONES DE MOVIL AERONAUTICO CON EL ELEMENTO DE ORDEN SUPERIOR	MEDIO DE CONECTIVIDAD DE BACK UP DESDE LAS ESTACIONES DE MOVIL AERONAUTICO CON EL ELEMENTO DE ORDEN SUPERIOR	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR AL CUAL SE CONECTA LA ESTACION DE MOVIL AERONAUTICO UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS
EXISTE UN PUNTO ALTERNATIVO O MAS DE ORDEN SUPERIOR AL CUAL SE CONECTARIA EN CASO DE FALLA DEL ELEMENTO DE ORDEN SUPERIOR PRINCIPAL (DIVERSIDAD DE INTERCONEXON); EN CASO DE QUE EXISTAN MAS DE UNO POR FAVOR DILIGENCIE LA INFORMACION DE AL MENOS UNO	TIPO DE ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO (ESTACION BASE, CENTRO DE OPERACIONES, ETC)	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE LAS ESTACIONES CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	MEDIO DE CONECTIVIDAD DE BACK UP DESDE LAS ESTACIONES CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO AL CUAL SE CONECTA LA ESTACION UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS				

COMPARTEL - MINTIC

Cantidad de puntos COMPARTEL en este MUNICIPIO (Por favor diligenciar información solicitada para cada estación). INSERTE TANTAS FILAS PARA CADA MUNICIPIO COMO SEA NECESARIO EN FUNCION DE LOS PUNTOS COMPARTEL INSTALADOS)	UBICACIÓN PUNTOS COMPARTEL UTILICE COORDENADAS GEOGRAFICAS WGS 84	DIRECCION PUNTO COMPARTEL	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS	TIPO DE ELEMENTO DE ORDEN SUPERIOR (HUB, CENTRO DE OPERACIONES, ETC)	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE LOS PUNTOS COMPARTEL CON EL ELEMENTO DE ORDEN SUPERIOR	MEDIO DE CONECTIVIDAD DE BACK UP DESDE LAS PUNTOS COMPARTEL CON EL ELEMENTO DE ORDEN SUPERIOR	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR AL CUAL SE CONECTA EL PUNTO COMPARTEL UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS
EXISTE UN PUNTO ALTERNATIVO O MAS DE ORDEN SUPERIOR AL CUAL SE CONECTARIA EL PUNTO COMPARTEL EN CASO DE FALLA DEL ELEMENTO DE ORDEN SUPERIOR PRINCIPAL (DIVERSIDAD DE INTERCONEXON); EN CASO DE QUE EXISTAN MAS DE UNO POR FAVOR DILIGENCIE LA INFORMACION DE AL MENOS UNO	TIPO DE ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO (HUB, CENTRO DE OPERACIONES, ETC)	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE LOS PUNTOS COMPARTEL CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	MEDIO DE CONECTIVIDAD DE BACK UP DESDE LOS PUNTOS COMPARTEL CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO AL CUAL SE CONECTA EL PUNTO COMPARTEL UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS				

RADIOAFICIONADOS - MINTIC

NUMERO DE RADIOAFICIONADOS (Para las ciudades de Armenia, Cajamarca y Tumaco por favor anexar listado de radioaficionados con Dirección)

INFORMACION PARA LA APLICACIÓN DEL MODELO EN LAS ZONAS DE AMENAZA (67 MUNICIPIOS - 308 CENTROS POBLADOS)

REDES DE EMERGENCIA

CARACTERIZACION ESTACION (CLOPAD /CREPAD /CRUZ ROJA / DEFENSA CIVIL / BOMBEROS / ALCALDIA)						CARACTERIZACION ELEMENTO SUPERIOR DE RED							
Cantidad de ESTACIONES en este MUNICIPIO (Por favor diligenciar información solicitada para cada estación). INSERTE TANTAS FILAS PARA CADA MUNICIPIO COMO SEA NECESARIO EN FUNCION DE LAS ESTACIONES INSTALADAS)	UBICACIÓN ESTACIONES UTILICE COORDENADAS GEOGRAFICAS WGS 84	BANDA DE FRECUENCIA UTILIZADA (MHz)	SISTEMA DE TELECOMUNICACION UTILZADO	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS	TIPO DE ELEMENTO DE ORDEN SUPERIOR (ESTACION BASE, CENTRO DE OPERACIONES, ETC)	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE LAS ESTACIONES CON EL ELEMENTO DE ORDEN SUPERIOR	EN CASO DE QUE EL MEDIO DE CONECTIVIDAD PRINCIPAL SEA RADIO ESPECIFIQUE LA FRECUENCIA EN MHz	MEDIO DE CONECTIVIDAD DE BACK UP DESDE LAS ESTACIONES CON EL ELEMENTO DE ORDEN SUPERIOR	EN CASO DE QUE EL MEDIO DE CONECTIVIDAD DE BACK UP SEA RADIO ESPECIFIQUE LA FRECUENCIA EN MHz	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR AL CUAL SE CONECTA LA ESTACION UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS
CARACTERIZACION ELEMENTOS ALTERNATIVOS DE ORDEN SUPERIOR DE RED													
EXISTE UN PUNTO ALTERNATIVO O MAS DE ORDEN SUPERIOR AL CUAL SE CONECTARIA EN CASO DE FALLA DEL ELEMENTO DE ORDEN SUPERIOR PRINCIPAL (DIVERSIDAD DE INTERCONEXON); EN CASO DE QUE EXISTAN MAS DE UNO POR FAVOR DILIGENCIE LA INFORMACION DE AL MENOS UNO	TIPO DE ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO (ESTACION BASE, CENTRO DE OPERACIONES, ETC)	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE LAS ESTACIONES CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	EN CASO DE QUE EL MEDIO DE CONECTIVIDAD PRINCIPAL SEA RADIO ESPECIFIQUE LA FRECUENCIA EN MHz	MEDIO DE CONECTIVIDAD DE BACK UP DESDE LAS ESTACIONES CON EL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO	EN CASO DE QUE EL MEDIO DE CONECTIVIDAD DE BACK UP SEA RADIO ESPECIFIQUE LA FRECUENCIA EN MHz	UBICACIÓN DEL ELEMENTO DE ORDEN SUPERIOR ALTERNATIVO AL CUAL SE CONECTA LA ESTACION UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS					
INTEROPERABILIDAD CON OTRAS REDES DE EMERGENCIA													
TIENE CONEXION CON OTRAS REDES DE EMERGENCIA PARA CASOS DE DESASTRE ; EN CASO DE QUE EXISTA CONEXIÓN CON MAS DE UNA RED DE EMERGENCIA INSERTE TANTAS LINEAS COMO REDES DE EMERGENCIA A LAS QUE ESTA CONECTADO LA ESTACION REFERENCIADA EN LA COLUMNA G DE ESTA HOJA	TIPO DE ELEMENTO DE LA RED DE EMERGENCIA A LA QUE ESTA CONECTADO (ESTACION BASE, CENTRO DE OPERACIONES, ETC)	MEDIO DE CONECTIVIDAD PRINCIPAL DESDE LAS ESTACIONES CON EL ELEMENTO DE LA RED DE EMERGENCIA A LA QUE ESTA CONECTADO	EN CASO DE QUE EL MEDIO DE CONECTIVIDAD PRINCIPAL SEA RADIO ESPECIFIQUE LA FRECUENCIA EN MHz	MEDIO DE CONECTIVIDAD DE BACK UP DESDE LAS ESTACIONES CON EL ELEMENTO DE DE LA RED DE EMERGENCIA A LA QUE ESTA CONECTADO	EN CASO DE QUE EL MEDIO DE CONECTIVIDAD DE BACK UP SEA RADIO ESPECIFIQUE LA FRECUENCIA EN MHz	UBICACIÓN DEL ELEMENTO DE LA RED DE EMERGENCIA AL CUAL SE CONECTA LA ESTACION UTILICE COORDENADAS GEOGRAFICAS WGS 84	UTILIZA SISTEMA DE ENERGIA DE RESPALDO (UPS, BATERIAS, GRUPO MOTOGENERADOR, CELDAS SOLARES)	TIEMPO DE AUTONOMIA EN HORAS					

9 ANEXO 2 BUENAS PRÁCTICAS ESTADOS UNIDOS DE NORTEAMÉRICA

(FUENTE: NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL (URIC) FCC)

Federal Communications Commission (USA)
NRIC Best Practices Result

Network Type(s): Cable AND Internet/Data AND Satellite AND Wireless AND Wireline
Industry Role(s): Service Provider AND Network Operator
Keyword(s): Network Design

79 Best Practices are found.

*Press Best Practice number to get detailed information.

Number	Description
7-5-0514	When available, Network Operators and Service Providers should utilize a management system capability (e.g., CORBA, SNMP) providing a single interface with access to alarms and monitoring information from all critical network elements.
07/06/5073	Network Operators, Service Providers and Equipment Suppliers should perform risk assessment on significant network changes (e.g., technology upgrades).
07/06/5098	Network Operators, Service Providers and Equipment Suppliers should ensure that all network infrastructure equipment meets the minimum requirements of ANSI T1.319 (fire resistance).
07/06/5149	Network Operators, Service Providers and Equipment Suppliers should, where feasible, ensure that intentional emissions (e.g., RF and optical) from network equipment and transmission facilities are secured sufficiently to ensure that monitoring from outside the intended transmission path or beyond facility physical security boundaries cannot lead to the obtaining of critical network operations information.
07/06/5210	Network Operators, Service Providers and Property Managers should discourage use of Emergency Power Off (EPO) switches between the primary battery supplies and the main power distribution board. EPO switches are not recommended for use in traditional -48V DC battery plants.
07/06/5248	Network Operators, Service Providers and Equipment Suppliers should perform risk assessment on significant network changes, both temporary and permanent, resulting from restoration efforts.
07/06/5255	Network Operators, Service Providers and Equipment Suppliers should ensure that temporary wireless networks (e.g., terrestrial microwave, free-space optical, satellite, point-to-point, multi-point, mesh) used during an incident are subsequently disabled or secured.
07/06/8015	Segmenting Management Domains: For OAM&P activities and operations centers, Network Operators and Service Providers should segment administrative domains with devices such as firewalls that have restrictive rules for traffic in both directions and that require authentication for traversal. In particular, segment OAM&P networks from the Network Operator's or Service Provider's intranet and the Internet. Treat each domain as hostile to all other domains. Follow industry recommended firewall policies for protecting critical internal assets.
07/06/8016	OAM&P Security Architecture: Network Operators and Service Providers should design and deploy an Operations, Administration, Management, and Provisioning (OAM&P) security architecture based on industry recommendations.
07/06/8021	Switched Hubs for OAM&P Networks: In critical networks for Operations, Administration, Management, and Provisioning (OAM&P), Network Operators, Service Providers and Equipment Suppliers should use switched network hubs so that devices in promiscuous mode are less likely to be able to see/spoof all of the traffic on that network segment.
07/06/8047	Protect Against DNS (Domain Name System) Denial of Service: Network Operators and Service Providers should provide DNS DoS protection by implementing protection techniques such as: 1) increase DNS resiliency through redundancy and robust network connections 2) Have separate name servers for internal and external traffic as well as critical infrastructure, such as OAM&P and signaling/control networks 3) Where feasible, separate proxy servers from authoritative name servers 4) Protect DNS information by protecting master name servers with appropriately configured firewall/filtering rules, implement secondary masters for all name resolution, and using Bind ACLs to filter zone transfer requests.
7-7-0402	Single Point of Failure: Network Operators and Service Providers should, where appropriate, design networks to minimize the impact of a single point of failure (SPOF).
7-7-0404	Network Performance: Service Providers, Network Operators and Equipment Suppliers should incorporate methodologies that continually improve network or equipment performance.
7-7-0405	Network Performance: Network Operators and Service Providers should periodically examine and review their network to ensure that it meets the current design specifications.
7-7-0490	Network Operators and Service Providers should consult National Fire Prevention Association Standards (e.g., NFPA 75 and 76) for guidance in the design of fire suppression systems. When zoning regulations require sprinkler systems, an exemption should be sought for the use of non-destructive systems.
7-7-0505	Network Operators and Service Providers should have procedures in place to process court orders and subpoenas for wire taps or other information.
7-7-0507	Attack Trace Back: Network Operators, Service Providers and Equipment Suppliers should have the processes and/or capabilities to analyze and determine the source of malicious traffic, and then to trace-back and drop the packets at, or closer to, the source. The references provide several different possible techniques. (Malicious traffic is that traffic such as Distributed Denial of Service (DDoS) attacks, smurf and fraggle attacks, designed and transmitted for the purpose of consuming resources of a destination of network to block service or consume resources to overflow state that might cause system crashes).
7-7-0508	Network Operators and Service Providers should establish company-specific interconnection agreements, and where appropriate, utilize existing interconnection templates and existing data connection trust agreement.
7-7-0510	Network Operators, Service Providers and Equipment Suppliers should, by design and practice, manage critical Network Elements (e.g., Domain Name Servers, Signaling Servers) that are essential for network connectivity and subscriber service as critical systems (e.g., secure, redundant, alternative routing).

7-7-0519	Capacity Monitoring: Network Operators and Service Providers should engineer and monitor networks to ensure that operating parameters are within capacity limits of their network design (e.g., respect limitations of deployed packet switches, routers and interconnects, including managed networks and managed CPE). These resource requirements should be re-evaluated as services change or grow.
7-7-0520	Network Operators and Service Providers should have a route policy that is available, as appropriate. A consistent route policy facilitates network stability and inter-network troubleshooting.
7-7-0521	Industry Standards: Network Operators, Service Providers and Equipment Suppliers should work toward implementing industry standards for interconnection points.
7-7-0546	Network Operators and Service Providers should minimize single points of failure (SPOF) in paths linking network elements deemed critical to the operations of a network (with this design, two or more simultaneous failures or errors need to occur at the same time to cause a service interruption).
7-7-0547	Network Operators and Service Providers should place critical network databases (e.g., directory server, feature server, Service Control Point (SCP)) in a secure environment across distributed locations to provide service assurance (e.g., maintainability, connectivity, security, reliability) consistent with other critical network elements.
7-7-0605	Network Operators and Service Providers should assess the synchronization needs of the network elements and interfaces that comprise their networks to develop and maintain a detailed synchronization plan.
7-7-0608	Network Operators and Service Providers should utilize network surveillance and monitoring to keep overflow traffic conditions from adversely affecting networks. Interconnecting companies should address the control of overflow conditions in their bilateral agreements.
7-7-0618	Network Operators and Service Providers should establish mutually agreed upon reliability thresholds with Equipment Suppliers for new hardware (e.g., routers, switches, call servers, signaling servers) brought into service on the network.
7-7-0622	Network Operators, Service Providers, and Property Managers should use ANSI T1.311-1998 Standard for Telecommunications Environmental Protection, DC Power Systems for key equipment locations (e.g., routers, central office switches, and other critical network elements) to reduce fires associated with DC power equipment.
7-7-0651	Network Operators, Service Providers and Property Managers should consider providing diversity within power supply and distribution systems so that single point failures (SPOF) are not catastrophic. For large battery plants in critical offices, consider providing dual AC feeds (odd/even power service cabinets for rectifiers). Transfer switches should be listed to a UL standard for Transfer Switch Equipment. When transfer breaker systems are used, they must be mechanically and electrically interlocked.
7-7-0652	Network Operators, Service Providers, Equipment Suppliers and Property Managers should adhere to the following applicable power engineering design standards; Telcordia GR-513-CORE (Power - LSSGR section 13), Telcordia GR-63-CORE (NEBS), Telcordia GR-295-CORE (Isolated Ground Planes), Telcordia GR-1089-CORE (Electromagnetic Compatibility), and ANSI T1.311 (DC power Systems).
7-7-0657	Network Operators, Service Providers and Property Managers should design standby generator systems for fully automatic operation and for ease of manual operation, when required.
7-7-0672	Network Operators and Service Providers should provide a minimum of 3 hours battery reserve for central offices equipped with fully automatic standby systems.
7-7-0675	Network Operators, Service Providers and Property Managers should, for new installations, consider using multiple small battery plants in place of single very large plants, and consider using multiple battery strings in each plant.
7-7-0676	Network Operators and Service Providers should not use low voltage disconnects or battery disconnects at central office battery plants.
7-7-0677	Network Operators, Service Providers and Property Managers should only use rectifier sequence controllers where necessary to limit load on the backup power generator.
7-7-0679	Network Operators, Service Providers and Equipment Suppliers should provide diverse power feeds for all redundant links (e.g., SS7, BITS clocks) and any components identified as critical single points of failure (SPOF) in transport and operations of the network.
7-7-0683	Network Operators, Service Providers and Equipment Suppliers should not mix DC power cables, AC power cables and telecommunications cables wherever possible.
7-7-0692	Network Operators, Service Providers and Equipment Suppliers should consider using fail-safe, normally closed contacts that open for an alarm, for critical alarms produced by single contacts (one on one).
7-7-0759	Network Operators and Service Providers should ensure that engineering, design, and installation processes address how new network elements are integrated into the office and network synchronization plan(s).

7-7-0760	Network Operators and Service Providers should maintain records that accurately track the diversity of internal wiring for office synchronization, including timing leads and power.
7-7-0775	Network Operators and Service Providers should consult and update the synchronization plan whenever facility (e.g., intra-/inter-office or inter-provider interconnect circuits) rearrangements, additions, deletions, or consolidations are planned. Verify the completed changes against the synchronization plan.
7-7-0823	For the deployment of Residential Internet Access Service, Network Operators, Service Providers and Equipment Suppliers should design, build, and operate broadband networks considering performance aspects of the data facilities employed, such as: packet loss ratio, Bit Error Ratio, latency, and compression, where feasible.
7-7-1015	Network Operators and Service Providers should make available to the disaster recovery team as-built drawings of network sites.
7-7-1050	Network Operators and Service Providers should consider tertiary carrier/transport methods such as satellite, microwave or wireless to further reduce point of failures or as hot transport backup facilities.
7-7-1065	Network Operators and Service Providers should identify and manage critical network elements and architecture that are essential for network connectivity and subscriber services considering security, functional redundancy and geographical diversity.
07/07/3220	E9-1-1 Selective Router Database (SRDB) Diversity: Network Operators and Service Providers that operate E9-1-1 Selective Router Databases (SRDBs) should deploy SRDBs with redundancy and geographic diversity.
07/07/3222	E9-1-1 Selective Router (SR) to Public Safety Answering Point (PSAP) Trunking Architecture: Network Operators, Service Providers and Public Safety Answering Points (PSAPs) should provide, where appropriate, at least one additional trunk between the E9-1-1 Selective Router (SR) and the PSAP than the switching entity source with the largest total number of trunks serving that PSAP.
07/07/3223	Originating Source to E9-1-1 Selective Router Trunking Architecture: Network Operators and Service Providers should implement dedicated trunk groups between the Mobile Switching Center (MSC) end office or similar source and the E9-1-1 Selective Router (SR), based on the geography served by the default Public Safety Answering Points (PSAPs). This should be done rather than aggregating traffic from centralized switching architectures serving wide spread geographic areas onto a single trunk group to the E9-1-1 Selective Router. This should be done in conjunction with the local PSAP jurisdictional authorities to ensure that correct choices are made.
07/07/3224	E9-1-1 Dedicated Trunking: Network Operators and Service Providers should use dedicated Signaling System 7 (SS7) or Multi Frequency (MF) controlled trunk groups for the normal routing of E9-1-1 calls from originating switching entities to E9-1-1 Selective Routers rather than using shared Public Switched Telephone Network trunking.
07/07/3225	Mobile Positioning Center (MPC) Capacity Reserve: Network Operators and Service Providers that deploy geographically diverse 9-1-1 Mobile Positioning Centers (MPC) with dual load sharing nodes should ensure that the utilization on either node is less than half of each node's capacity so that if one node fails the other node will absorb the load.
07/07/3227	9-1-1 Voice traffic and Location Data concurrency: Network Operators, Service Providers and Equipment Suppliers should deploy location solutions such that the E9-1-1 related data traffic between the Position Determining Entity (PDE) and the mobile subscriber associated with location determination should not interfere with the voice traffic, when feasible.
07/07/3228	Global Positioning System (GPS) Location accuracy for E9-1-1: Network Operators, Service Providers and Equipment Suppliers that use Global Positioning System (GPS) enabled Phase II location solutions should ensure that the GPS satellite location information (e.g., GPS ephemeris, almanac, etc.) is as current as is feasible to assist the handset in providing improved accuracy of the GPS fix, aiding in the reduction of the time of database responses and reduction of the number of database query rebids.
07/07/3231	Satellite Location Identification information Transfer Delay: Network Operators and Service Providers that use Global Positioning System (GPS) enabled Phase II location solutions should ensure that the GPS satellite location identification information (e.g., GPS ephemeris, almanac, etc.) is transmitted to the Phase II Mobile Subscriber or Position Determining Entities (PDE) as soon as is feasible after the E9-1-1 call commences in order to reduce the number of database query rebids.
07/07/5058	Back-up Power: Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure that all critical infrastructure facilities, including the security equipment, devices and appliances protecting it, are supported by backup power systems (e.g., batteries, generators, fuel cells).
07/07/5072	Network Operators, Service Providers and Equipment Suppliers should perform risk assessments on key network facilities and control areas on a regular basis. Assessments should address natural disasters and unintentional or intentional acts of people on facility or nearby structures.
07/07/5075	Network Diversity: Network Operators and Service Providers should ensure that networks built with redundancy are also built with geographic separation where feasible (e.g., avoid placing mated pairs in the same location and redundant logical facilities in the same physical path).
07/07/5076	Network Operators and Service Providers should ensure and periodically review intra-office diversity of critical resources including power, timing source and signaling leads (e.g., SS7).
07/07/5078	Network Operators and Service Providers should be automatically notified upon the loss of alarm data and react accordingly.
07/07/5079	Network Operators and Service Providers should, where feasible, provide both physical and logical diversity of critical facilities links (e.g., nodal, network element). Particular attention should be paid to telecom hotels and other concentration points.

07/07/5107	Network Operators, Service Providers and Equipment Suppliers should evaluate and manage risks (e.g., alternate routing, rapid response to emergencies) associated with a concentration of infrastructure components.
07/07/5113	Network Operators, Service Providers and Property Managers, when feasible, should provide multiple cable entry points at critical facilities (e.g., copper or fiber conduit) avoiding single points of failure (SPOF).
07/07/5203	Network Operators, Service Providers, and Property Managers should develop, maintain and administer a comprehensive program to sustain a reliable power infrastructure.
07/07/5204	Service Providers, Network Operators and Property Managers should ensure availability of emergency/backup power (e.g., batteries, generators, fuel cells) to maintain critical communications services during times of commercial power failures, including natural and manmade occurrences (e.g., earthquakes, floods, fires, power brown/black outs, terrorism). The emergency/backup power generators should be located onsite, when appropriate.
07/07/5212	Network Operators, Service Providers and Property Managers should consider placing generator sets and fuel suppliesÄŸfor critical sites within a secured area to prevent unauthorized access, reduce the likelihood of damage and/or theft, and to provide protection from explosions and weather.
07/07/5213	Network Operators, Service Providers and Property Managers should, where feasible, place fuel tanks in a secured and protected area. Access to fill pipes, fuel lines, vents, manways, etc. should be restricted (e.g., containment by fencing, walls, buildings, buried) to reduce the possibility of unauthorized access.
07/07/5214	Network Operators, Service Providers and Property Managers should consider placing all power and network equipment in a location to increase reliability in case of disaster (e.g., floods, broken water mains, fuel spillage). In storm surge areas, consider placing all power related equipment above the highest predicted or recorded storm surge levels.
07/07/5222	Network Operators, Service Providers and Equipment Suppliers should consider providing trouble call centers with a physically diverse back-up capability that can quickly be configured to receive the incoming traffic and take appropriate action.
07/07/5223	Network Operators, Service Providers and Equipment Suppliers should establish a plan for providing technical support that prevents the loss of one facility or location from disabling their ability to provide support.
07/07/5229	Network Operators, Service Providers and Property Managers should have controlled access to comprehensive facility cabling documentation (e.g., equipment installation plans, network connections, power, grounding and bonding) and keep a backup copy of this documentation at a secured off-site location.
07/07/5241	Network Operators, Service Providers and Equipment Suppliers should consider placing access and facility alarm points to critical or sensitive areas on backup power.
07/07/5242	Network Operators, Service Providers and Equipment Suppliers should reassess the criticality of associated facilities following a catastrophic incident (i.e. loss of one facility may make others more critical).
07/07/5263	Network Operators, Service Providers and Equipment Suppliers should use cables with adequate reliability and cable signal integrity. Such properties as flammability, strain reliefs and signal loss should be considered. If non-standard cables are used because of an emergency restoration, they should be marked as temporary and should be replaced with standard cables as soon as practical.
07/07/5281	Network Operators, Service Providers and Property Managers with buildings serviced by more than one emergency generator, should design, install and maintain each generator as a stand alone unit that is not dependent on the operation of another generator for proper functioning, including fuel supply path.
07/07/8000	Disable Unnecessary Services: Network Operators and Service Providers should establish a process, during design/implementation of any network/service element or management system, to identify potentially vulnerable, network-accessible services (such as Network Time Protocol (NTP), Remote Procedure Calls (RPC), Finger, Rsh-type commands, etc.) and either disable, if unneeded, or provided additional external network protection, such as proxy servers, firewalls, or router filter lists, if such services are required for a business purpose.
07/07/8003	Control Plane Reliability Network Operators and Service Providers should minimize single points of failure (SPOF) in the control plane architecture (e.g., Directory Resolution and Authentications services). Critical applications should not be combined on a single host platform. All security and reliability aspects afforded to the User plane (bearer) network should also be applied to the Control plane network architecture.
07/07/8005	Document Single Points of Failure: Network Operators and Service Providers should implement a continuous engineering process to identify and record single points of failure (SPOF) and any components that are critical to the continuity of the infrastructure. The process should then pursue architectural solutions to mitigate the identified risks as appropriate.
07/07/8008	Network Architecture Isolation/Partitioning:Network Operators and Service Providers should implement architectures that partition or segment networks and applications using means such as firewalls, demilitarized zones (DMZ), or virtual private networks (VPN) so that contamination or damage to one asset does not disrupt or destroy other assets. In particular, where feasible, it is suggested the user traffic networks, network management infrastructure networks, customer transaction system networks, and enterprise
07/07/8025	Protection from SCADA Networks: Telecom/Datacomm OAM&P networks for Network Operators and Service Providers should be isolated from other OAM&P networks, e.g., SCADA networks, such as for power, water, industrial plants, pipelines, etc.
	Isolate the SCADA network from the OAM&P network (segmentation)
	Put a highly restrictive device, such as a firewall, as a front-end interface on the SCADA network for management access.
	Use an encrypted or a trusted path for the OAM&P network to communicate with the SCADA "front-end."
07/07/8506	Document Single Points of Failure During Recovery: Following a compromise and reestablishment of lost service, Network Operators and Service Providers should re-evaluate the architecture for single points of failure (SPOF). Review the process of evaluating and documenting single points of failure and provide spares for redundancy in the architecture to ensure adequacy of the security architecture.

Federal Communications Commission (USA)
NRIC Best Practices Result

Network Type(s): Cable AND Internet/Data AND Satellite AND Wireless AND Wireline
Industry Role(s): Service Provider AND Network Operator
Keyword(s): Business Continuity

72 Best Practices are found.

*Press Best Practice number to get detailed information.

Number	Description
7-6-1006	Network Operators, Service Providers and Equipment Suppliers should consider establishing a designated Emergency Operations Center. This center should contain tools for coordination of service restoral including UPS, alternate means of communications, maps, and documented procedures to manage business interruptions and/or disasters.
7-6-1007	Network Operators, Service Providers and Equipment Suppliers should consider establishing a geographically diverse back-up Emergency Operations Center.
7-6-1013	Service Providers, Network Operators and Equipment Suppliers should review their insurance requirements in order to maintain business continuity in the event of massive property damage or loss, incapacitation of senior officers, and other interruptive situations.
7-6-1016	Network Operators and Service Providers should develop processes or plans to quickly account for all employees (e.g. field techs) in or near the impact area of a disaster.
7-6-1017	Network Operators and Service Providers should have documented plans or processes to assess damage to network elements, outside plant, facility infrastructure, etc. for implementation immediately following a disaster.
7-6-1022	Network Operators, Service Providers and Equipment Suppliers should consider the development of a vital records program to protect vital records that may be critical to restoration efforts.
7-6-1038	Network Operators, Service Providers and Equipment Suppliers should consider during times of disaster, communicating the disaster response status frequently and consistently to all appropriate employees - so that they all understand what processes have been put in place to support customers and what priorities have been established in the response.
7-6-1051	Network Operators and Service Providers should work with Equipment Suppliers and Government entities to identify criteria and procedures for handling network elements affected by nuclear attack or nuclear accidents (e.g., shock wave, Electro-magnetic Pulse (EMP), Thermal, Fallout, fiber darkening of phosphorous based fiber cable).
07/06/5228	Network Operators, Service Providers and Equipment Suppliers should consider including cross-subsidiary resource sharing and communications in business continuity plans to support emergency response and restoration.
7-7-0435	**ID Network Reliability Functions:** Network Operators, Service Providers, Equipment Suppliers and Property Managers should assess the functions of their organization and identify those critical to ensure network reliability.
7-7-0507	**Attack Trace Back:** Network Operators, Service Providers and Equipment Suppliers should have the processes and/or capabilities to analyze and determine the source of malicious traffic, and then to trace-back and drop the packets at, or closer to, the source. The references provide several different possible techniques. (Malicious traffic is that traffic such as Distributed Denial of Service (DDoS) attacks, smurf and fraggle attacks, designed and transmitted for the purpose of consuming resources of a destination of network to block service or consume resources to overflow state that might cause system crashes).
7-7-0513	Network Operators and Service Providers should maintain a 24 hours by 7 days contact list of other providers and operators for service restoration of inter-connected networks. Where appropriate, this information should shared with Public Safety Service and Support providers.
7-7-0541	Network Operators, Service Providers and Equipment Suppliers should store multiple software versions for critical network elements and be able to fallback to an earlier version.
7-7-0546	Network Operators and Service Providers should minimize single points of failure (SPOF) in paths linking network elements deemed critical to the operations of a network (with this design, two or more simultaneous failures or errors need to occur at the same time to cause a service interruption).
7-7-0584	Service Providers, Network Operators and Equipment Suppliers and Government representatives [of the National Security Emergency Preparedness (NS/EP) community] should work together to support appropriate industry and international organizations to develop and implement NS/EP standards in packet networks.
7-7-0587	Government, Network Operators and Service Providers of critical services to National Security and Emergency Preparedness (NS/EP) users should avail themselves of the Telecommunications Service Priority (TSP) program and support / promote as applicable.
7-7-0592	Network Operators and Service Providers should provide duplicated, non-co-located maintenance administration, surveillance and support for network elements. Monitoring and administration locations should be minimized to provide consistency of operations and overall management.
7-7-0599	Network Operators and Service Providers should conduct exercises periodically to test a network's operational readiness through planned drills or simulated exercises. The exercise should be as authentic as practical. Scripts should be prepared in advance and team members should play their roles as realistically as possible.
7-7-0609	Network Operators and Service Providers should provide and maintain the contact information for mutual aid coordination for inclusion in mutual aid processes.
7-7-0657	Network Operators, Service Providers and Property Managers should design standby generator systems for fully automatic operation and for ease of manual operation, when required.

7-7-0658	Network Operators, Service Providers and Property Managers should maintain adequate fuel on-site and have a well-defined re-supply plan. Generator life support systems (e.g., radiator fan, oil cooler fan, water transfer pumps, fuel pumps, engine start battery chargers) should be on the essential AC bus of the generator they serve.
7-7-0660	Network Operators, Service Providers and Property Managers should have a plan that is periodically verified for providing portable generators to offices with and without stationary engines.
7-7-0695	Network Operators, Service Providers and Property Managers should develop and test plans to address situations where normal power backup does not work (e.g., commercial AC power fails, the standby generator fails to start, automatic transfer switch fails).
7-7-1001	Network Operators, Service Providers, Equipment Suppliers and Property Managers should formally document their business continuity processes in a business continuity plan covering critical business functions and business partnerships. Key areas for consideration include: Plan Scope, Responsibility, Risk Assessment, Business Impact Analysis, Plan Testing, Training and Plan Maintenance.
7-7-1002	Network Operators, Service Providers and Equipment Suppliers should consider establishing a business continuity executive steering committee (composed of executive managers and business process owners) to ensure executive support and oversight.
7-7-1004	Network Operators, Service Providers, Equipment Suppliers and Property Managers should review their Business Continuity Plan(s) on an annual basis to ensure that plans are up-to-date, relevant to current objectives of the business and can be executed as written.
7-7-1005	Network Operators, Service Providers and Equipment Suppliers should perform a Business Impact Analysis (BIA) to assess the impact of the loss of critical operations, support systems and applications.
7-7-1008	Network Operators, Service Providers, and Equipment Suppliers should use the Incident Command System Standard for incident coordination and control in the emergency operations center and at the incident site.
7-7-1009	Network Operators, Service Providers and Equipment Suppliers should regularly conduct exercises that test their Disaster Recovery Plans. Exercise scenarios should include natural and man-made disasters (e.g., hurricane, flood, nuclear, biological, and chemical).
7-7-1010	Network Operators, Service Providers and Equipment Suppliers should designate personnel responsible for maintaining Business Continuity and Disaster Recovery Plans.
7-7-1011	Network Operators, Service Providers, Equipment Suppliers and Public Safety Authorities should establish alternative methods of communicationÃŸfor criticalÃŸpersonnel.
7-7-1015	Network Operators and Service Providers should make available to the disaster recovery team as-built drawings of network sites.
7-7-1018	Network Operators, Service Providers and Equipment Suppliers should emphasize employee and public safety during a disaster and all phases of disaster recovery.
7-7-1020	Network Operators, Service Providers and Equipment Suppliers should assess the need for Chemical, Biological, Radiological and Nuclear (CBRN) response program to safely restore or maintain service in the aftermath of fuel/chemical contamination or a Weapons of Mass Destruction (WMD) attack.
7-7-1023	Network Operators, Service Providers and Equipment Suppliers should identify essential staff within their organizations that are critical to disaster recovery efforts. Planning should address the availability of these individuals and provide for backup staff.
7-7-1024	Network Operators, Service Providers and Equipment Suppliers should plan for the possibility of a disaster occurring during a work stoppage.
7-7-1025	Network Operators and Service Providers should consider using a team to quickly determine appropriate actions both pro-active or re-active to address potential or real threats.
7-7-1026	Network Operators and Service Providers should consider creating a corporate policy statement that defines a remote system access strategy, which may include a special process for disaster recovery.
7-7-1028	Network Operators, Service Providers and Property Managers should engage in preventative maintenance programs for network site support systems including emergency power generators, UPS, DC plant (including batteries), HVAC units, and fire suppression systems.

7-7-1029	Network Operators and Service Providers should periodically review their portable power generator needs to address changes to the business.
7-7-1031	Network Operators and Service Providers should consider entering into Mutual Aid agreements with partners best able to assist them in a disaster situation using the templates provided on the NRIC and NCS websites. These efforts could include provisions to share spectrum, fiber facilities, switching, and/or technician resources.
7-7-1032	Network Operators and Service Providers should document their critical equipment suppliers, vendors, contractors and business partners in their Business Continuity Plans along with an assessment of the services, support, and capabilities available in the event of a disaster.
7-7-1035	Network Operators and Service Providers should include trial deployment of emergency mobile assets in disaster response exercises to evaluate level of personnel readiness.
7-7-1037	Network Operators, Service Providers, Equipment Suppliers and Public Safety Authorities should use a disaster recovery support model that provides a clear escalation path to executive levels, both internally and to business partners.
7-7-1040	Network Operators, Service Providers and Equipment Suppliers should consider using lab, demonstration or training equipment if replacement equipment is unavailable in disaster situations.
7-7-1045	Network Operators and Service Providers should use their escalation process, as needed, to address resource issues identified through damage and resource assessments.
7-7-1047	Network Operators and Service Providers should develop a process to routinely archive critical system backups and provide for storage in a secure off-site facility which would provide geographical diversity.
7-7-1048	Network Operators and Service Providers should consider supplementing media backup storage with full system restoral media and documented restoration procedures that can be utilized at an alternate hot site, in case of total failure of the primary service site.
7-7-1050	Network Operators and Service Providers should consider tertiary carrier/transport methods such as satellite, microwave or wireless to further reduce point of failures or as hot transport backup facilities.
7-7-1052	Network Operators and Service Providers should periodically assess the functionality of business critical systems during a disaster exercise.
7-7-1054	Network Operators, Service Providers and Property Managers should install fire detection systems and consider the use of suppression systems or devices at buildings supporting network functionality.
7-7-1058	Network Operators, Service Providers and Equipment Suppliers should work collectively with local, state, and federal governments to develop relationships fostering efficient communications, coordination and support for emergency response and restoration.
7-7-1061	Service Provider, Network Operators and Equipment Suppliers should ensure that Telecommunication Service Priority (TSP) records and data bases are reconciled annually.
07/07/5031	Network Operators, Service Providers and Equipment Suppliers should establish a role for the security function (i.e., physical and cyber) in business continuity planning, including emergency response plans and periodic tests of such plans.
07/07/5091	Network Operators, Service Providers and Equipment Suppliers should develop and implement, as appropriate, travel security awareness training and briefings before traveling internationally.
07/07/5095	Network Operators, Service Providers, Equipment Suppliers and Property Managers should implement a tiered security response plan for communications facilities that recognizes the threat levels identified in the Homeland Security Advisory System.
07/07/5107	Network Operators, Service Providers and Equipment Suppliers should evaluate and manage risks (e.g., alternate routing, rapid response to emergencies) associated with a concentration of infrastructure components.
07/07/5112	Network Operators, Service Providers and Equipment Suppliers should, at the time of the event, coordinate with the appropriate local, state, or federal agencies to facilitate timely access by their personnel to establish, restore or maintain communications, through any governmental security perimeters (e.g., civil disorder, crime scene, disaster area).
07/07/5160	Network Operators, Service Providers, Equipment Suppliers and Property Managers should account for the possible absence of critical personnel in their business continuity plan.

07/07/5221	Network Operators, Service Providers and Equipment Suppliers should consider limiting the dissemination of information relating to future locations of key leadership.
07/07/5222	Network Operators, Service Providers and Equipment Suppliers should consider providing trouble call centers with a physically diverse back-up capability that can quickly be configured to receive the incoming traffic and take appropriate action.
07/07/5223	Network Operators, Service Providers and Equipment Suppliers should establish a plan for providing technical support that prevents the loss of one facility or location from disabling their ability to provide support.
07/07/5225	Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure that Business Continuity Plan(s) are restricted to those with a need-to-know.
07/07/5267	Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure that operating procedures are clearly defined, and followed by personnel during emergency situations in order to avoid degradation of cyber and physical security due to a diversion.
07/07/5271	Network Operators and Service Providers should consider physical and cyber security issues in Mutual Aid Agreements (e.g., authorization, access control, badging).
07/07/5275	Network Operators, Service Providers and Equipment Suppliers should consider backup power capabilities for Command and Control (Crisis Teams) so that communications and access to critical systems can be maintained in the event of a significant disruption to commercial power.
07/07/8007	**Define Security Architecture(s):** Network Operators and Service Providers should develop formal written Security Architecture(s) and make the architecture(s) readily accessible to systems administrators and security staff for use during threat response. The Security Architecture(s) should anticipate and be conducive to business continuity plans.
07/07/8061	**IR (Incident Response) Procedures:** Network Operators and Service Providers should establish a set of standards and procedures for dealing with computer and network security events. These procedures can and should be part of the overall business continuity/disaster recovery plan. Where possible, the procedures should be exercised periodically and revised as needed. Procedures should cover likely
07/07/8089	**Conduct Risk Assessments to Determine Appropriate Security Controls:** Network Operators, Service Providers and Equipment Suppliers should perform a risk assessment of all systems and classify them by the value they have to the company, and the impact to the company if they are compromised or lost. Based on the risk assessment, develop a security policy which recommends and assigns the appropriate controls to protect the system.
07/07/8131	**Include Security Incidents in Business Recovery Plan:** A Network Operator's or Service Provider's Business Recovery Plan should factor in potential Information Security threats of a plausible likelihood or significant business impact.
07/07/8132	**Leverage Business Impact Analysis for Incident Response Planning:** Network Operators and Service Providers should leverage the Business Continutiy Planning/Disaster Recovery (BCP/DR) Business Impact Assessment (BIA) efforts as input to prioritizing and planning Information and/or Physical Security Incident Response efforts.
07/07/8549	**Lack of Business Recovery Plan:** When a Business Recovery Plan (BRP) does not exist, Network Operators and Service Providers should bring together an ad-hoc team to address the current incident. The team should have technical, operations, legal, and public relations representation. Team should be sponsored by senior management and have a direct communication path back to management sponsor. If situation exceeds internal capabilities consider contracting response/recovery options to 3rd party security provider.

PAGINA EN BLANCO

10 ANEXO 3 BUENAS PRÁCTICAS VOLUNTARIAS EUROPEAS

(FUENTE: AVAILABILITY AND ROBUSTNESS OF ELECTRONIC COMMUNICATIONS INFRASTRUCTURES FINAL REPORT FEBRUARY 2007, ALCATEL LUCENT)

	POWER BEST PRACTICES
EU06-5231	Network Operators, Service Providers, Equipment Suppliers and Property Managers should develop documentation for the restoration of power for areas of critical infrastructure including such things as contact information, escalation procedures, restoration steps and alternate means of communication. This documentation should be maintained both on-site and at centralized control centres.
EU06-0492	Network Operators should provide back-up power (e.g., some combination of batteries, generator, fuel cells) at cell sites and remote equipment locations, consistent with the site specific constraints, criticality of the site, the expected load and reliability of primary power.
EU06-0650	Network Operators, Service Providers and Property Managers should place strong emphasis on human activities related to the operation of power systems (e.g., maintenance procedures, alarm system operation, response procedures, and training) for operations personnel.
EU06-0657	Network Operators, Service Providers and Property Managers should design standby generator systems for fully automatic operation and for ease of manual operation, when required.
EU06-0662	Network Operators, Service Providers and Property Managers should exercise power generators on a routine schedule in accordance with manufacturers specifications. For example, a monthly 1 hour engine run on load, and a 5 hour annual run.
EU06-0695	Network Operators, Service Providers and Property Managers should develop and test plans to address situations where normal power backup does not work (e.g., commercial AC power fails, the standby generator fails to start, automatic transfer switch fails).
EU06-0773	Network Operators, Service Providers and Property Managers should perform annual capacity evaluation of power equipment, and perform periodic scheduled maintenance, including power alarm testing.
EU06-1029	Network Operators and Service Providers should periodically review their portable power generator needs to address changes to the business.
EU06-5204	Service Providers, Network Operators and Property Managers should ensure availability of emergency/backup power (e.g., batteries, generators, fuel cells) to maintain critical communications services during times of commercial power failures, including natural and manmade occurrences (e.g., earthquakes, floods, fires, power brown/black outs, terrorism). The emergency/backup power generators should be located onsite, when appropriate.
EU06-5206	Network Operators, Service Providers and Property Managers should maintain sufficient fuel supplies for emergency/backup power generators running at full load to allow for contracted refuelling.
EU06-5208	Network Operators, Service Providers, Equipment Suppliers and Property Managers should ensure that electrical work (e.g., AC and high current DC power distribution) is performed by qualified technicians.
EU06-5212	Network Operators, Service Providers and Property Managers should consider placing generator sets and fuel supplies for critical sites within a secured area to prevent unauthorized access, reduce the likelihood of damage and/or theft, and to provide protection from explosions and weather.
EU06-5213	Network Operators, Service Providers and Property Managers should, where feasible, place fuel tanks in a secured and protected area. Access to fill pipes, fuel lines, vents, manways, etc. should be restricted (e.g., containment by fencing, walls, buildings, buried) to reduce the possibility of unauthorized access.
EU06-5232	Network Operators, Service Providers, and Property Managers should test fuel reserves used for standby or backup power for contamination at least once a year or after any event (e.g., earth tremor, flood) that could compromise the integrity of the tank housing, fill pipe or supply pipe.

	HARDWARE BEST PRACTICES
EU06-0428	Software & Hardware Vulnerability Tracking: Service Providers should monitor software and hardware vulnerability reports and take the recommended action(s) to address problems, where appropriate. These reports and recommendations are typically provided by equipment suppliers and CERTs (Computer Emergency Response Teams).
EU06-0459	Equipment Suppliers should design outdoor equipment (e.g., base station) to operate in expected environmental conditions (e.g., weather, earthquakes).
EU06-0614	Equipment Identification: Network Operators, Service Providers and Equipment Suppliers should position the equipment designation information (e.g., location, labels, RFID tags) so that they are securely affixed. The equipment designation should not be placed on removable parts such as covers, panels, doors, or vents that can be removed and mistakenly installed on a different network element.
EU06-5083	Network Operators, Service Providers and Equipment Suppliers should maintain the availability of spares for critical network systems.
EU06-5118	Equipment Suppliers of critical network elements should test electronic hardware to ensure its compliance with design criteria for tolerance to electromagnetic energy, shock, vibration, voltage spikes, and temperature.
EU06-5200	Network Operators, Service Providers and Equipment Suppliers should establish and implement procedures for the proper disposal and/or destruction of hardware (e.g., hard drives) that contain sensitive or proprietary information.
EU06-5283	Equipment Suppliers should provide network element thermal specifications or other special requirements in order to properly size Heating, Ventilation, and Air Conditioning (HVAC) systems.

	SOFTWARE BEST PRACTICES
EU06-0430	Software Configurations: Equipment Suppliers should be able to recreate supported software from source and, where feasible, software obtained from third parties.
EU06-5121	Network Operators, Service Providers and Equipment Suppliers should develop and consistently implement software delivery procedures that protect the integrity of the delivered software in order to prevent software loads from being compromised during the delivery process.
EU06-8020	Expedited Security Patching: Network Operators, Service Providers and Equipment Suppliers should have special processes and tools in place to quickly patch critical infrastructure systems when important security patches are made available. Such processes should include determination of when expedited patching is appropriate and identifying the organizational authority to proceed with expedited patching. This should include expedited lab testing of the patches and their affect on network and component devices.
EU06-8034	Software Patching Policy: Network Operators and Service Providers should define and incorporate a formal patch/fix policy into the organization's security policies.
EU06-8035	Software Patch Testing: The patch/fix policy and process used by Network Operators and Service Providers should include steps to appropriately test all patches/fixes in a test environment prior to distribution into the production environment.

	NETWORK BEST PRACTICES
EU06-0401	Network Surveillance: Network Operators and Service Providers should monitor the network to enable quick response to network issues.
EU06-0405	Network Performance: Network Operators and Service Providers should periodically examine and review their network to ensure that it meets the current design specifications.
EU06-0407	NOC Communications: Network Operators and Service Providers should establish processes for NOC-to-NOC (Network Operations Centre) peer communications for critical network activities (e.g., scheduled maintenance, upgrades and outages).
EU06-0415	Data Back-up Verification: Network Operators and Service Providers should test the restoral process associated with critical data back-up, as appropriate. The goal is to demonstrate that data restoration is complete and works as expected.
EU06-0501	Network Operators and Service Providers should report problems discovered from their operation of network equipment to the Equipment Supplier whose equipment was found to be the cause of problem.
EU06-0510	Network Operators, Service Providers and Equipment Suppliers should, by design and practice, manage critical Network Elements (e.g., Domain Name Servers, Signaling Servers) that are essential for network connectivity and subscriber service as critical systems (e.g., secure, redundant, alternative routing).
EU06-0513	Network Operators and Service Providers should maintain a "24 hours by 7 days" contact list of other providers and operators for service restoration of inter-connected networks. Where appropriate, this information should shared with Public Safety Service and Support providers.
EU06-0532	Diversity Audit: Network Operators should periodically audit the physical and logical diversity called for by network design and take appropriate measures as needed.
EU06-0546	Network Operators and Service Providers should minimize single points of failure (SPOF) in paths linking network elements deemed critical to the operations of a network (with this design, two or more simultaneous failures or errors need to occur at the same time to cause a service interruption).
EU06-0590	Network Operators, Service Providers and Equipment Suppliers should prepare Methods of Procedure (MOPs) for core infrastructure hardware and software growth and change activities as appropriate.
EU06-0595	Network Operators and Service Providers should be aware of the dynamic nature of peak traffic periods and should consider scheduling potentially service-affecting procedures (e.g., maintenance, high risk procedures, growth activities) so as to minimize the impact on end-user services.
EU06-0599	Network Operators and Service Providers should conduct exercises periodically to test a network's operational readiness through planned drills or simulated exercises. The exercise should be as authentic as practical. Scripts should be prepared in advance and team members should play their roles as realistically as possible.
EU06-0600	Network Operators and Service Providers should establish and document a process to plan, test, evaluate and implement major change activities onto their network.
EU06-0603	Schedule System Backups: Network Operators and Service Providers should establish policies and procedures that outline how critical network element databases will be backed up onto a storage medium (e.g., tapes, optical diskettes) on a scheduled basis.
EU06-0612	Network Operators and Service Providers should verify both local and remote alarms and remote network element maintenance access on all new critical equipment installed in the network, before it is placed into service.
EU06-0628	Network Operators and Service Providers should develop and implement defined procedures for removal of unused equipment and cable (e.g., cable mining) if this work can be economically justified without disrupting existing service.
EU06-0731	Network Operators should provide physical diversity on critical inter-office routes when justified by a risk or value analysis.

	NETWORK BEST PRACTICES
EU06-0761	Network Operators and Service Providers should conduct periodic verification of the office synchronization plan and the diversity of timing links, power feeds and alarms.
EU06-5075	Network Diversity: Network Operators and Service Providers should ensure that networks built with redundancy are also built with geographic separation where feasible (e.g., avoid placing mated pairs in the same location and redundant logical facilities in the same physical path).

	PAYLOAD BEST PRACTICES
EU06-0449	Network Operators and Service Providers should, where feasible, deploy SPAM controls in relevant nodes (e.g., message centers, email gateways) in order to protect critical network elements and services.
EU06-0507	Attack Trace Back: Network Operators, Service Providers and Equipment Suppliers should have the processes and/or capabilities to analyze and determine the source of malicious traffic, and then to trace-back and drop the packets at, or closer to, the source. The references provide several different possible techniques. (Malicious traffic is that traffic such as Distributed Denial of Service (DDoS) attacks, smurf and fraggle attacks, designed and transmitted for the purpose of consuming resources of a destination of network to block service or consume resources to overflow state that might cause system crashes).
EU06-0520	Network Operators and Service Providers should have a route policy that is available, as appropriate. A consistent route policy facilitates network stability and inter-network troubleshooting.
EU06-0805	Service Providers, Network Operators and Equipment Suppliers should work to establish operational standards and practices that support broadband capabilities and interoperability (e.g., video, voice, data, wireless).
EU06-0814	For the deployment of Residential Internet Access Service, Broadband Network Operators should design in the ability to take active measures to detect and restrict or inhibit any network activity that adversely impacts performance, security, or usage policy.
EU06-0822	For the deployment of Residential Internet Access Service, a Broadband Network Operator should incorporate multilevel security schemes for network data integrity, as applicable, in the network design to prevent user traffic from interfering with network operations, administration, and management use.
EU06-5149	Network Operators, Service Providers and Equipment Suppliers should, where feasible, ensure that intentional emissions (e.g., RF and optical) from network equipment and transmission facilities are secured sufficiently to ensure that monitoring from outside the intended transmission path or beyond facility physical security boundaries cannot lead to the obtaining of critical network operations information.
EU06-8007	Define Security Architecture(s): Network Operators and Service Providers should develop formal written Security Architecture(s) and make the architecture(s) readily accessible to systems administrators and security staff for use during threat response. The Security Architecture(s) should anticipate and be conducive to business continuity plans.
EU06-8008	Network Architecture Isolation/Partitioning: Network Operators and Service Providers should implement architectures that partition or segment networks and applications using means such as firewalls, demilitarized zones (DMZ), or virtual private networks (VPN) so that contamination or damage to one asset does not disrupt or destroy other assets. In particular, where feasible, it is suggested the user traffic networks, network management infrastructure networks, customer transaction system networks, and enterprise communication/business operations networks be separated and partitioned from one another.
EU06-8056	Operational Voice over IP (VoIP) Server Hardening: Network Operators should ensure that network servers have authentication, integrity, and authorization to prevent inappropriate use of the servers. Enable logging to detect inappropriate use.
EU06-8073	Intrusion Detection/Prevention (IDS/IPS) Tools Deployment: Network Operators and Service Providers should deploy Intrusion Detection/Prevention Tools with an initial policy that reflects the universe of devices and services known to exist on the monitored network. Due to the ever evolving nature of threats, IDS/IPS tools should be tested regularly and tuned to deliver optimum performance and reduce false positives.
EU06-8092	Adopt and Enforce Acceptable Use Policy: Network Operators and Service Providers should adopt a customer-directed policy whereby misuse of the network would lead to measured enforcement actions up to and including termination of services.
EU06-8111	Protect Sensitive Data in Transit for Externally Accessible Applications: Network Operators and Service Providers should encrypt sensitive data from web servers, and other externally accessible applications, while it is in transit over any networks they do not physically control.

	POLICY BEST PRACTICES
EU06-0505	Network Operators and Service Providers should have procedures in place to process court orders and subpoenas for wire taps or other information.
EU06-0508	Network Operators and Service Providers should establish company-specific interconnection agreements, and where appropriate, utilize existing interconnection templates and existing data connection trust agreement.
EU06-0803	Network Operators, Service Providers and Equipment Suppliers are encouraged to continue to participate in the development and expansion of industry standards for traffic management that promote interoperability and assist in meeting end user quality of service needs.
EU06-1032	Network Operators and Service Providers should document their critical equipment suppliers, vendors, contractors and business partners in their Business Continuity Plans along with an assessment of the services, support, and capabilities available in the event of a disaster.
EU06-1058	Network Operators, Service Providers and Equipment Suppliers should work collectively collectively with regional, and national governments as well as European agencies to develop relationships fostering efficient communications, coordination and support for emergency response and restoration.
EU06-5070	Network Operators, Service Providers and Equipment Suppliers should consider establishment of a senior management function for a chief security officer (CSO) or functional equivalent to direct and manage both physical and cyber security.
EU06-5071	In order to prepare for contingencies, Network Operators, Service Providers and Property Managers should maintain liaison with local law enforcement, fire department and other security and emergency agencies to exchange critical information related to threats, warnings and mutual concerns.
EU06-5100	Network Operators, Service Providers and Equipment Suppliers should interact as needed with regional, and national governments as well as European agencies to identify and address potential adverse security impacts of new laws and regulations (e.g., exposing vulnerability information, required security measures, fire codes).
EU06-5110	Network Operators should not share information pertaining to the criticality of individual communication facilities or the traffic they carry, except with trusted entities for justified specific purposes with appropriate protections against further disclosure.
EU06-5112	Network Operators, Service Providers and Equipment Suppliers should, at the time of the event, coordinate with the appropriate regional, and national governments as well as European agencies to facilitate timely access by their personnel to establish, restore or maintain communications, through any governmental security perimeters (e.g., civil disorder, crime scene, disaster area).
EU06-5226	Network Operators, Service Providers and Property Managers should maintain liaison with local law enforcement, fire department, other utilities and other security and emergency agencies to ensure effective coordination for emergency response and restoration.
EU06-5265	Network Operators', Service Providers', Equipment Suppliers' and Property Managers' senior management should actively support compliance with established corporate security policies and procedures.
EU06-8065	Sharing Information with Law Enforcement: Network Operators, Service Providers and Equipment Suppliers should establish a process for releasing information to members of the law enforcement and intelligence communities and identify a single Point of Contact (POC) for coordination/referral activities.

PAGINA EN BLANCO

11 REFERENCIAS

- Alcatel-Lucent Technologies. (2007). *Availability and Robustness of Electronic Communications Infrastructures*. European Commission, Information Society and Media, Directorate General. http://ec.europa.eu/information_society/index_en.htm
- Dirección de Gestión de Riesgos - Corporación Osso. (2009). *Estudio de vulnerabilidad física y funcional a fenómenos volcánicos en el área de influencia del volcán Galeras*. Bogotá D.C.: Ministerio del Interior y de la Justicia.
- Dwyer, A., Zoppou, C., Nielsen, O., Day, S. & Roberts, S. (2004). *Quantifying Social Vulnerability: A methodology for identifying those at risk to natural hazards Natural Hazard.* Canberra: Australian Government. http://www.ga.gov.au/image_cache/GA4267.pdf
- Human, Roy; Palit, Manasi; Simpson, David. *Improving Risk Assessment Methodology: The University of Louisville and the Disaster Resistant University (DRU) Program*. Louisville: Center for Hazards Research and Policy Development University of Louisville. http://hazardcenter.louisville.edu/pdfs/wp0503.pdf
- Kienberger, Stefan. *Assessing the Vulnerability to Natural Hazards on the Provincial/Community Level in Mozambique: The Contribution of Giscience and Remote Sensing*. Salzburg: Centre for Geoinformatics - Salzburg University.
- Luiijf, Eric; Burger, Helen; Klaver, Marieke. *Critical (information) Infrastructure Protection in The Netherlands*. The Hague, The Netherlands: TNO Physics and Electronics Laboratory (TNO-FEL). http://subs.emis.de/LNI/Proceedings/Proceedings36/GI-Proceedings.36-1.pdf

- Luiijf, H.A.M.; Klaver, M.H.A. (2000). *Vulnerability of the Netherlands ICT-infrastructure and consequences for the information society*. INFODROME (http://www.infodrome.nl)
- Ministerio de las Tecnologías de la Información y las Comunicaciones. (2010). *Cuadro Nacional de Atribución de Frecuencias*. Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones.
- Moore, Alexandra; Hancock, Ken; Stacey, Roger; Stacey, Paul. (2001). *The Vulnerability of Mobile Telecommunications to Natural Hazard*. Ottawa: Office of Critical Infrastructure Protection and Emergency Preparedness. http://dsp-psd.pwgsc.gc.ca/collection_2008/ps-sp/D82-82-2003E.pdf
- New York State Department of Public Service Office of Communications. (2002). *Network Reliability After 9/11*. New York: New York State Department of Public Service Office of Communications. http://www.neutraltandem.com/documents/NetworkReliability.pdf
- OCHA Colombia. (2010).*Natural Disasters and Emergencies Floods, Landslides and Avalanches*. Bogotá D.C.: Oficina para la Coordinación de Asuntos Humanitarios - Naciones Unidas Colombia. http://www.colombiassh.org/site/
- Pedraza, William. (2010). *Documento de Alcance - Atención de desastres*. Bogotá. D.C.: Ministerio de las Tecnologías de la Información y las Comunicaciones.
- Posas, Paula; Bender, Stephen. (2004). *Managing Natural Hazard Risk: Issues and Challenges.* Organization of American States Unit for Sustainable Development & Environment. http://www.oas.org/dsd/policy_series/4_eng.pdf

- Tanislav, Dan; Costache, Andra; Murătoreanu, George.(2009). *Vulnerability to Natural Hazards in Romania*.Forum Geografic. Studii şi cercetări de geografie şi protecția mediului.
- Townsend, Anthony; Moss, Mitchell (2005). *Telecommunications infrastructure in disasters*: *Preparing Cities for Crisis Communications.* New York: Center for Catastrophe Preparedness and Response & Robert F. Wagner Graduate School of Public Service New York University. http://www.nyu.edu/ccpr/pubs/NYU-DisasterCommunications1-Final.pdf
- United States Government Accountability Office. (2009). *Vulnerabilities Remain and Limited Collaboration and Monitoring Hamper Federal Efforts.* Washington: United States Government Accountability Office. http://www.gao.gov/new.items/d09604.pdf
- Utne, I.; Hokstad, P.; Kjølle, G.; Vatn, J.; Tøndel, I. A.; Bertelsen, D.; Fridheim, H.; Røstum J. *Risk and Vulnerability Analysis of Critical Infrastructures - The DECRIS Approach*. Trondheim: Norwegian University of Science and Technology.
- Zimmerman, Rae. (2007). *Allocation of Resources for Risk Management*. New York: New York University. http://create.usc.edu/research/past_projects/NYU2007-AllocationofResourcesforRiskManagement.pdf
- Información del Ministerio de Tecnologías de la Información y las Comunicaciones de la República de Colombia y del Centro de Investigación de las Telecomunicaciones - CINTEL dispuesta en el marco del proyecto.