UNIVERSIDAD EAN

DESARROLLO DE UNA METODOLOGÍA PARA GESTIONAR RIESGOS DE DESASTRES, EN EMPRESAS QUE OFRECEN SERVICIOS PÚBLICOS DE INTERNET, TELEFONÍA FIJA, Y MÓVIL, EN CUMPLIMIENTO DE LA LEY 1523 DE 2012 Y DEL DECRETO 2157 DEL 2017

LUISA GRACIELA ARCINIEGAS ZAMORA

UNIVERSIDAD EAN
ESPECIALIZACIÓN DE GERENCIA DE PROYECTOS DE TECNOLOGÍA
SEMINARIO DE INVESTIGACIÓN
2018

DEDICATORIA

Este trabajo está dedicado a mi hija Andrea Camila Ponce Arciniegas, quien es la persona que más amo en mi vida, también dedico este trabajo a Alexander García Pérez, quien me apoyó a lo largo de mi especialización y sé que sin su apoyo no hubiera sido tan constructivo el paso por la Universidad EAN.

También agradezco a Dios por esta realización y por el conocimiento recibido en esta especialización.

TABLA DE CONTENIDO

1. PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

Actualmente en Colombia, todas aquellas empresas que realizan actividades que generen riesgos de desastre están obligadas a gestionar planes de Gestión de Riesgo de Desastres.

Ejemplo de este tipo de empresas son aquellas que prestan servicios públicos, planifican o ejecutan obras civiles de gran impacto social, empresas que transporten o almacenan carga o realicen construcciones de alta complejidad, tales empresas están obligadas a formular y ejecutar un Plan de Gestión del Riesgo de Desastres, por medio del cual deben: "Identificar, establecer, implementar y monitorear las acciones necesarias para conocer y reducir las condiciones de riesgo de sus instalaciones y de aquellas derivadas de su propia actividad que generen amenaza para su propia realización o del entorno ambiental y social.

Las empresas deben así, dar respuesta a los desastres que puedan presentarse, permitiendo además su articulación con los sistemas de gestión locales, municipales y nacionales de la gestión del riesgo de desastre estipulados en la Ley 1523 de 2012 para la gestión del riesgo de desastres y el decreto 2157 del 2017, documentos que indican las directrices generales para la elaboración del Plan de Gestión del Riesgo de desastres de las entidades públicas y privadas.

En el caso de empresas de Telecomunicaciones se debe cumplir tanto la gestión de riesgos de desastres ambientales (desastres causados accidental o intencionalmente por

personas) como la gestión de riesgos de desastres que infraestructuras expuestas o críticas pudiesen ocasionar sobre poblaciones que dependen de estos servicios ya sea que esa dependencia sea ocasionada por vivir o trabajar en las áreas de influencia de las estructuras o por depender del servicio que es vital para el normal desempeño de tales poblaciones,

es fundamental por tanto que las empresas de Telecomunicaciones posean una metodología de gestión de los riesgos anteriormente nombrados.

2. JUSTIFICACIÓN

El presente trabajo de investigación se propone en establecer una metodología de aplicación de la ley 1523 del 2012 y del Decreto 2157 del 2017 para empresas de que proveen servicios de internet y telefonía local y móvil y que requieran implementar un modelo de Gestión de Riesgos de Desastres.

Este tipo de organizaciones necesita una metodología de referencia dado que en Colombia la probabilidad de que ocurran desastres ambientales es alta por la geografía que caracteriza al país.

El segmento de las telecomunicaciones ocupa uno de los primeros escalones de la economía mundial, este mercado incluye comunicaciones de voz, datos, imágenes y video, que viajan por tierra, mar y aire; donde las redes información se convierten en el sistema nervioso de la sociedad y se definen como infraestructuras fundamentales para el normal desenvolvimiento de las actividades de las naciones del mundo.

En consecuencia, las telecomunicaciones conforman uno de los más importantes sectores que fundamentan, no solo las comunicaciones públicas para todos los habitantes del territorio nacional sino también las comunicaciones de las entidades territoriales y del Gobierno, y organismos de socorro en casos de emergencia o desastre.

Es así que las redes públicas de telecomunicaciones corren gran riesgo de quedar colapsadas e interrumpidas en los instantes que siguen a las catástrofes naturales. La pérdida de comunicación genera por si misma 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 y para conectarse con 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, dentro y fuera de la zona de emergencia.

No se puede prestar una asistencia humanitaria adecuada si no funcionan las telecomunicaciones en la zona de emergencia, y estas resultan esenciales para 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 que impiden prestar adecuadamente los servicios de asistencia humanitaria y operaciones de búsqueda, salvamento y rescate. Así mismo se dificultan enormemente las operaciones de emergencia por parte de las autoridades

en la medida en que las comunicaciones colapsan.

3. OBJETIVOS

3.1. Objetivo General

Realizar una investigación sobre los documentos y normativas existentes que permitan modelar una metodología de gestión de riesgos de desastres para empresas de Telecomunicaciones en Colombia a implementar de Sistema de Gestión de Riesgo de Desastres en el marco de las exigencias de la ley 1523 de 2012 , el Decreto 2157 del 2017.

3.2. Objetivos Específicos

3.1.1. Establecer las exigencias legales de ley 1523 del 2102, el decreto 2157 del 2017, para determinar que se debe estudiar, analizar, implementar, medir y mejorar para el cumplimiento cabal de las mismas dentro de empresas de Telecomunicaciones.

3.1.2. Modelar una metodología para la gestión de riesgos de desastres según lo exigido por la ley fundamentado en el estado del arte realizado por otros autores en Colombia y América Latina.

4. MARCO TEÓRICO

Los sistemas de prestación de servicios públicos en sus diferentes componentes se encuentran en constante interacción con el entorno y por tanto es de vital importancia analizar

como el entorno puede representar en dado momento una amenaza y generar afectación en la infraestructura de prestación de los servicios y a su vez ocasionar un impacto en efecto dominó sobre las poblaciones circundantes.

Los factores de riesgo de las infraestructuras pueden ser determinados por deficiencias en el diseño, instalación y funcionamiento de los sistemas de prestación de servicios públicos y desestabilización de terrenos, procesos de contaminación de fuentes hídricas, contaminación del suelo, enfermedades de transmisión hídrica por mal manejo de desechos, incidentes terroristas o accidentes involuntarios del personal que maneja las infraestructuras.

También se consideran riesgos aquellos que se desencadenan por la ausencia de prestación del servicio público de comunicaciones y que en una situación de emergencia pueden hacer más crítica la situación de desastre.

La ley 1523 para gestión de desastres se sancionó en 2012 , pero dadas las emergencias por fenómenos naturales en Colombia, la presidencia de la República estableció el decreto 2157 de 2017 para agilizar la gestión de riesgos de desastres en Colombia, debido a la sucesión continua de catástrofes de impacto ambiental, social y financiero que se han presentado en los últimos años y para las cuales no se ha concretado planes efectivos para reparar todos los daños causados sino más bien, el país ha tenido que aceptar todas las pérdidas multimillonarias ante imposibilidad de reacción y recuperación de las actividades ante la materialización de los desastres.

Los programas de Gestión del Riesgo de Desastres deben incluir todas las estrategias

para lograr un adecuado conocimiento de los riesgos, que lleven a estructurar las obras y actividades para la reducción del riesgo y planificar el manejo de las posibles consecuencias; este último aspecto a su vez permite a los prestadores de servicios dar cumplimiento a las normas vigentes en lo relacionado con la formulación de planes de contingencia o planes operacionales de emergencia.

Dentro de los trabajos ya realizados por el Gobierno se encuentran documentos realizados por Mintic como el Diseño de red de telecomunicaciones de emergencia realizado por el Consorcio ITELCA para Mintic en 2013, también Mintic ha diseñado un sistema de telecomunicaciones de Emergencia Nacional, por tanto esos trabajos son referentes para el presente estudio y se analizarán para sugerir una posible metodología de Gestión de Riesgo de Desastres para proveedores de Telecomunicaciones en Internet, telefonía Local y Telefonía Móvil en Colombia.

5. METODOLOGÍA

El presente trabajo de investigación plantea un problema de estudio delimitado y concreto teniendo en cuenta investigaciones anteriores en el país sobre Gestión de Riesgos de Desastres para empresas de Telecomunicaciones.

La metodología de la presente investigación es de carácter teórica, cualitativa y exploratoria, está fundamentada en análisis de trabajos ya realizados en Gestión de riesgos de desastres cuyas fuentes de consulta se encuentran públicas en internet y que corresponden a documentos publicados por Mintic y cuyo análisis en el presente trabajo no

ocasiona violación a la propiedad intelectual, pues los documentos públicos no representan para quien los analiza amenaza sobre uso de propiedad intelectual. Los resultados de la investigación serán cualitativos, se utilizará la metodología ISO 31000 para Gestión del Riesgo aplicada a la gestión de Riesgo de Desastres, por tanto, se espera que como resultado de la investigación se pueda formular una plantilla de gestión de riesgos acorde al contexto de las empresas que ofrecen este tipo de servicios y relacionada con las exigencias del marco legal del presente trabajo.

5.1 Alcance

En primera instancia se hará un análisis documental de las leyes y decretos y sus exigencias y posteriormente se propondrán plantillas de Gestión del Riesgo que puedan abarcar al máximo los requerimientos de tales leyes y decretos, tal es el caso de Riesgos de Desastres que afecten la telefonía fija, móvil e internet.

Posteriormente se plantearán plantillas para amenazas de desastres naturales fundamentadas en los riesgos de vulnerabilidad social y exposición al riesgos de la población en el entorno de las infraestructuras de Telecomunicaciones.

Posteriormente y tomando como fundamento estas amenazas se planteará una metodología para gestión de riesgos de desastres para empresas de Telecomunicaciones.

5.2 Pregunta de investigación

La pregunta de investigación para el presente trabajo es:

Es posible mediante los trabajos hechos por MINTIC formular una metodología de Gestión de Riesgos de desastres para empresas que ofrecen servicios públicos, específicamente servicios de Telefonía fija, móvil e internet, de acuerdo a la ley 1523 de 2012 y el decreto 2157 de 2017

5.3. Variables

Las variables de la investigación son: Amenazas de desastres naturales en Colombia y riesgos de desastres.

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.

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.

5.4. Pasos de la metodología

1. Análizar y Síntetizar de la Ley 1523 de 2012, el decreto 2157 de 2017 por información pública de fuentes MinTIC , UNGRD, IDEAM, SGC, DIMAR, Informes, anexos y levantamiento de información.
2. Análisis del documento Diseño de una Red de Telecomunicaciones de Emergencia creado por MINTIC.

3. Sugerencia de una posible metodología de Riesgo de Desastres propuesta.

5.5. Estructura del diseño metodológico

La Ilustración 1 representa la estructura de trabajo metodológico, la cual consta tres fases:

FASE 1: recolección de información de fuentes primarias, provenientes de documentos sobre Gestión de Desastres en Colombia, de estos documentos proviene los requerimientos y bases establecidas por el Gobierno para el desarrollo de la metodología propuesta en el siguiente trabajo.

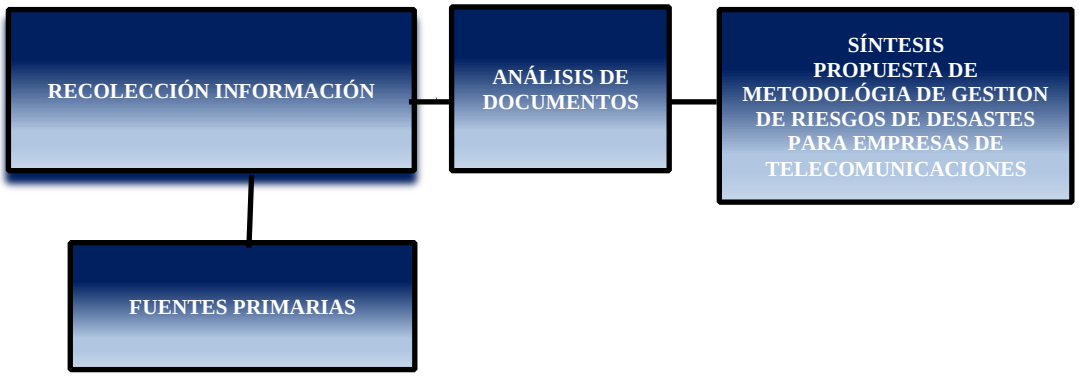


Ilustración 1. Estructura del diseño metodológico de la investigación

5.6. Fuentes primarias de información

Fuentes primarias**:** Estudio y análisis de trabajos de documentos Gubernamentales y metodologías de gestión de riesgos de desastres en países con riesgos de desastres similares a Colombia.

6. INSTRUMENTO DE RECOLECCION DE DATOS

El instrumento de recolección de datos se define de la siguiente manera, en la siguiente tabla se identifica el requerimiento y el documento pertinente a indagar para encontrar la información que se resumen en la tabla No. 1.

DOCUMENTO A ANALIZAR	ELEMENTOS BUSCADOS
Decreto 2137 de 2017	Lineamientos de implementación de un Sistema de Gestión de Desastres para empresas de Telecomunicaciones
Ley 1523 del 2012	Lineamientos de implementación de un Sistema de Gestión de Desastres para empresas de Telecomunicaciones
Información cartográfica suministrada por el Instituto Geográfico Agustín Codazzi (IGAC): Cartografía de Colombia escala 1:500.000; Cartografía de Colombia escala 1:100.000.	Estudio de amenazas Naturales en Colombia, su objetivo es determinar cuales son las ciudades o municipios con riesgos de desastres en los que se debe enfocar la gestión inmediata del riesgo.
Diseño de red una red de Teleco-municaciones de emergencia naturales desastrosos – MinTIC.	Determinar cuales son las amenzas de la red de proveedores de Telefonia Fija, Internet y Telefonía Movil.

Tabla 1. Instrumento de Recolección de datos

6.1. Presentación y análisis de documentos

6.1.1 Documento de estudio ley 1523 2012

Documento recuperado de:
http://www.ideam.gov.co/documents/24189/390483/11.+LEY+1523+DE+2012.pdf/4e93527d-3bb8-4b53-b678-fbde8107d340?version=1.2

De acuerdo al artículo 42 de la ley 1523 de 2012 si una entidad pública o privada presta servicios públicos, planifica o ejecuta obras civiles, desarrolla actividades industriales u otras que puedan ocasionar un riesgo de desastres para la sociedad y el ambiente, transporta o almacena carga, planifica o realiza construcciones bajo categorías IV de alta complejidad o es responsable de espacios físicos que generan aglomeraciones, entonces este tipo de entidad debe formular un plan de gestión de Riesgo de desastres, mediante el cual debe "identificar, priorizar, formular, programar y hacer seguimiento a las acciones necesarias para conocer y reducir las condiciones de riesgo (actual y futuro) de sus instalaciones y de aquellas derivadas de su propia actividad u operación que pueden generar daños y pérdidas a su entorno, así como dar respuesta a los desastres que puedan presentarse, permitiendo además su articulación con los sistemas de gestión de la entidad, los ámbitos territoriales, sectoriales e institucionales de la gestión del riesgo de desastre y los demás instrumentos de planeación estipulados en la Ley 1523 de 2012 para la gestión del riesgo de desastres.

De acuerdo a este decreto las entidades que prestan servicios públicos de internet, telefonía local y móvil, deben ser responsables de prestar sus servicios de forma continua en eventos de desastres, ya que el incumplimiento de este tipo de normas acarrea sanciones administrativas,

penales, económicas, con temporal o permanente pérdida de las licencias de funcionamiento, además de tutelas, acciones populares o de cumplimiento, demandas y otras complicaciones, adicionalmente, las leyes en Colombia sobre las responsabilidades en caso de desastre son cada vez más claras y contundentes: quien genera el riesgo, paga por los daños y las pérdidas de los desastres que pueda provocar.

Si la empresa que provee un servicio público no ha gestionado y reducido los riesgos de desastres, como la ley expresamente lo obliga, en consecuencia las aseguradoras no cubrirán los riesgos asegurados, pues se deben cumplir a cabalidad las normas legales que los contemplan.

6.1.2 Documento de estudio del decreto 2157 de 2017

Recuperado de:

http://es.presidencia.gov.co/normativa/normativa/DECRETO%202157%20DEL%2020%20DE%20DICIEMBRE%20DE%202017.pdf

6.1.2.1 Condiciones del decreto para el establecimiento de una metodología de gestión de riesgo de desastres. Dentro del Decreto se establecen los siguientes artículos que contienen las características de la metodología de Gestión de Riesgos de Desastres:

6.1.2.2 Objetivo de un plan de gestión de riesgo de desastres. De acuerdo al Artículo 2.3.1.5.2.1. del decreto en cuestión, el plan de Gestión del Riesgo de Desastres de las Entidades Públicas y Privadas (PGRDEPP), se define como el instrumento mediante el cual las entidades públicas y privadas que prestan servicios de internet, telefonía local y móvil deberán: identificar, priorizar, formular, programar y hacer seguimiento a las acciones

necesarias para conocer y reducir las condiciones de riesgo (actual y futuro) de sus instalaciones y de aquellas derivadas de su propia actividad u operación que pueden generar daños y pérdidas a su entorno, así como dar respuesta a los desastres que puedan presentarse, permitiendo además su articulación con los sistemas de gestión de la entidad, los ámbitos territoriales, sectoriales e institucionales de la gestión del riesgo de desastres y los demás instrumentos de planeación estipulados en la Ley 1523 de 2012 para la gestión del riesgo de desastres.

6.1.2.3 Definición de los tipos de amenazas a tener en cuenta dentro del plan de gestion de riesgo de desastres. Según el artículo 2.3.1.5.1.2.1.del decreto en cuestión se definen los tipos de amenazas como:

Origen natural: estas amenazas se clasifican en:

Hidrometeorológicas*:* Inundaciones, deslizamientos, granizadas, avalanchas, vendavales, mares de leva, tormentas, huracanes, tornados, sequías, incendios forestales.

Geológicas*:* Fallas, sismos, tsunamis.

Volcánicas*:* 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.

***Amenazas Antrópicas**:* 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.

6.1.2.4 Alcance del plan de gestión de riesgo de desastres según el decreto. Según el artículo 2.3.1.5.1.1.2 del decreto en mención el alcance del plan de Gestión del Riesgo de Desastres de las Entidades Públicas y Privadas (PGRDEPP) incluirá, entre otros aspectos, el análisis específico de riesgo que considere los posibles efectos de eventos de origen natural, socio-natural, tecnológico, biosanitario o humano no intencional, sobre la infraestructura expuesta y aquellos que se deriven de los daños de la misma en su área de influencia de posible afectación por la entidad, así como de su operación que puedan generar una alteración intensa, grave y extendida en las condiciones normales de funcionamiento de la sociedad.

6.1.2.5 Metodología internacional sugerida a usar según el decreto. La determinación de la metodología para la identificación de riesgos deberá tener en cuenta el tipo de actividades de empresas que prestan servicios de Internet, telefonía local y móvil y la naturaleza de los

escenarios de riesgo identificados. También se podrá adoptar cualquiera de los métodos sugeridos en la **NTC IEC IS0 31010** o las demás normas que la reglamenten o sustituyan.

6.1.2.6 Definición de las etapas de la gestión de riesgo de desastres. Según el Artículo 2.3.1.5.2.1.1. del decreto 2157 el proceso de Conocimiento del Riesgo se relaciona con los siguientes aspectos:

a. Establecimiento del contexto: Contempla como mínimo los siguientes elementos:
b. Información general de la actividad: descripción de la actividad donde se debe incluir como mínimo los siguientes puntos:

Nombre del establecimiento o razón social, ubicación, vías de acceso, actividad principal y complementaria, descripción de producción o servicio resaltando la actividad que pueda generar riesgo de desastre para la sociedad, listado general y la descripción, cantidad de procesos, de sustancias químicas, de maquinaria que pueden ser fuente de desastres, área total construida, área libre, disposición de edificaciones, número de pisos, año de licencia de construcción, tipo de espacios y número, espacios comunitarios y equipamiento para emergencias existente, horario de funcionamiento, población expuesta al interior de la instalación evaluada, entre otros. Adicionalmente, se podrá incluir otra información de la actividad que se considere pertinente para el plan de gestión el riesgo de la entidad.

6.1.2.7 Caracterización de la infraestructura. Dentro de este ítem se debe definir:

- Descripción del entorno del establecimiento/actividad en relación a sus condiciones biofísicas y de localización.

- Identificación de instalaciones que puedan originar amenazas o producir efecto dominó mediante análisis cualitativo de acuerdo a la información disponible por las entidades pertinentes.

- Planes de ordenación y manejo de unidades ambientales costeras-POMIUAC
- Planes de ordenamiento territorial-POT
- Planes municipales de gestión del riesgo-PMGRD
- Estrategias municipales de respuesta-EMRE
- Planes territoriales y sectoriales de cambio climático

6.1.2.8 Contexto interno. Corresponde al ambiente intrínseco en el cual las entidades públicas y privadas buscan alcanzar sus objetivos y se relaciona con la alineación de la gestión del riesgo en los procesos propios de la actividad, la cultura, estructura y estrategia de la entidad evaluada.

Estos procesos deben estar alineados con los objetivos de la organización y el compromiso, la credibilidad y la confianza que se debe generar con los trabajadores, los clientes y la comunidad del área de influencia. Como mínimo debe incluir: a. Gobierno, estructura organizacional, funciones y responsabilidades.

6.1.2.9 Políticas, objetivos y estrategias diseñadas para la implementación del plan de gestión del riesgo. Dentro de estas políticas se debe incluir:

- Capacidades (Recursos disponibles, conocimiento).
- Las relaciones con las partes involucradas internas y sus percepciones y valores.

- La cultura de la organización.
- Forma y extensión de las relaciones contractuales.
- Normas, directrices y modelos adoptados por la organización.
- Listado de las directivas de la entidad con datos y líneas relevantes y actuales de comunicación.
- Descripción de las principales actividades, procesos, métodos operativos y zonas del establecimiento/actividad que estén expuestas a afectaciones/daños (proyecto, servicio, trabajadores, etc.).
- Contexto del proceso de gestión del riesgo: se orienta a definir aspectos de actuación en la toma de decisiones frente a la intervención del riesgo de desastres.
- Definición las metodologías de valoración del riesgo.
- Identificar los estudios necesarios para la elaboración del proyecto de intervención del riesgo.
- Criterios del riesgo: herramienta para la toma de decisiones para tener en cuenta en la valoración inicial del riesgo, la cual como mínimo debe tener en cuenta:

    a. Cómo se va a definir la probabilidad.

b. Los marcos temporales de la probabilidad, consecuencias o ambas.

c. Cómo se va a determinar el nivel de riesgo.

d. Nivel en el cual el riesgo se torna aceptable o tolerable.

e. La definición de estas variables deberá ajustarse al tipo de riesgo que se está evaluando y podrá integrarse; en lo pertinente, con los sistemas de gestión implementados por las entidades públicas y privadas.

Valoración del riesgo. La valoración del riesgo incluye la identificación del riesgo, el análisis del riesgo y la evaluación del riesgo.

La valoración del riesgo podrá realizarse teniendo en cuenta los contenidos mínimos que se describen a continuación:

Identificación del riesgo. Corresponde a la caracterización del riesgo diferenciado en las entidades públicas y privadas tanto en el contexto interno como en el contexto externo; esta identificación debe ser exhaustiva con el fin de cubrir todas las posibilidades.

Se deberían identificar dentro de esta sección los siguientes atributos del riesgo:

Las causas y fuentes de riesgo, en donde se debe tener en cuenta la descripción, ubicación y frecuencia de ocurrencia, tanto para las actividades o procesos existentes como futuros, además la afectación que se pueda generar en la actualidad o a futuro en el área de influencia (el área de influencia a la zona que podría ser afectada por consecuencia de efectos relacionados con la actividad desarrollada por la entidad pública y privada).

Caracterización de controles preventivos y correctivos, en donde se deben identificar los elementos que constituyen el riesgo.

Amenazas, tanto internas como externas, que puedan afectar la entidad.

Listado de escenarios posibles y previsibles.

Áreas de afectación probables (impactos esperados acorde al tipo de evento amenazante). ldentificación de los elementos expuestos dentro del área de afectación probable.

Consecuencias potenciales o colaterales.

Experiencias y lecciones aprendidas (posterior a la emergencia).

Actores relacionados.

Análisis del riesgo. Consiste en la determinación de consecuencias y probabilidades del riesgo, permitiendo su reconocimiento y comprensión y el detalle de las amenazas, los elementos expuestos y el riesgo.

El análisis del riesgo es un examen detallado para conocer sus características, cualidades o su estado y extraer conclusiones considerando las partes que lo constituyen; haciendo una

diferenciación de la magnitud y gravedad de las consecuencias a nivel interno de las instalaciones de la actividad y del área de influencia de probable afectación.

decisión de la entidad (NTC-ISO 31000). El método elegido deberá cumplir con ser sistémico, repetible, exhaustivo y auditable.

Para realizar el análisis del riesgo se pueden utilizar métodos cualitativos, cuantitativos o semi-cuantitativos, cuyo grado de detalle requerido dependerá de la aplicación particular, la disposición de datos confiables de las necesidades para la toma de Los puntos a desarrollar como mínimo en esta etapa son:

a. Nivel de consecuencias: efectos sociales, económicos y ambientales, deben incluirse los escenarios de mayores consecuencias y/o eventos extremos.

b. Definición del método para la estimación de la probabilidad: La posibilidad se entiende como el panorama general de alternativas que pueden suceder frente a un proceso o evento determinado (NTC-ISO 31000) y la probabilidad se refiere a la ocurrencia especifica de un proceso o evento determinado (NTC-ISO 31000).

c. Factores que afectan las probabilidades y las consecuencias, incluidos los esquemas de control establecidos por la entidad en el marco de los sistemas de gestión.

d. Valoración de los controles existentes, en cuanto a la existencia, capacidad y funcionamiento o la comparación con criterios de seguridad establecidos por la entidad.

e. Análisis de consecuencias a través de: una descripción sencilla o un modelo cuantitativo detallado o un análisis de vulnerabilidad; según se defina para cada tipo de actividad.

Evaluación del riesgo. Permite determinar el nivel asociado nivel de probabilidad de que un riesgo tiene asociado un nivel de probabilidad de que dicho riesgo se

concrete y el nivel de severidad de las consecuencias de la materialización del riesgo, mediante la estimación de los daños y las pérdidas potenciales o nivel estimado del riesgo con los criterios de riesgo definidos y establecidos en el contexto.

6.1.3 Documento de estudio diseño de la red nacional de telecomunicaciones de emergencia en Colombia.

MINTIC, Recuperado de https://colombiatic.mintic.gov.co/679/w3-article-73949.html

Este documento es la propuesta de Mintic para el diseño de una red de Telecomunicaciones de emergencia, el documento contiene las posibles amenazas naturales que pueden presentarse en el territorio colombiano.

En Colombia, dadas las estructuras geológicas y tectónicas, así como por las condiciones climáticas, se presentan eventualmente fenómenos catastróficos de origen geológico (terremotos, erupciones volcánicas, deslizamientos), hidro-meteorológico (tormentas, inundaciones, sequías) y mixtos (remoción en masa, avalanchas, entre otros).

Lo que cambia según el contexto natural es la vulnerabilidad, ya sea por el tipo de accidentes naturales, por el aumento de población en las cabeceras municipales, por los desplazamientos o por las mismas construcciones.

Conceptualmente, se debe definir la interrelación de amenaza, vulnerabilidad y riesgo. Dicha relación se establece incluso matemáticamente a través de la siguiente ecuación:

RIESGO = AMENAZA X VULNERABILIDAD

El término de amenaza se relaciona con los peligros que representan los fenómenos de origen natural, tales como atmosféricos, hidrológicos y geológicos, tanto para el hombre como para el ambiente. Estas amenazas son fenómenos naturales que eventual o frecuentemente constituyen restricciones al uso del territorio; dado el origen, alcance y la magnitud, sus efectos pueden ser considerados inmanejables por el hombre.

La amenaza surge de la probabilidad de ocurrencia y grado de impacto con la que cierto evento se presenta en un período y área determinada; aspectos de base para definir magnitud, características y extensión probable.

La vulnerabilidad está referida a la exposición de infraestructura, elementos y lo más importante, personas o habitantes de un territorio; a causa de haberse presentado la ocurrencia de un evento desastroso.

Un riesgo se refiere a la probabilidad, la estimación y la cuantificación de la magnitud y las consecuencias de los daños ambientales, sociales, económicos o culturales y/o pérdidas humanas, de bienes, especies, prácticas culturales, sitios simbólicos y lugares de rituales, entre amenaza se transforma en un riesgo de acuerdo a la vulnerabilidad que tiene una persona o los asentamientos humanos frente a las amenazas.

sismicidad, vulcanismo, remoción en masa, incendios, inundaciones y tsunamis.

Amenazas de origen natural: Estas amenazas son todos los fenómenos atmosféricos, hidrológicos y geológicos, que forman parte de la historia geológica, geomorfológica, climática y oceánica del planeta y que por ubicación, severidad y frecuencia, tienen el potencial de afectar adversamente al ser humano o a sus estructuras habitacionales e infraestructura artesanal o de bajas características de sismo resistencia o competencia ante un fenómeno natural. Por ello es que estas ciudades y todo el territorio, siempre tendrán la misma amenaza constante para ocasionar sismos o volcanes, pero su vulnerabilidad cada vez puede tender a ser más alta, aumentando proporcionalmente el factor Riesgo.

En la Ilustración No 2., se interrelaciona la frecuencia, con el número de víctimas y viviendas destruidas, todo basado en el tipo de amenaza geológica o hidro-metereológicas que afectó el suceso.

Si analizamos la Ilustración 2, se presenta una proporcionalidad directa en los eventos sísmicos y volcánicos en cuanto a la generación de víctimas y daños a viviendas, siendo que su frecuencia (número de eventos) es baja; frente a eventos como deslizamientos e inundaciones, cuya frecuencia es mucho más alta pero el número de pérdida de vidas y de viviendas destruidas es menor.

De la ilustración 2 podemos concluir que los sismos amenazan las infraestructuras, la erupción de volcanes así sea esporádica causa la mayor cantidad de muertes por unidad de tiempo y las inundaciones causan la mayor cantidad de pérdida de vidas, no por evento sino por la gran probabilidad de ocurrencia.

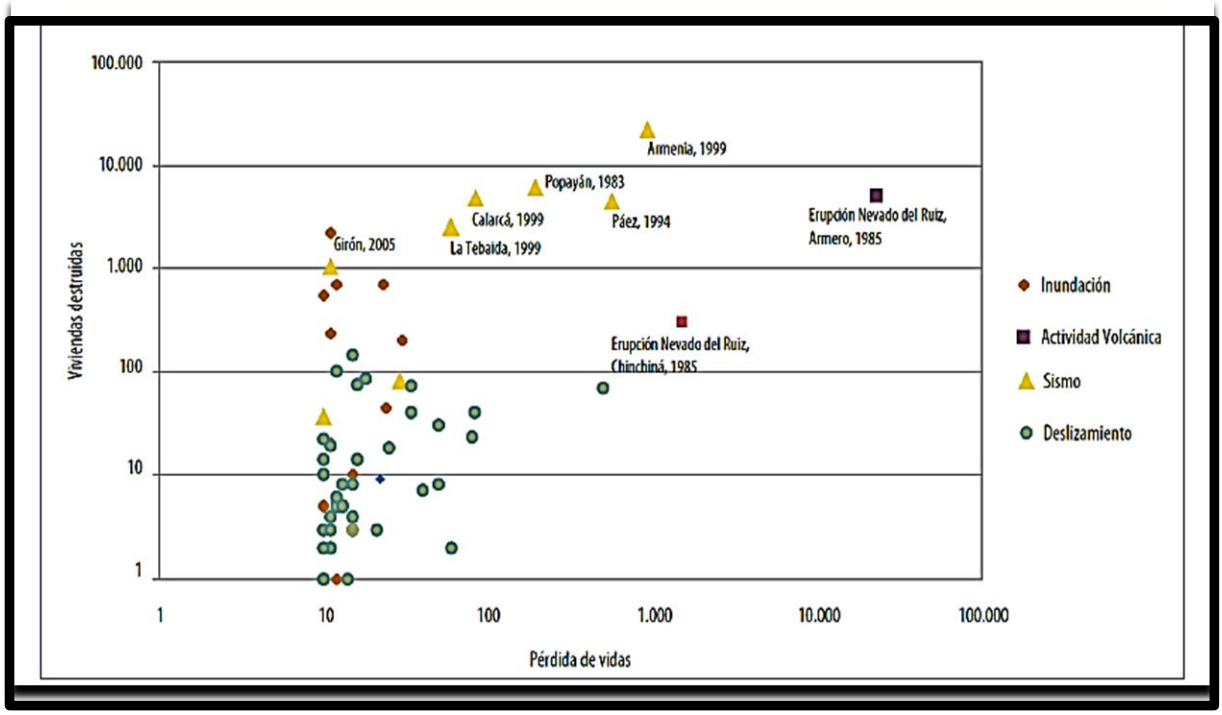


Ilustración 2. Relación entre viviendas destruidas y pérdidas de vida, 1970-2011 por eventos hidrometereológicos y geológicos en Colombia. Fuente: corporación Osso35

En la Ilustración No 3 observamos que la mayor cantidad de pérdida de vidas ocurre en municipios de bajos ingresos.

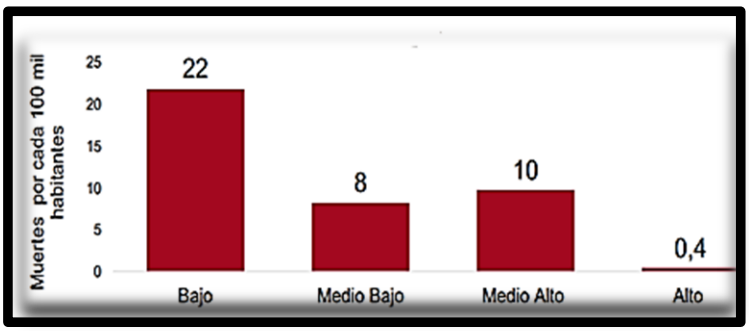


Ilustración 3. Muertes por desastres según nivel de ingresos. Origen: Indice municipal de riesgo de desastres de Colombia abril 2018

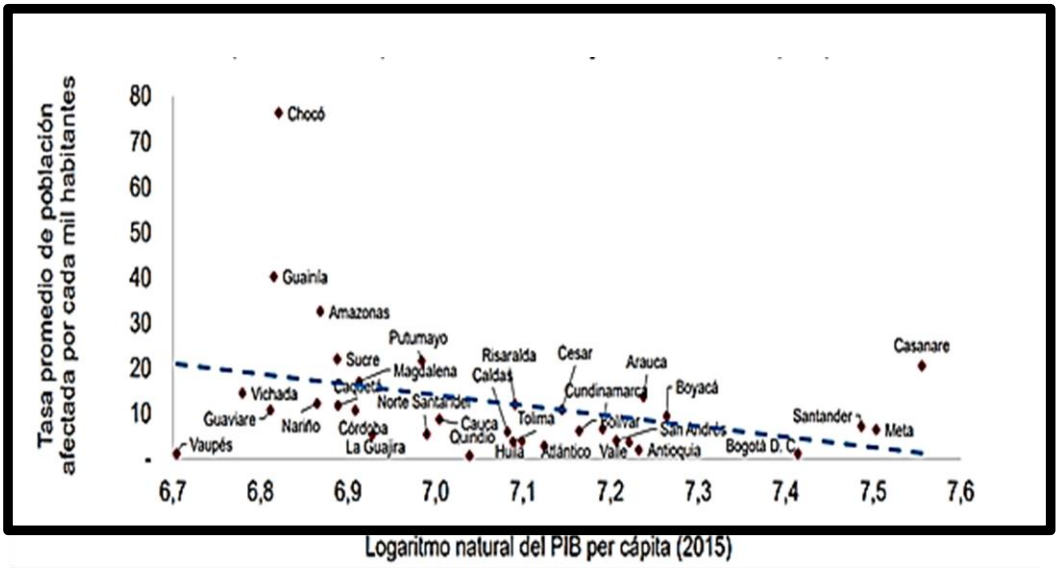


Ilustración 4. Tasa de población afectada por eventos hidrometerológicos 2010-2015. Fuente: Indice municipal de riesgo de desastres de Colombia abril 2018

En la Ilustración No 4 se observan que los departamentos con menor PIB per cápita en Colombia son los que presentan mayor índice de población afectada por eventuales desastres naturales.

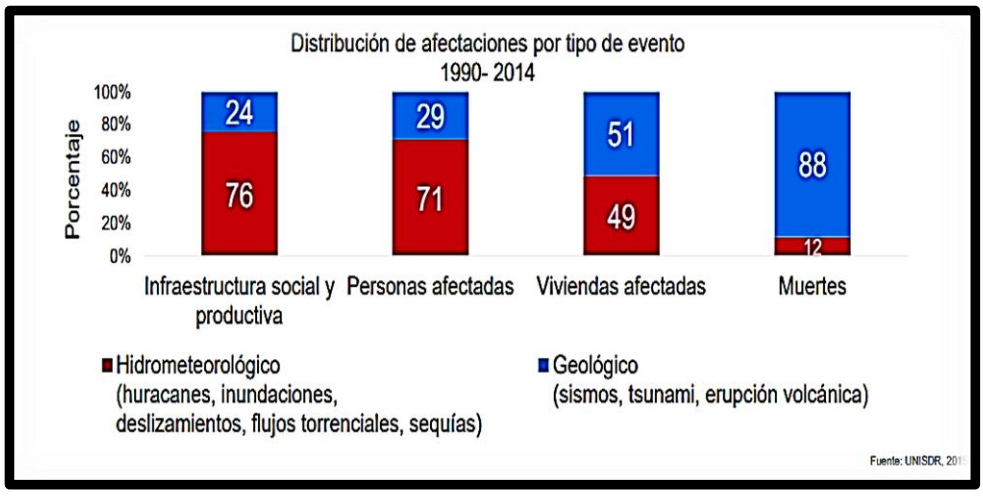


Ilustración 5. Distribución de afectaciones por tipo de evento. Índice municipal de riesgo de desastres de Colombia abril 2018

En la ilustración 5 observamos que la infraestructura social y productiva es mayormente afectada por fenómenos meteorológicos como huracanes, inundaciones, deslizamientos, flujos torrenciales y sismos, en la ilustración 5 también se observa que las muertes por evento son más probables cuando ocurren tsunamis, erupción de volcanes o sismos.

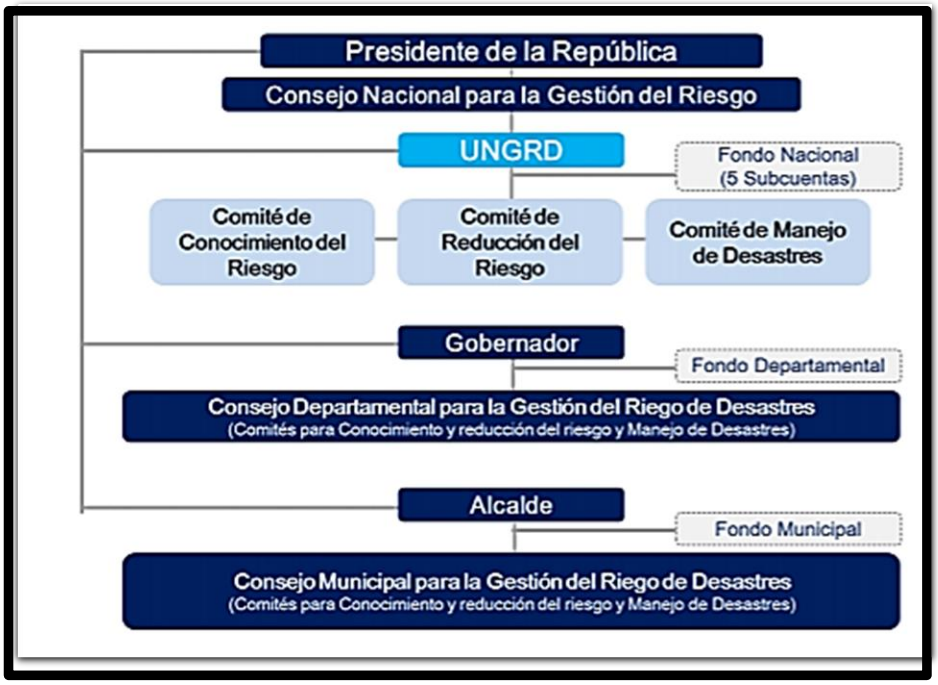


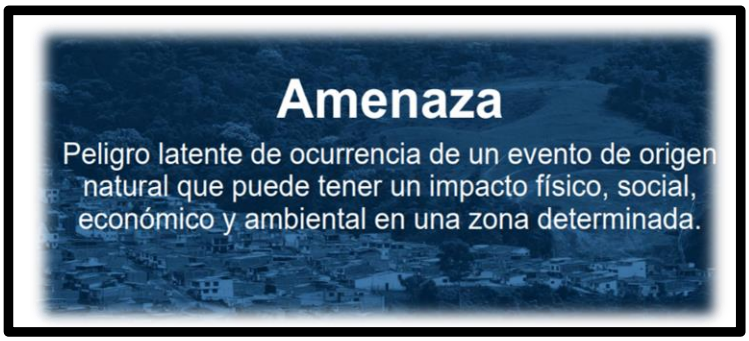
Ilustración 6. Sistema nacional de riesgo de desastres en colombia

Fuente: UNGRD, 2012

En 2012 se adoptó por primera vez en Colombia una Política Nacional de Gestión del Riesgo de Desastres Se crearon instrumentos nacionales y territoriales para fortalecer la gestión del riesgo de desastres, en la Ilustración No 6 se observa la organización del Sistema Nacional en gestión de riesgos de desastres.

Amenaza sísmica

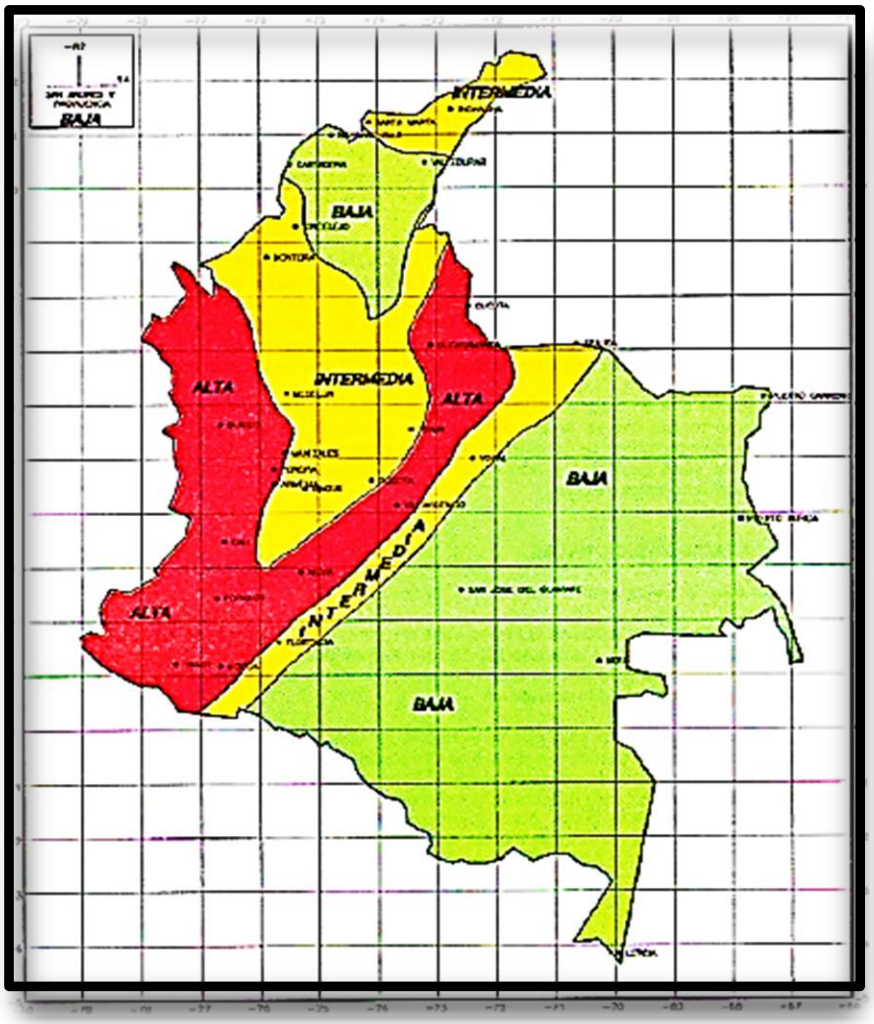
Colombia está situada en la convergencia de tres placas litosféricas: Nazca, Caribe y América del Sur, lo que significa que se ve afectada por una variedad de fuentes sísmicas



asociadas con la zona de subducción del Pacífico, así como las fallas superficiales relacionadas con la acumulación de los esfuerzos en el continente (Corporación OSSO, 1998). La amenaza sísmica se expresa por los movimientos directos de las vibraciones sísmicas que actúan sobre la superficie y afectan la infraestructura. Estas vibraciones dependen de las características del terremoto, magnitud y profundidad, así como de las características del suelo y subsuelo. Las vibraciones pueden generar efectos secundarios como deslizamientos y *licuación* de suelos.

La región Pacífica del país se encuentra expuesta a amenaza sísmica alta, asociada con la zona de subducción del océano Pacífico, la cual tiene la capacidad de liberar las mayores cantidades de energía sísmica en Colombia. En dicha fuente ocurrieron los sismos de 1906 y 1979, los cuales se destacan, además, por ocasionar un tsunami que afectó principalmente la población de Tumaco, municipio localizado en la costa Pacífica nariñense

En la región Andina las zonas de amenaza sísmica alta se asocian con la actividad de fallas superficiales como Romeral, Cauca, Palestina y Frontal de la Cordillera Oriental, la cuales tiene la característica de generar sismos superficiales de gran poder destructivo, como los de Suaza (1827), Huila (1967), Popayán (1983), Páez (1994), Tauramena (1995) y Eje Cafetero (1999), entre otros.



Mapa 1 Zonificación del riesgo sísmico en Colombia
Fuente: Reglamento colombiano de construcción sismo-resistente nsr-10, de enero de 2010

Algunos de estos sismos se han destacado por generar importantes movimientos en masa, lo que se explica por las características topográficas y geológicas de la región. En el norte del Valle del Cauca, sur del Chocó y Eje Cafetero se presenta sismicidad de profundidad intermedia (entre 66 y 300 km), con eventos de magnitud alrededor de 6,0 a 6,5, que han generado importantes daños en Cali (en

1925), así como en Manizales y Pereira, y en otras poblaciones entre del sur de Antioquia y del norte del Valle del Cauca (en 1938, 1961, 1962, 1973, 1979 y 1995).

Los Andes colombianos hacen parte del Cinturón de Fuego del Pacífico, catalogado como una de las zonas sísmicas más activas del planeta. En este país la zonificación de la sismicidad se empezó a definir en los estudios regionales que sustentaron el Reglamento Colombiano de Construcción Sismo-resistente NSR-10, de enero de 2010, cuyo mapa en su última versión, se reproduce en el mapa No 1.

A raíz del sismo de Popayán del 31 de marzo de 1983, se iniciaron en el país los estudios de microzonificación sísmica, el primero de los cuales se realizó en Popayán en 1992. En este tipo de estudios se mide la respuesta o comportamiento de los suelos frente a las ondas sísmicas, a fin de establecer tanto las restricciones para cierto tipo de construcciones como los de diseño para las posibles o potenciales edificaciones e infraestructura apta para su construcción, con base en las implementaciones de este tipo de normas de sismo resistencia.

La definición más usual de amenaza sísmica es la que se refiere a la probabilidad de que un parámetro como la aceleración, la velocidad o el desplazamiento del terreno producido por un sismo, supere o iguale un nivel de referencia. En este sentido, Ingeominas elaboró un mapa se afirma que el 86% de los colombianos se encuentran bajo un nivel de amenaza sísmica apreciable: en zonas de amenaza alta aparecen cerca de 475 municipios con el 35% de los habitantes; en zonas de amenaza intermedia 435 municipios con el 51% de la población; y en zonas de amenaza baja 151 municipios con aproximadamente el 14% de los colombianos.

general del país en el que zonifica el territorio de acuerdo al valor de aceleración sísmica Aa (g), el cual se reproduce en el mapa No 2.

En general, sobre los niveles de amenaza sísmica en las diferentes regiones de Colombia Sin embargo, el riesgo no sólo depende del grado de amenaza sísmica, sino del grado de vulnerabilidad que en general tienen las construcciones asociados a esta.

A nivel municipal, Cali representa la mayor población expuesta a amenaza sísmica alta, seguido por otras capitales como Cúcuta, Bucaramanga, Pereira, Villavicencio, Pasto y Manizales.

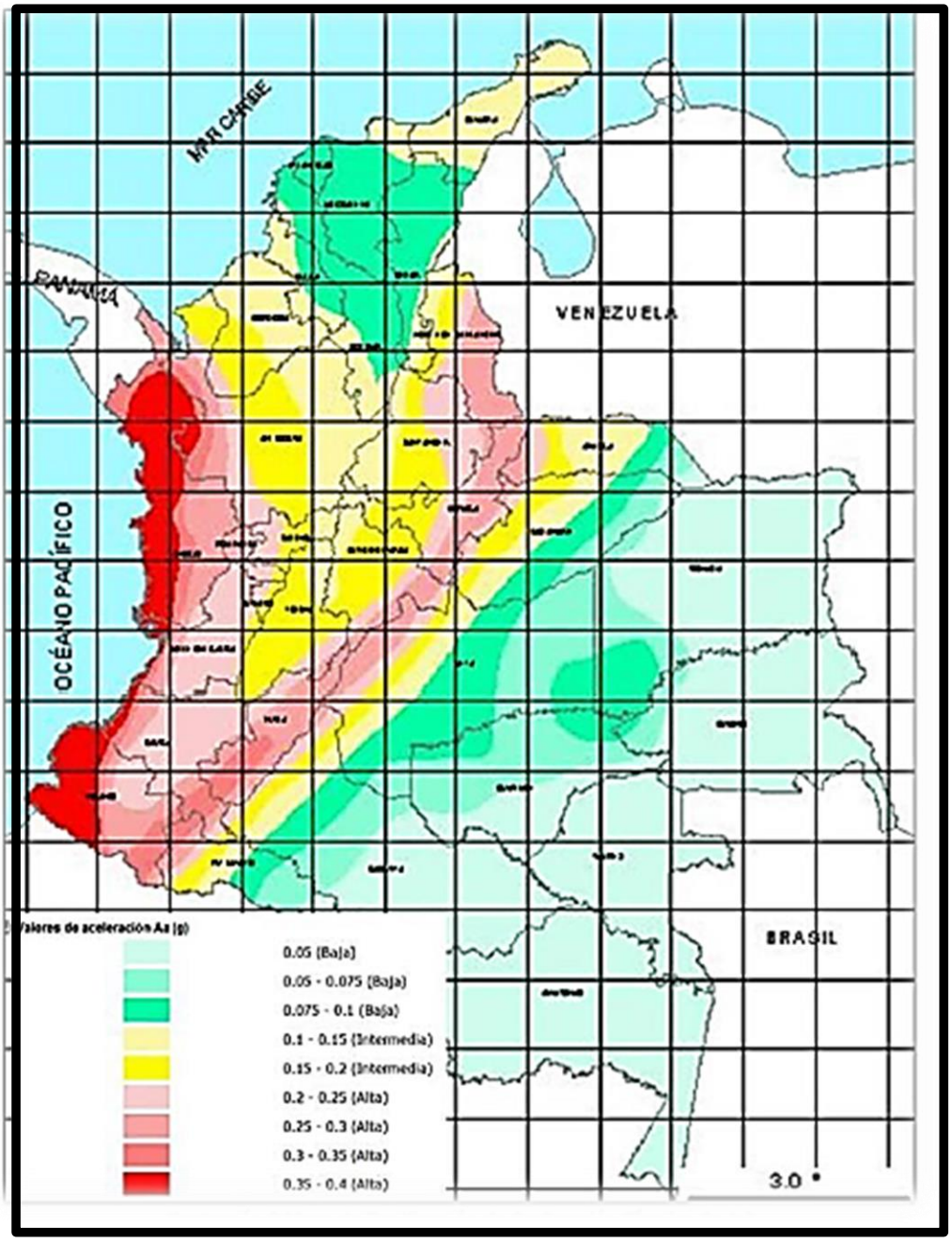
Amenaza: movimientos en masa

Los desplazamientos en masa son desplazamiento de rocas, suelos o escombros por una ladera por acción de la gravedad. Se incrementan por cambios en el uso del suelo, lluvias intensas de corta duración o prolongadas, y por intervenciones antrópicas.

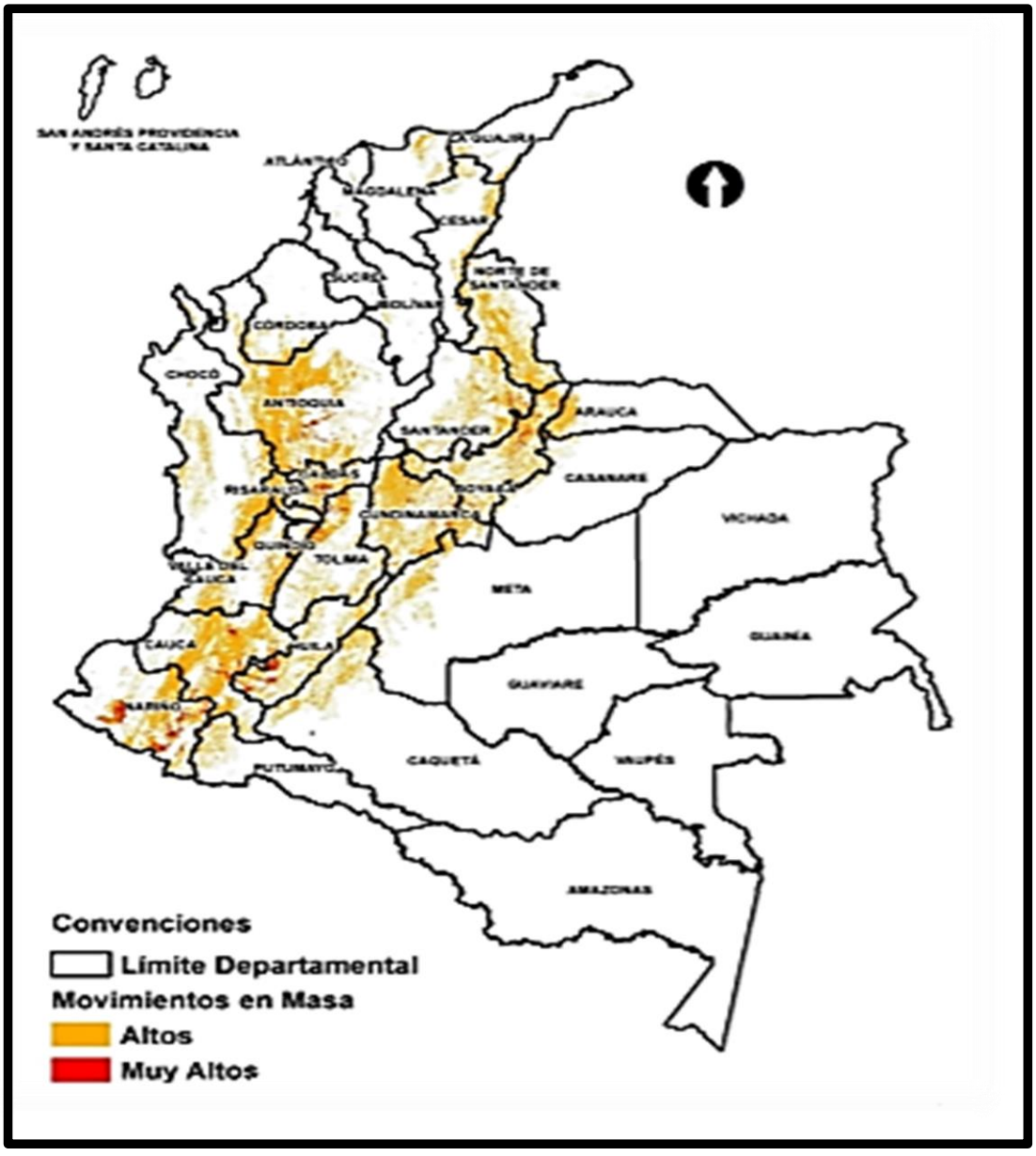
11,7 millones de hectáreas tienen mayor susceptibilidad a movimientos en masa, 66% de muertes se asocian con movimientos en masa, 14% de las viviendas afectadas por desastres se asocia a movimientos en masa. El mapa Numero 3 resumen estos porcentajes.

Amenaza volcánica. Ingeominas (Hoy Servicio Geológico Colombiano) es las entidad encargada de divulgar el Atlas de Amenaza Volcánica en Colombia. Además viene monitoreando con instrumentación sismológica y telemétrica los 14 volcanes activos que se considera existen en el país.

Juana, el volcán nevado de Puracé, el volcán Sotará, el volcán Cerro Bravo y el volcán Cerro Machín. (Ver Tabla No 2)



Mapa 2. Mapa de zonificación de aceleración sísmica aa (g)
Fuente: Ingeominas, 1999



Mapa 3. Mapa nacional de susceptibilidad a movimientos en masa a escala 1:100.000, Sgc, 2015. Fuente IDEAM – IGAC, 2012 e IDEAM, 2016

La amenaza volcánica está relacionada con la emisión de gases, la expulsión aérea de piroclastos, los flujos piroclásticos, los flujos de lava, los flujos de lodo y las ondas de choque generadas por las erupciones explosivas.

V. N. del Huila (5631 m)	Huila, Cauca, Tolima	Preliminar	1996
V. N. del Ruiz (5310 m)	Tolima	2ª versión	1986
V. N. del Tolima (5280 m)	Tolima	Preliminar	1989
V. N. Santa Isabel (5100 m)	Tolima, Caldas y Risaralda	Final	1993
V. Galeras (4276 m)	Nariño	3ª versión	1997
V. N. Cumbal (4764 m)	Nariño	Preliminar	1988
V. N. Chiles (4750 m)	Nariño	Preliminar	1997
V. Cerro Negro (4460 m)	Nariño	Preliminar	1997
V. Azufral (4070 m)	Nariño		Sin Información
V. Doña Juana (4250 m)	Nariño		Sin Información
V. N. Puracé (4700 m)	Cauca y Huila	Actualización	2008
V. Sotará (4580 m)	Cauca		Sin Información
V. Cerro Bravo (4020 m)	Caldas	Preliminar	1992
V. Cerro Machín (2750 m)	Tolima	Preliminar	2002

TABLA No. 2 Amenazas volcánicas en Colombia
Fuente Servicio Geológico Colombiano

El Servicio Geológico Colombiano y diferentes Corporaciones Autónomas Regionales y universidades han advertido que uno de los escenarios más críticos desde el punto de vista volcánico podría estar relacionado con una explosión del Cerro Machín.

Los efectos volcánicos más desastrosos en Colombia, han sido consecuencia de lahares o flujos de lodo, concentrados en las zonas de influencia de los volcanes Ruiz, Galeras y Huila.

La exposición de ciudades y poblaciones a fenómenos como erupciones volcánicas, lahares y avalanchas no ha sido estimada para todos los volcanes en términos de posibles impactos humanos y económicos; sin embargo, los datos parciales de los volcanes que cuentan con mapas

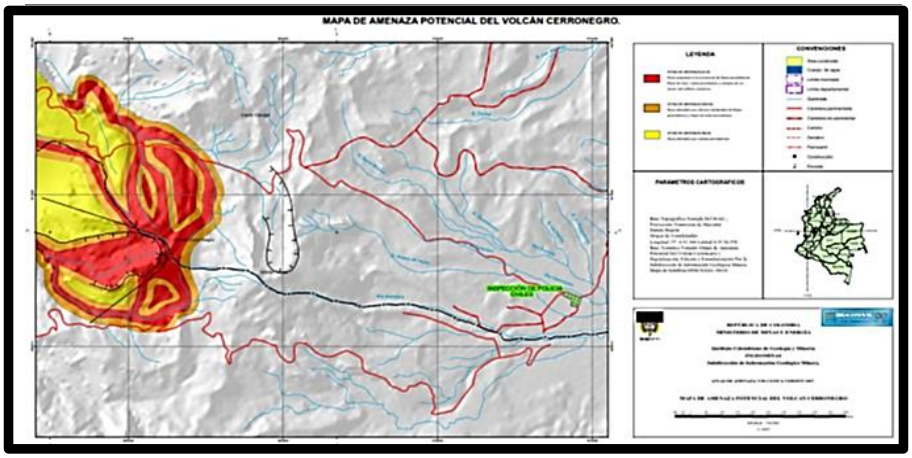
de amenaza indican que hay por los menos 1,9 millones de personas en la zona de influencia y de estos, aproximadamente 240 mil se localizan en zonas de amenaza alta.

Para la estructuración de la información se debe utilizar los mapas elaborados por el Instituto Colombiano de Geología y Minería, Dirección del Servicio Geológico, 2007, sobre el grado de amenaza volcánica. Para el ejemplo de la investigación utilizaremos el volcán Cerronegro (Mapa No 4), en donde podemos observar los siguientes grados de amenaza:

Grado de Amenaza Alta - Probabilidad de lavas, flujos piroclásticos, lahares, flujos de escombros y/o caída de piroclastos. (En color Rojo)

Grado de Amenaza Media (Moderada) - Probabilidad de flujos de lodo y/o piroclastos, lahares y/o caída de piroclastos. En el volcán Nevado del Huila flujos de lavas. (Color Naranja)

Grado de Amenaza Baja - Probabilidad de caída de piroclastos y/o flujos de lodo. Para el Volcán Nevado del Huila probabilidad de lavas. (Color amarillo)



MAPA No. 4 Mapa nacional de susceptibilidad a movimientos en masa a escala 1:100.000, SGC, 2015
Fuente IDEAM – IGAC, 2012 e IDEAM,

Amenaza: inundaciones lentas. Ocurren en zonas planas de ríos y valles extensos. Se generan por lluvias fuertes o continuas que aumentan el nivel de las aguas cubriendo áreas que normalmente están secas. Fuente: Mapa No 5.

Según este mapa, 10,2 millones de hectáreas inundables periódicamente • 900 mil hectáreas adicionales se inundan de manera recurrente en fenómenos de La Niña • 15% de muertes se asocian con inundaciones lentas • 85% de viviendas afectadas por desastres se asocia a inundaciones lentas.

En Colombia, la presencia de llanuras bajas y valles aluviales, aunada a las condiciones de precipitación facilitan la ocurrencia de inundaciones, algunas de manera lenta, que afectan grandes extensiones de terreno, y otras más rápidas asociadas a lluvias intensas en la parte alta de las cuencas con fuertes pendientes.

Algunos de los efectos ocasionados por inundaciones son:

• Anegamiento de las llanuras de inundación con pérdidas ocasionales de vidas, deterioros en viviendas, infraestructura y áreas de producción agropecuaria.

• Estancamiento de aguas por deficiencia de drenaje en las áreas, con repercusiones sobre salud pública.

• Cauces inestables en épocas de avenidas torrenciales por carga excesiva en el flujo de agua, causando por consiguiente erosión de márgenes, con consecuencias sobre la infraestructura como pérdida de puentes, caminos, viviendas, y de áreas productivas.

El IDEAM presentó en 1998 una caracterización de las inundaciones por región, la cual se resume así (Mapa 5):

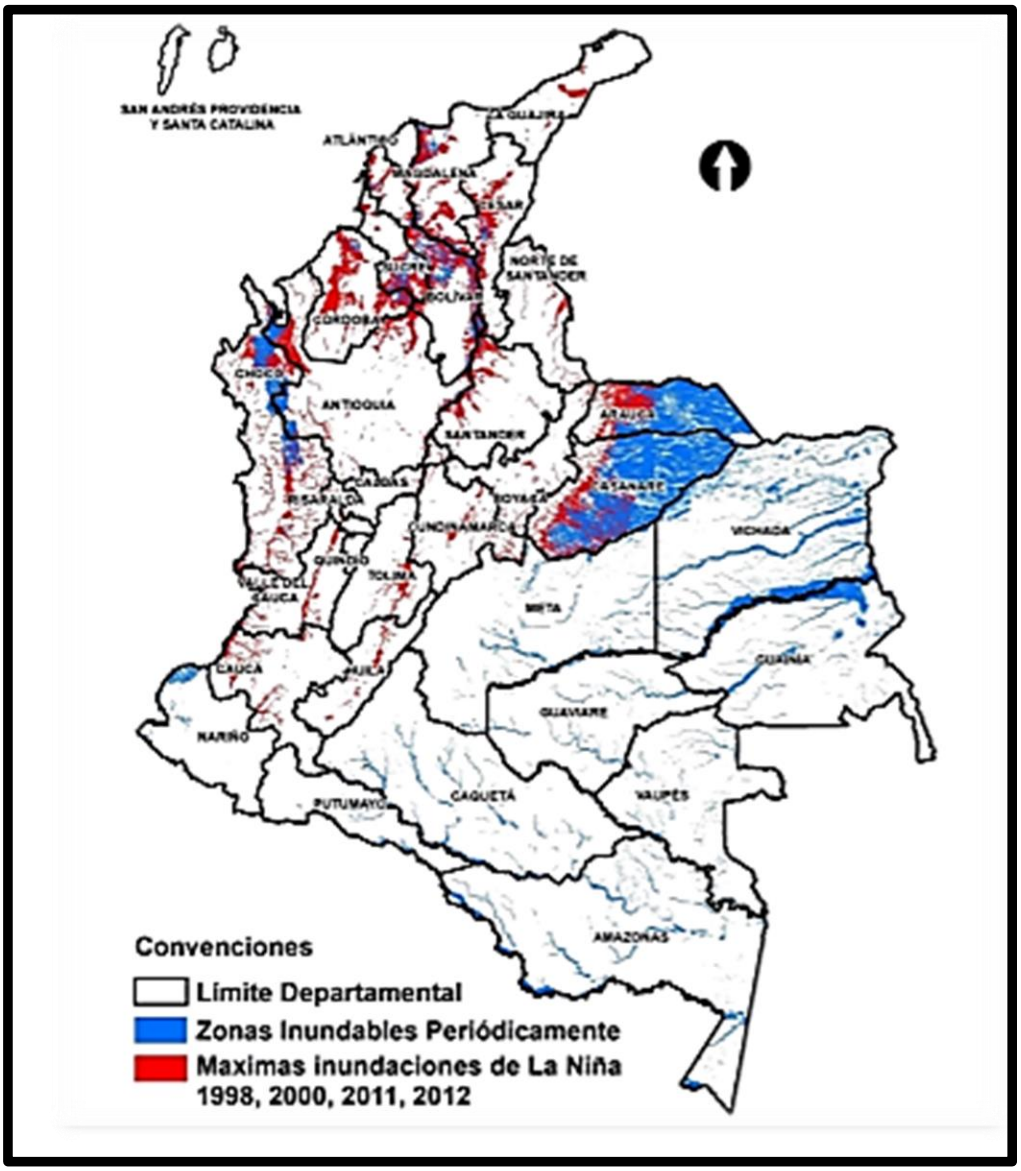
• En la Región Andina se presentan inundaciones súbitas y de incierta ocurrencia, causadas por avenidas de ríos cuyos caudales máximos en sus períodos de retorno acumulados de muchos años, o por eventos indirectos que impulsan estos fenómenos como son sismos o erupciones, asociados con el estado de las cuencas por efecto de las actividades antrópicas inadecuadas.

Los lugares en donde se presentan inundaciones rápidas y ocasionales, son Girón, Santander y en el noroeste de Antioquia, caracterizadas principalmente porque los efectos se concentran sobre lugares donde los ríos de montaña encuentran sus valles de salida, o en el ámbito de cuencas deforestadas, habida cuenta de la existencia de poblados en sus cabeceras.

En las Planicies deprimidas o zonas de ciénaga, relacionadas con inundaciones lentas y periódicas, propias de áreas agrícolas extensas no drenadas, permaneciendo sumergidas gran parte del año durante la estación invernal. Al igual que la anterior, las actividades antrópicas inadecuadas en las llanuras de inundación acentúan este fenómeno con sus consecuentes efectos negativos sobre la calidad de vida y del ambiente circundante.

Ejemplos de estas inundaciones periódicas y lentas corresponden a la Depresión Momposina, donde drenan los ríos Magdalena, Cauca, San Jorge y César; además del bajo Atrato, aguas abajo de Riosucio, Chocó. El fenómeno se caracteriza por las complejas consecuencias ambientales como desecación de las ciénagas de interés para los pescadores; reducción del amortiguamiento de las crecientes por la construcción de diques, en detrimento de la estabilidad de las áreas aguas abajo.

En el año 2010, el IDEAM publicó el Mapa de Zonas Susceptibles a Inundación en el territorio nacional (ver mapa No 5).



MAPA No. 5 Mapa de inundaciones a ESCALA 1:100.000
Fuente IDEAM – IGAC, 2012 e IDEAM, 2016

Para el Banco Mundial; las áreas con mayor susceptibilidad a inundarse son: (i) en el oriente del país, en las llanuras bajas de las cuencas de los ríos Orinoco y Amazonas; (ii) en los valles aluviales en las regiones Caribe y Pacífica, asociados con el río Magdalena, la depresión Momposina, los valles de los ríos Sinú y Alto San Jorge, y en las tierras bajas cercanas al río interandinos, principalmente de los ríos Cauca y Magdalena, lo mismo que en la Sabana de Atrato, en el Chocó, y los deltas de los ríos San Juan, Telembí, Patía y Mira; y (iii) en los valles Bogotá.

Amenaza: flujos torrenciales. Los flujos torrenciales incluyen un desplazamiento rápido de volúmenes importantes de agua, suelo, sedimentos y escombros por cauces de quebradas con altas pendientes, 12,4 millones de hectáreas en el país pueden presentar flujos torrenciales muy altos, 19% de muertes se asocian con flujos torrenciales, 1% de viviendas afectadas por desastres se asocia a flujos torrenciales,32,6 millones de hectáreas (29%) del territorio nacional tienen las condiciones más críticas de amenaza ante fenómenos hidrometeorológicos.

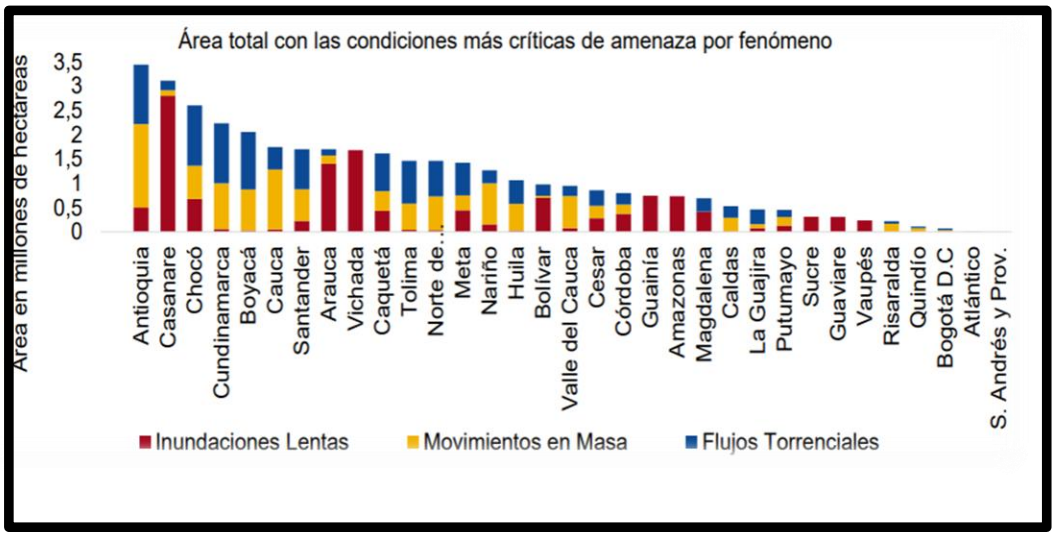
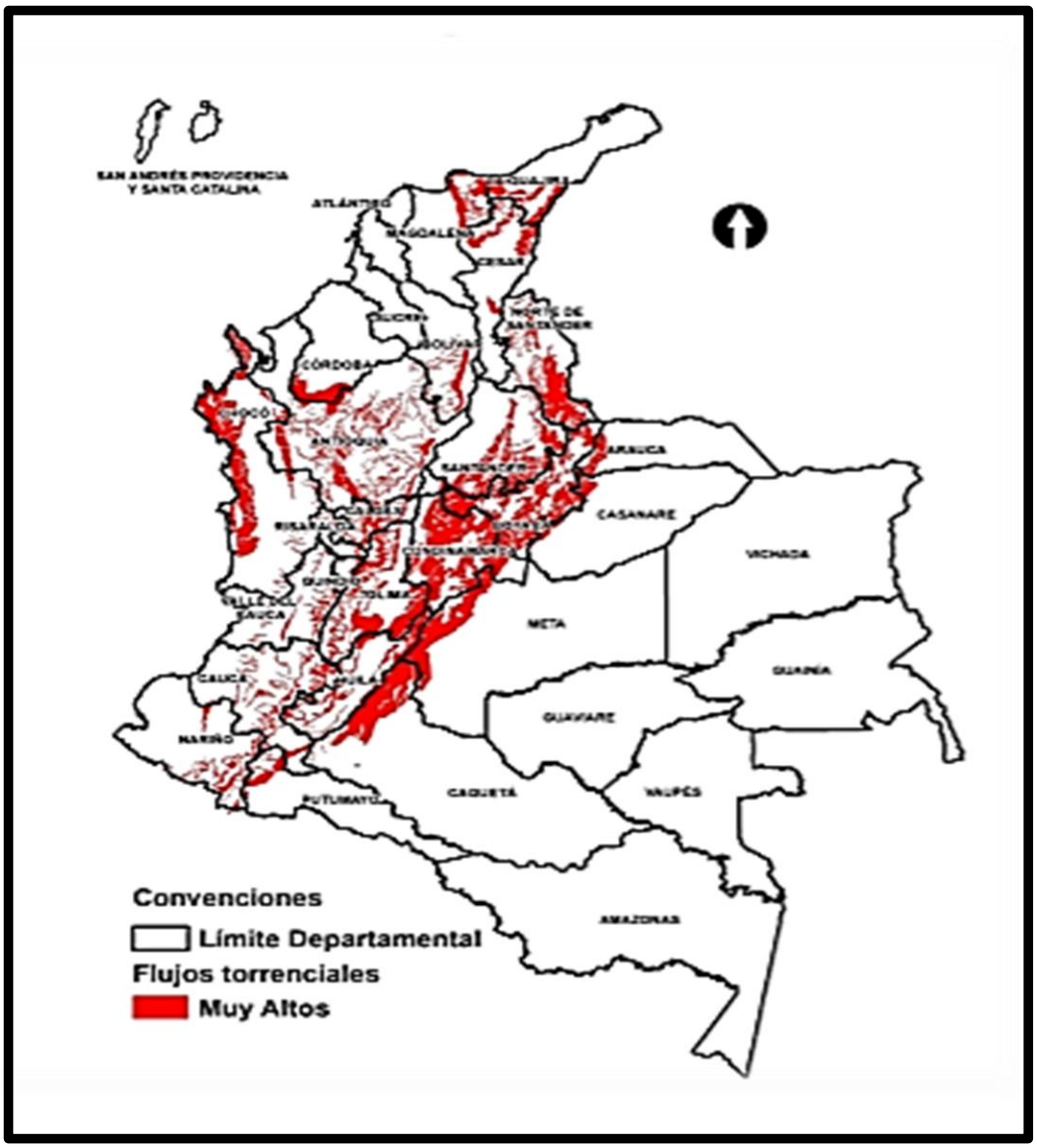
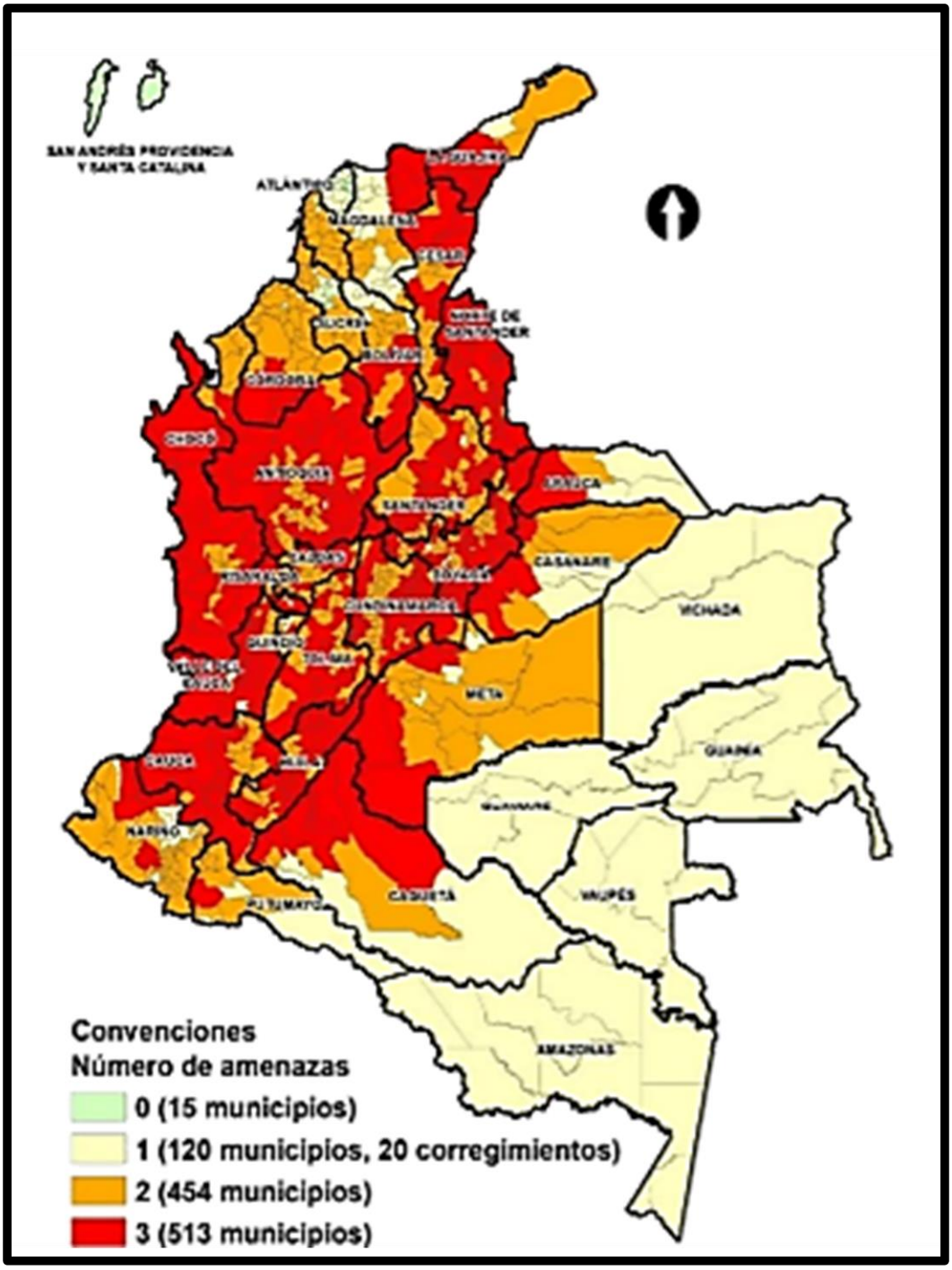


Ilustración No.7 Area total con las condiciones más críticas de amenaza por fenómeno
Fuente: DNP-DADS, 2018

En la Ilustración No. 7 podemos observar cómo se afectan los departamentos de Colombia por los que confluyen los tres tipos de amenazas hidrometeorológicas en sus condiciones más críticas, asimismo el mapa No 6 expone los departamentos con mayor proporción de amenazas hidrometereológicas, los departamentos más afectados se encuentran en la cordillera oriental, en la Ilustración No 8 se encuentran los municipios más afectados por amenazas meteorológicas.



MAPA No. 6. Mapa de flujos torrenciales a escala 1:500.000 IDEAM, 2010



Mapa No. 7 Numero de amenazas hidrometeorológicas
En el 75% de los departamentos del país confluyen los tres tipos de amenaza.

En la Ilustración No. 8 observamos los municipios de Colombia con mayor grado de amenazas hidrometeorológicas:

Municipios con mayor área amenazada a los tres tipos de fenómenos		
	Municipio	Área amenazada (Ha)
1	Riosucio – Chocó	537.330
2	Uribe – Meta	346.930
3	San Vicente del Caguán – Caquetá	340.871
4	Tame – Arauca	285.758
5	Puerto Rico – Caquetá	237.988
6	Tierralta – Córdoba	214.396
7	Carmen del Darién – Chocó	207.771
8	Ituango – Antioquia	186.899
9	El Tambo – Cauca	185.022
10	Bajo Baudó – Chocó	179.729

Ilustración No 8. Numero de amenazas hidrometeorológicas.
En el 75% de los departamentos del país confluyen los tres tipos de amenaza.

Exposición

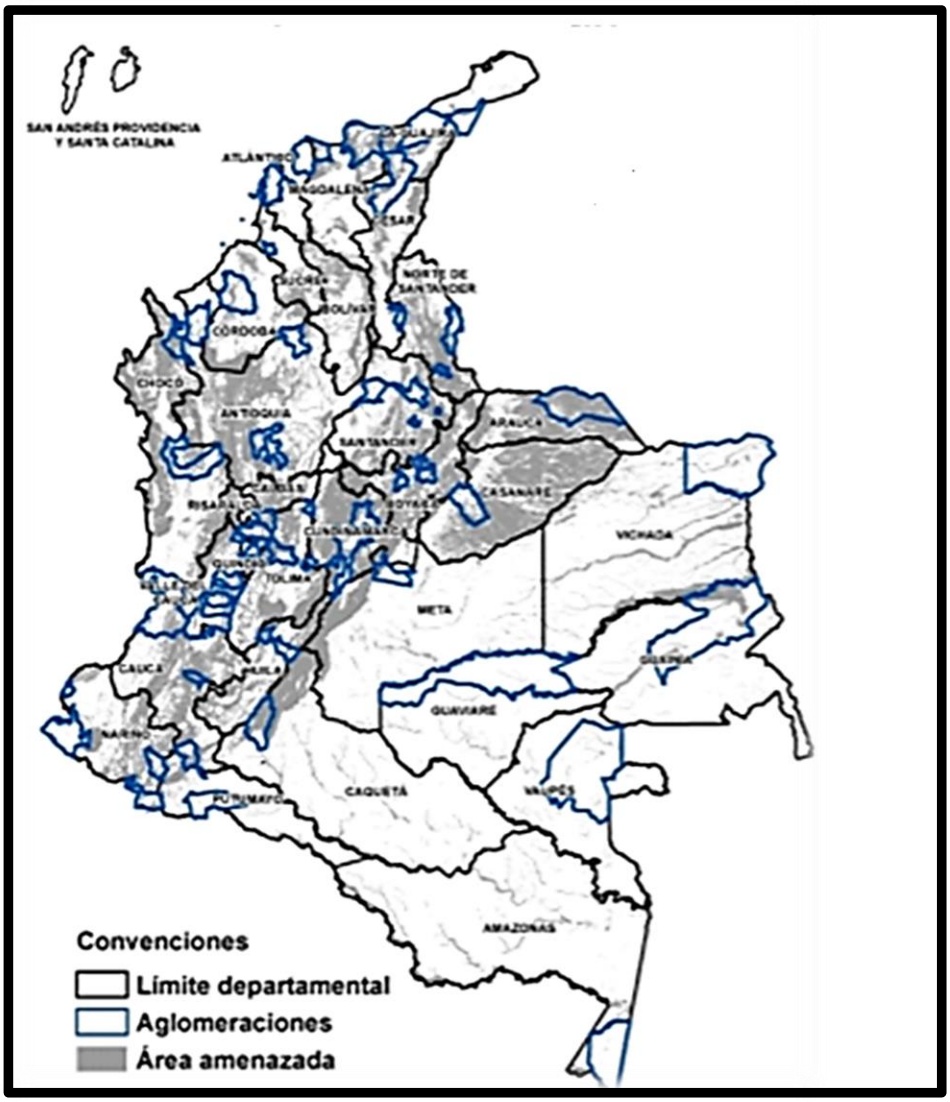
De acuerdo a la ilustración 8 y 9, 18 millones de personas están localizadas en zonas con las condiciones más críticas a amenazas hidrometereológicas, 61% de las personas expuestas vive en aglomeraciones urbanas, la mayor población expuesta se encuentra en las aglomeraciones de: Bogotá, Medellín, Putumayo, Caquetá, Guaviare, Amazonas, Vaupés, Cali. En total siete departamentos tienen más del 50% de su población expuesta a amenazas hidrometeorológicas.

	Departamento	Porcentaje población expuesta		Departamento	Porcentaje población expuesta
1	Cundinamarca	62,3	18	Valle del Cauca	33,6
2	Arauca	61,8	19	Bolívar	33,1
3	Cauca	59,7	20	Guainía	25,1
4	Boyacá	59,6	21	Bogotá D.C	24,9
5	Caldas	53,4	22	Putumayo	23,1
6	Casanare	51,3	23	Córdoba	22,1
7	Tolima	51,0	24	Meta	21,1
8	Norte de Santander	47,1	25	La Guajira	19,6
9	Antioquia	46,8	26	Vichada	17,0
10	Huila	44,0	27	Quindío	16,6
11	Nariño	43,7	28	Sucre	12,2
12	Magdalena	42,7	29	Guaviare	6,2
13	Chocó	42,5	30	Amazonas	5,9
14	Santander	39,5	31	Vaupés	4,3
15	Caquetá	39,3	32	Atlántico	0,8
16	Risaralda	36,8	33	Archipiélago de San Andrés	0,0
17	Cesar	35,4		Nacional	36,4

100% Alta exposición

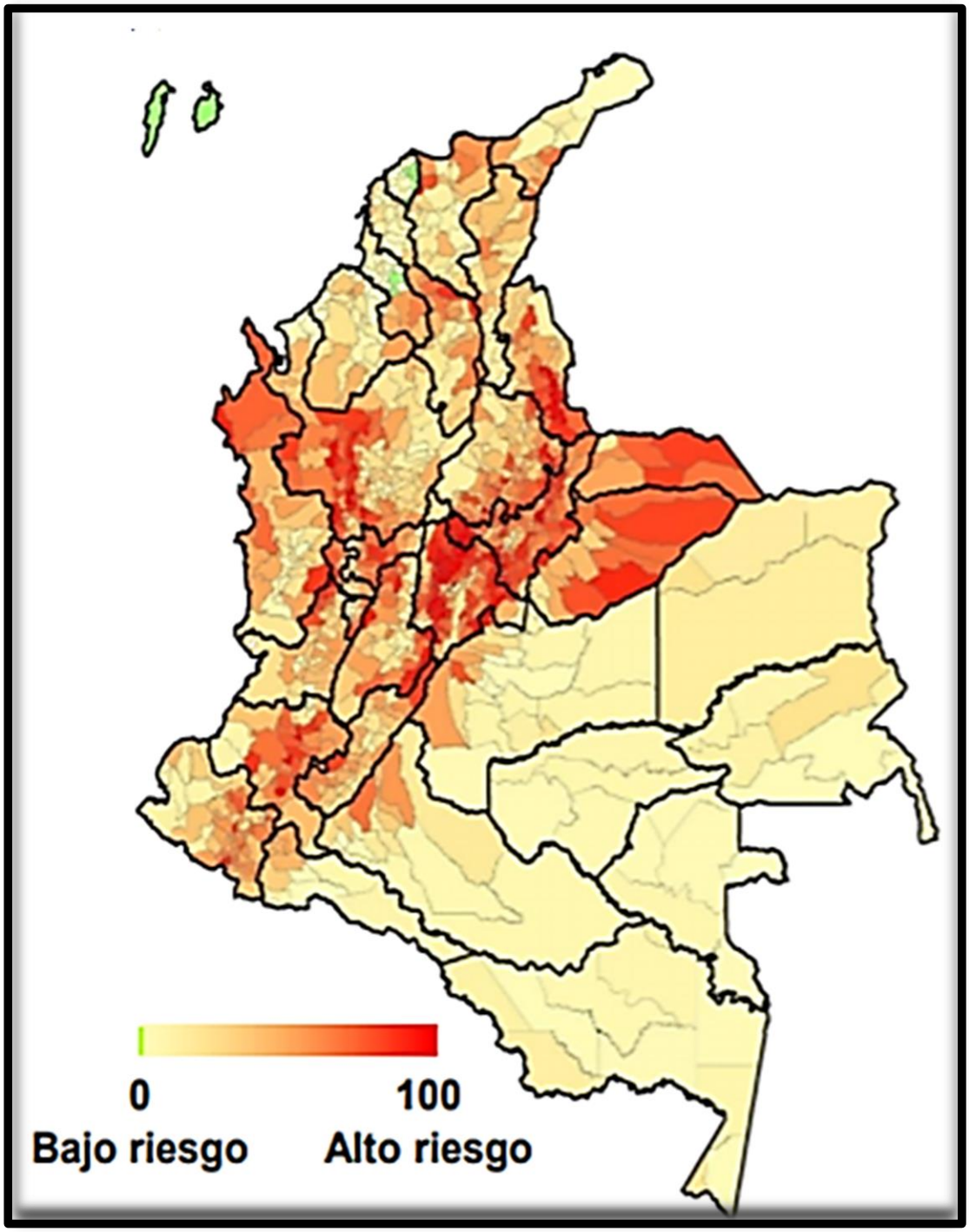
0% Baja exposición

ILUSTRACIÓN 9 Ranking departamental según su población expuesta
Fuente: DNP-DADS, 2018



MAPA No. 8 AGLOMERACIONES Y ÁREA AMENAZADA
Fuente: DNP, Sistema de Ciudades 2017, metodología DADS, 2018

Según la Ilustración No. 9, 26 municipios tienen toda su población expuesta a inundaciones, movimientos, en masa o flujos torrenciales. Ver también Mapa No.9



MAPA No 9 Proporción de población expuesta
Fuente: DNP-DADS, 2018

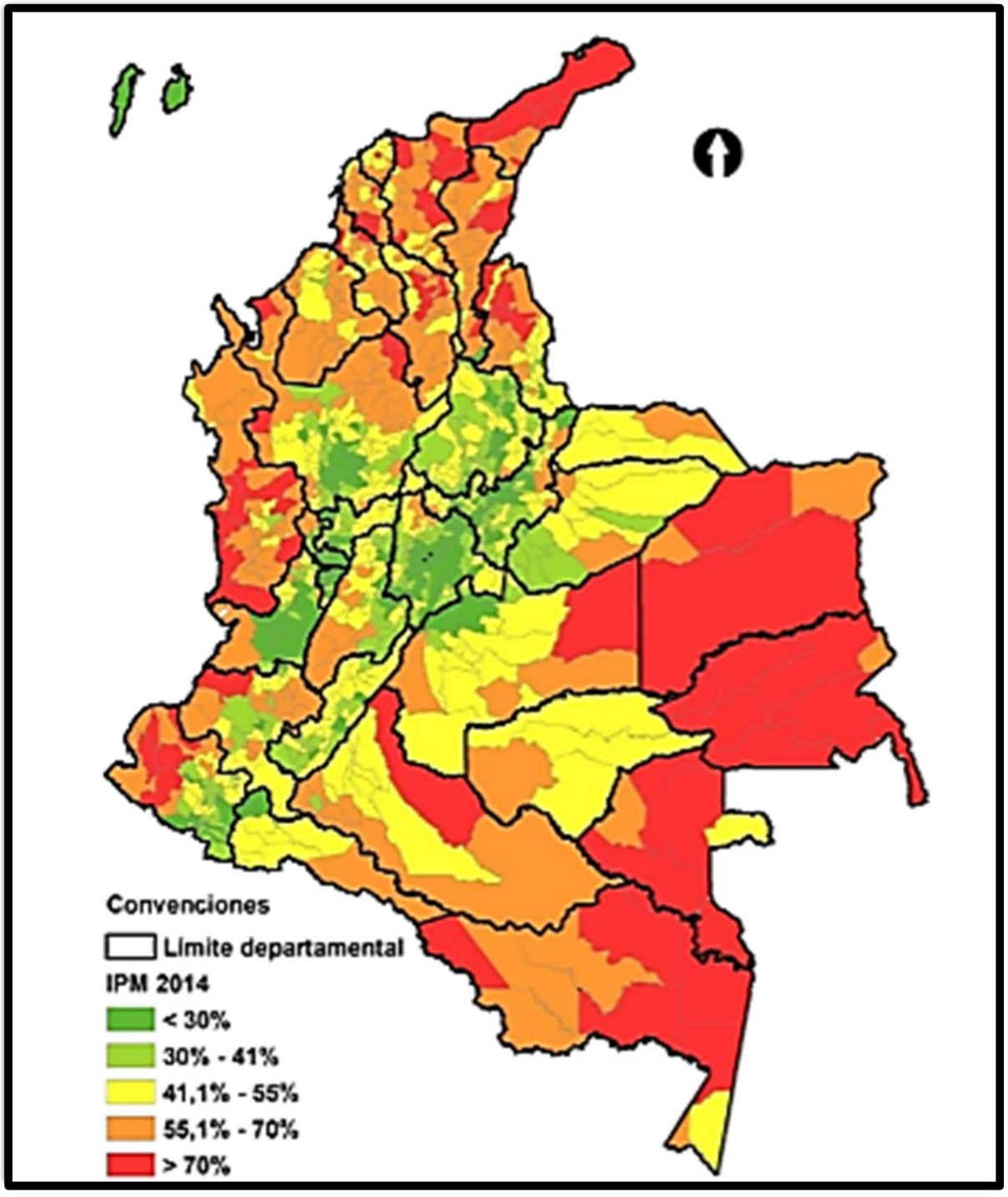
Municipios con mayor población expuesta		
	Municipio	Población expuesta
1	Sasaima – Cundinamarca	10.828
2	Muzo – Boyacá	8.668
3	Nocaima – Cundinamarca	8.157
4	Maripí – Boyacá	7.335
5	Bochalema - Norte de Santander	7.103
6	Buenavista - Boyacá	5.751
7	Pandi - Cundinamarca	5.717
8	Pamplonita - Norte de Santander	4.971
9	Armenia – Antioquia	3.945
10	Durania - Norte de Santander	3.679

Ilustración 10. 26 municipios que tienen toda su población expuesta a inundaciones, movimientos en masa o flujos torrenciales.

Vulnerabilidad social

Puede ser medida con el Índice de Pobreza Multidimensional (IPM), cuyas dimensiones reflejan la limitación en oportunidades que tienen los hogares para acceder y movilizar activos para gestionar el riesgo. La ilustración 11 muestra el indicie de vulnerabilidad según diferentes factores socio-ambientales.

En la Ilustración No. 12 se muestra los departamentos más vulnerables de acuerdo al índice de vulnerabilidad. En el mapa No 10 se ubican en el mapa los departamentos más vulnerables.



MAPA NO 10. Son 429 Municipios los que tienen más del 50% de su población con condiciones de vulnerabilidad social.

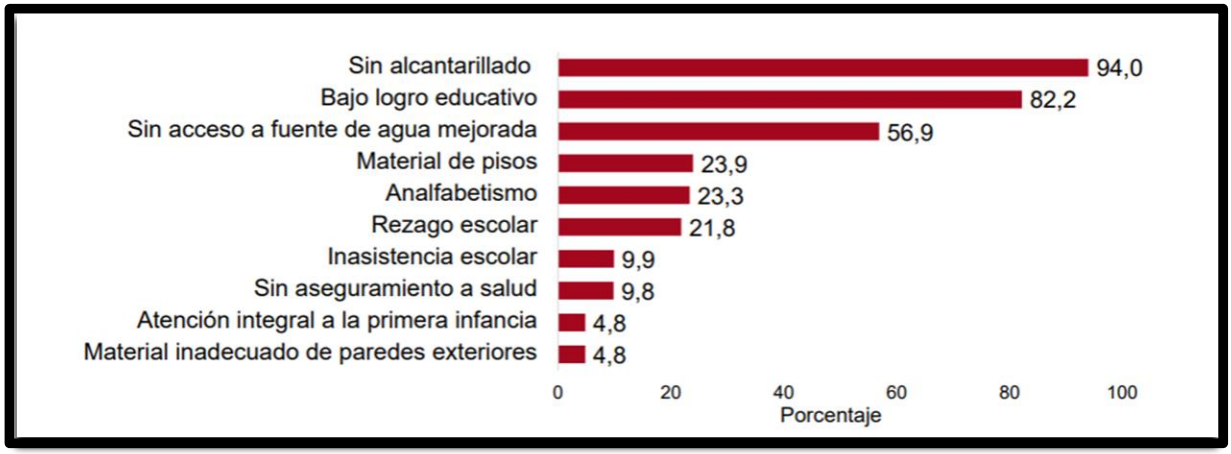


Ilustración 11. Vulnerabilidad social medida con el índice de pobreza multidimensional (IPM) Fuente: DANE con base en el Censo Rural Agropecuario, 2015

Ranquin departamental según vulnerabilidad

	Departamento	Porcentaje población vulnerable
1	La Guajira	79,8
2	Vichada	76,6
3	Vaupés	75,3
4	Guainía	71,6
5	Magdalena	67,0
6	Chocó	65,8
7	Cesar	62,8
8	Sucre	59,8
9	Córdoba	55,5
10	Caquetá	54,5
11	Guaviare	54,0
12	Bolívar	53,9
13	Arauca	52,6
14	Amazonas	52,4
15	Atlántico	52,0
16	Norte de Santander	49,4
17	Cauca	46,0

	Departamento	Porcentaje población vulnerable
18	Casanare	44,2
19	Nariño	43,8
20	Putumayo	43,7
21	Tolima	43,0
22	Huila	41,4
23	Meta	34,4
24	Santander	34,0
25	Caldas	32,7
26	Antioquia	31,7
27	Boyacá	29,3
28	Valle del cauca	27,0
29	Bogotá D.C	26,7
30	Cundinamarca	25,5
31	Archipiélago de San Andrés	24,0
32	Risaralda	23,9
33	Quindío	18,6
	Nacional	**38,8**

Bajo IPM
< 30%
30% - 41%
41,1% - 55%
55,1% - 70%
> 70%
Alto IPM

Ilustración No 12. Vulnerabilidad social 15 departamentos tienen más del 50% de su población en condiciones de vulnerabilidad social
Fuente: DANE con base en el Censo Rural Agropecuario, 2015

Indice de riesgo de desastres

Es una medida que cuantifica la proporción de la población municipal que es vulnerable socialmente y está expuesta a las condiciones más críticas de amenazas hidrometeorológicas. Ver cuadro de comentario 1.

FICHA DE COMENTARIO

FUENTE FORMULA INDICE MUNICIPAL DE RIESGOS EN COLOMBIA
PAGINA 38
EDICION
AUTOR LUIS FERNANDO MEJIA
ORIGEN DOCUMENTO DEPARTAMENTO NACIONAL DE PLANEACIÓN AÑO 2018
TEMA GESTION DE RIESGOS DE DESASTRES EN COLOMBIA

FÓRMULA GENERAL

$$Indice\ de\ Riesgo_i = \left(\frac{Población\ expuesta\ a\ la\ amenaza_i}{Población\ total_i}\right) \times \left(\frac{Población\ Vulnerable_i}{Población\ total_i}\right)$$

$$Población\ expuesta\ a\ la\ amenaza_i = Densidad\ poblacional_i \times Área\ amenazada_i$$
$$i = municipio$$

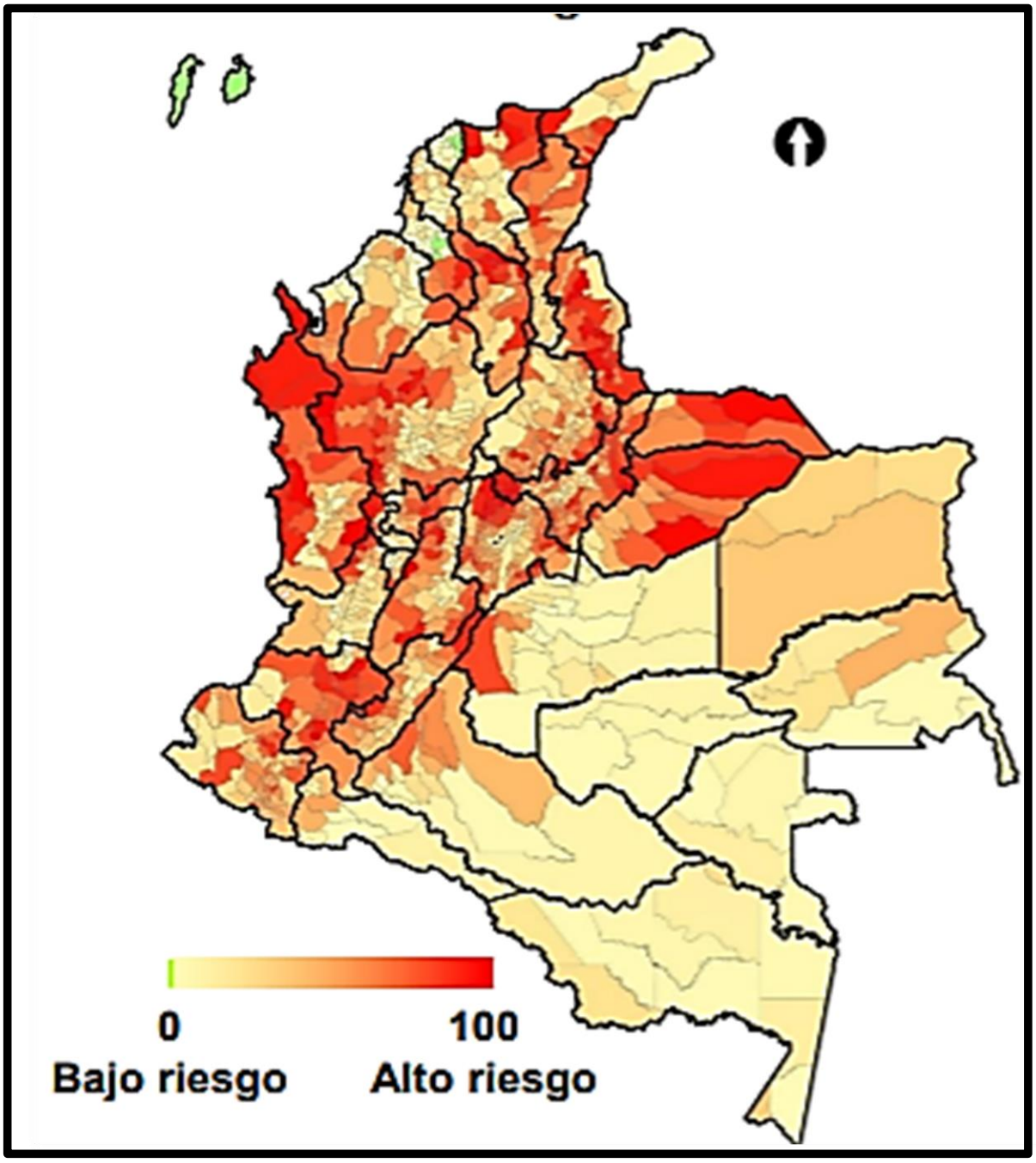
FICHA COMENTARIO 1 Formula para cálculo de indice del riesgo

En la ilustración 13 se muestran los municipios con mayor índice de riesgos o vulnerables socialmente en el país.

Municipios con mayor porcentaje de población en riesgo		
	Municipio	Porcentaje población vulnerable
1	El Tarra - Norte de Santander	75,6
2	Murindó - Antioquia	75,2
3	El Peñón - Bolívar	62,3
4	Lourdes - Norte de Santander	61,7
5	Cácota - Norte de Santander	61,0
6	Muzo - Boyacá	60,5
7	San José del Palmar - Chocó	59,8
8	Quípama - Boyacá	58,3
9	Hatillo de Loba - Bolívar	57,7
10	Almaguer - Cauca	57,3

Ilustración No 13. 6,7 millones de colombianos, equivalentes al 13% de la población del país, son vulnerables socialmente y están expuestos a las condiciones más críticas de amenazas hidrometeorológicas. Fuente: DNP-DADS, 2018

El mapa No 11 muestra que 6,7 millones de colombianos, equivalentes al 13% de la población del país, son vulnerables socialmente y están expuestos a las condiciones más críticas de amenazas hidrometeorológicas.



Mapa no 11. 6,7 millones de colombianos, equivalentes al 13% de la población del país, son vulnerables socialmente y están expuestos a las condiciones más críticas de amenazas hidrometeorológicas.
FUENTE: DNP-DADS, 2018

6.1.4. Documento de estudio de vulnerabilidad y riesgo de las redes e infraestructura de telecomunicaciones en zonas vulnerables expuestas a eventos naturales desastrosos.

Mintic, Recuperado de https://colombiatic.mintic.gov.co/679/w3-article-73949.html

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 geográfico.

Este estudio está enfocado en el análisis de vulnerabilidad física y funcional de la infraestructura de telecomunicaciones ante diferentes tipos de amenaza, el estudio también incluye 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 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.

Vulnerabilidad y riesgo de infraestructuras de telecomunicaciones. 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 que 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.

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 Riesgo = Amenaza o Peligro x Vulnerabilidad

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

En este orden de ideas, en la presente investigación se incluirá 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, 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.

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 , así se tiene: P (X > Xo / t).

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.

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.

Modelo de gestión del riesgo de desastres propuesto por MINTIC

El Ministerio de Tecnologías de la Información y las Telecomunicaciones ha definido un modelo estándar que incluye una gestión integrada del riesgo en términos de aplicar buenas prácticas en los procesos corporativos tanto de las instituciones, en este modelo los pasos en la gestión del riesgo son:

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 riesgo

Definiciones importantes:

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 cómo 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.

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.

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.

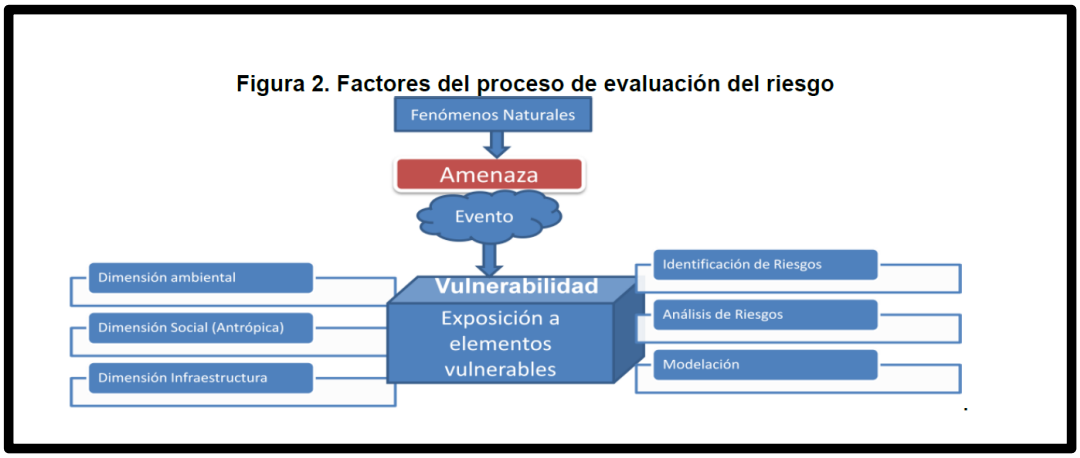


Ilustración No 13 factores del proceso de evaluaciòn del riesgo
fuente: Cintel

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. Esta 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 dado que la población colombiana necesita servicios constantes y continuos de los servicios portador, telefonía celular, telefonía fija e internet.

Definición de umbrales de tolerancia de riesgos. Los umbrales de tolerancia se definen para cada una de las amenazas, en la medida en que una amenaza natural afecta las comunicaciones en ese umbral entonces se debe definir un riesgo como ALTO y la empresa que es proveedora de los servicios debe establecer controles ante un riesgo, las entidades nacionales ya han predefinido los umbrales de riesgo de la siguiente manera:

Diagnóstico de las amenazas naturales:

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

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

o **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.

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

6.1.4.5 Infraestructuras sujetas a vulnerabilidades. Dentro de una infraestructura de telecomunicaciones los elementos sujetos a vulnerabilidades son:

- 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 de riesgo y bajo al menor nivel de riesgo.

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

Ilustración No. 14. Definición de niveles de riesgo
Fuente: Cintel

Definicion de riesgos. Para definir este universo de riesgos se requiere superponer las capas georreferenciadas en un mismo mapa, se debe definir cuáles son las sedes de infraestructuras críticas dentro de este sistema de capas para el funcionamiento de la Red Nacional de telefonía fija, telefonía móvil e internet del proveedor en cuestión.

Esta información dentro de la presente investigación no se encontró disponible en internet y es importante pues se requiere superponer la capa de las antenas de telecomunicaciones del proveedor con los mapas de amenazas naturales emitidos por las entidades gubernamentales. Se debería recopilar la ubicación de todos los elementos de la infraestructura crítica de telecomunicaciones y superponer este mapa

con el mapa de amenazas críticas para las amenazas hidrometereológicas, sismos y volcanes.

Se debe establecer en el sistema de capas 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.

De acuerdo a la amenaza hay una cobertura geográfica específica de la misma que debe ser establecida, en donde se debe establecer una gradualidad de alta a baja por evento o amenaza natural.

Amenaza Volcánica. Se debería realizar un mapa de cobertura por 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. La cuidad de Tumaco y en general las ciudades y pueblos donde históricamente se hayan presentado Tsunamis poseen mapas de amenazas como licuación, golpe de ola e inundación salobre, extraídas de los mapas proporcionados por las

entidades de prevención y atención de desastres, este mapa debería superponerse con cada elemento de la red de telecomunicaciones en estas ciudades.

Amenaza por Inundación. Con base en la información reciente de las inundaciones ocurridas en Colombia, se procedió e debería elaborar un mapa de inundación con los parámetros ya preestablecidos por el instituto Agustín Codazzi:

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. 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.

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 SRTM8 de 90 metros de la Nasa.

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 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.***

Se deberían identificar todos los elementos físicos y funcionales que hacen parte de la de la red de telecomunicaciones que por servicio se va a modelar con las capas superpuestas del mapa de inundaciones.

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 anterior, los pasos para realizar la identificación de los riesgos se pueden determinar de la siguiente manera:

1. Selección de los servicios y las infraestructuras vitales 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 en una base de datos georreferenciada.
7. Estructuración de las capas de información para análisis espacial.
8. Análisis espacial y extracción de los elementos de red sometidos a cada amenaza.

9. Identificación de la exposición de cada elemento a determinado tipo de amenaza.
10. Identificación y consolidación de los elementos expuestos a amenazas.
11. Identificación de la vulnerabilidad de todos los elementos de las infraestructuras crítica por proveedor 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, porcentaje de 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.

Calificación de amenazas por vulnerabilidades y su priorización. Los riesgos son resultado de los siguientes valores:

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

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

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

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

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

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

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

- Mapa y tablas de Amenaza Sísmica Red Telefonía Móvil
- Mapa y tablas de Amenaza Volcánica Red Telefonía Móvil
- Mapa y tablas de Amenaza Tsunami Red Telefonía Móvil
- Mapa y tablas de Amenaza Inundación Red Telefonía Móvil

Para el cálculo se debe asumir 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 alta) 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.

Los mapas georreferenciados pueden ser obtenidos de las bases de datos mencionadas en la Ilustración 15.

para ejecutar el modelo por una entidad gubernamental o un operador de la infraestructura de telecomunicaciones se debe definir:

Definición de niveles de adversidad al riesgo: Se definen cuáles son los mínimos y máximos

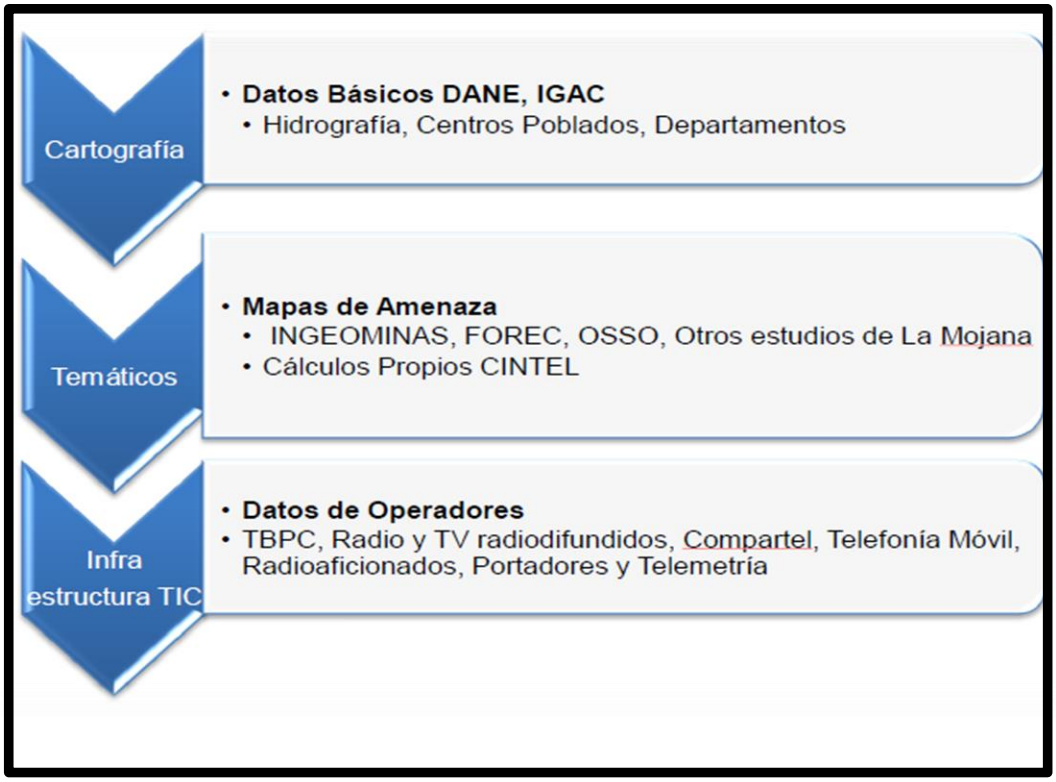


Ilustración No 15. Fuentes de mapas y tablas para la base de datos de riesgos Índice municipal de riesgo de desastres de Colombia ABRIL 2018

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, amenazas antrópicas, 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.

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.

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 tipos de impacto asociados y los planes de mitigación y contingencia que se deben ejecutar para minimizar el impacto. Es importante determinar adicionalmente el impacto social y medio-ambiental 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.

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. Actualmente, en Colombia y a nivel internacional, sin lugar a dudas, los servicios de telefonía móvil celular y los servicios de acceso a INTERNET se constituyen en servicios vitales para la totalidad de los sectores sociales y económicos del país, ver mapa 12, índice de penetración de internet por departamentos.

En la ilustración No 16 se detalla la cantidad de hogares con teléfono celular en

comparación de hogares con internet fijo. El uso de dispositivos móviles se ha incrementado en Colombia un 16% en los últimos cinco años. En cuanto a los computadores y tabletas la tenencia ha incrementado un 14 %.

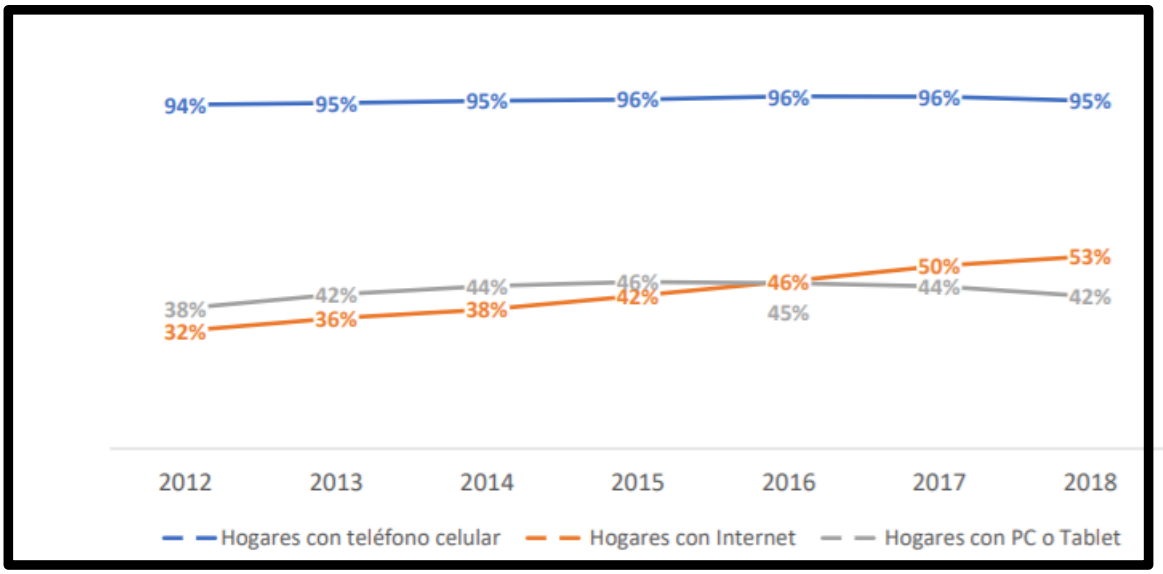


Ilustración No 16 Porcentaje de hogares con teléfono celular, internet fijo y PC
Fuente Dane

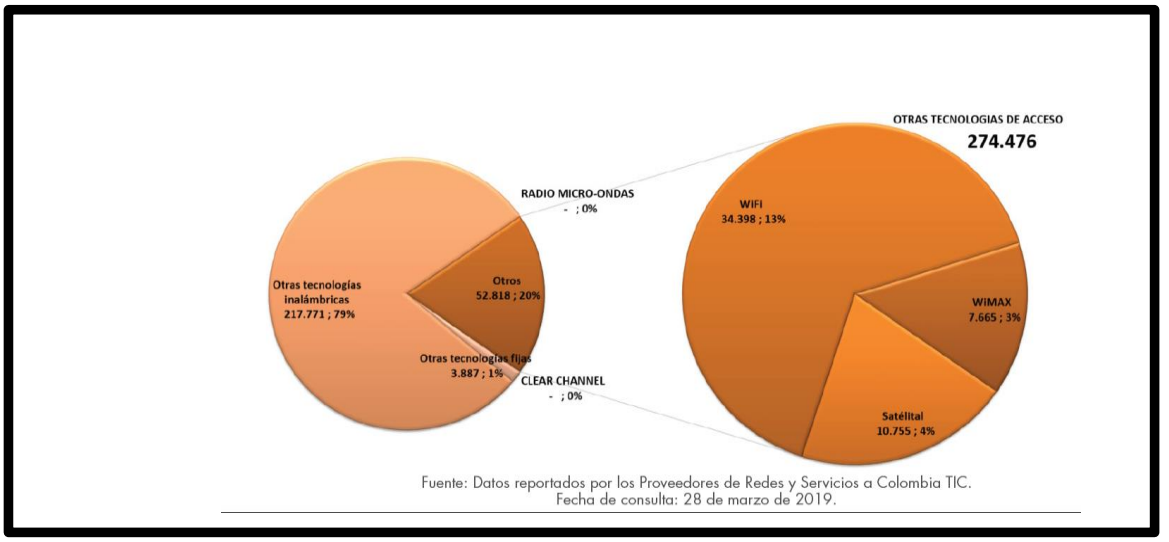
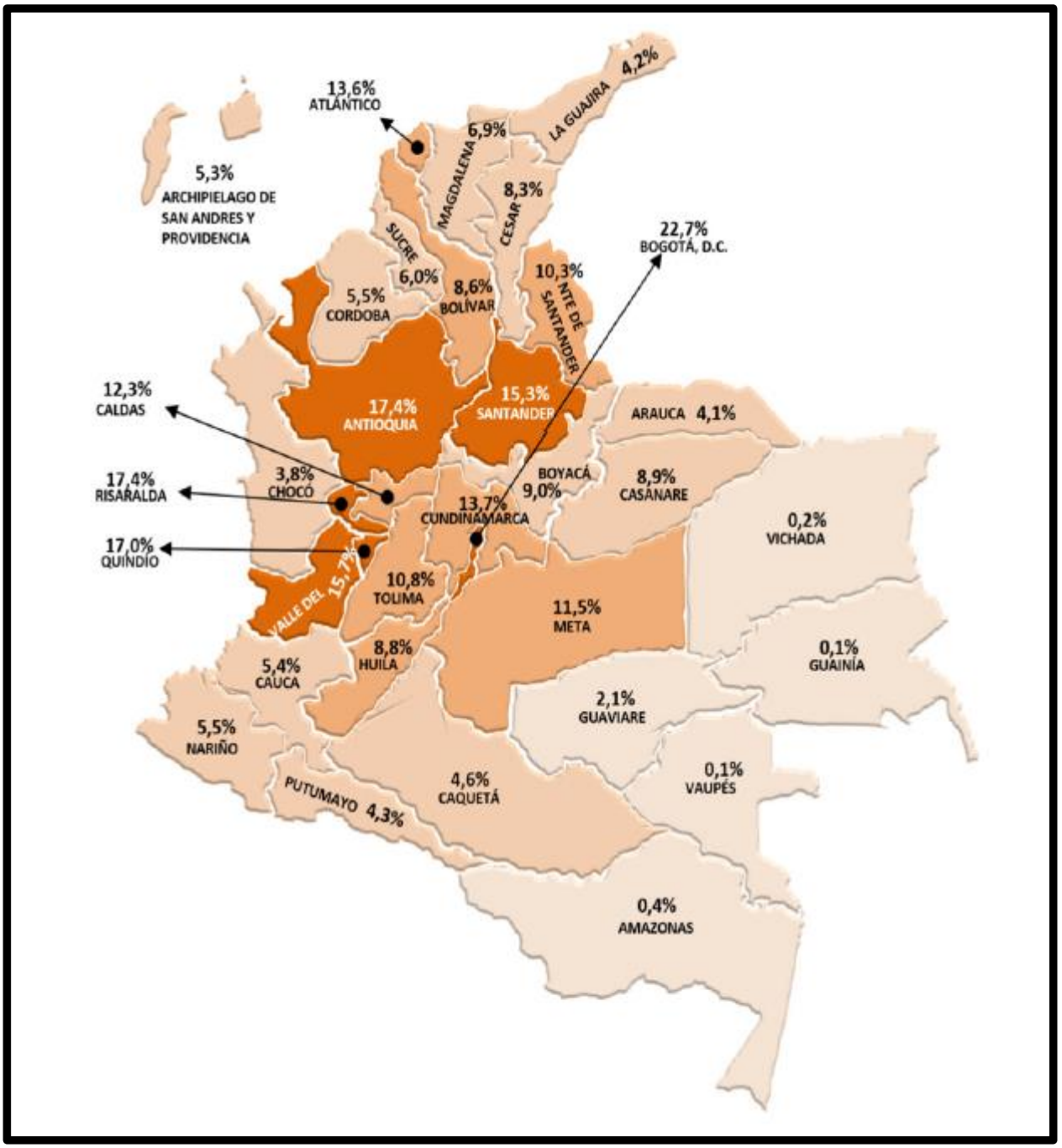
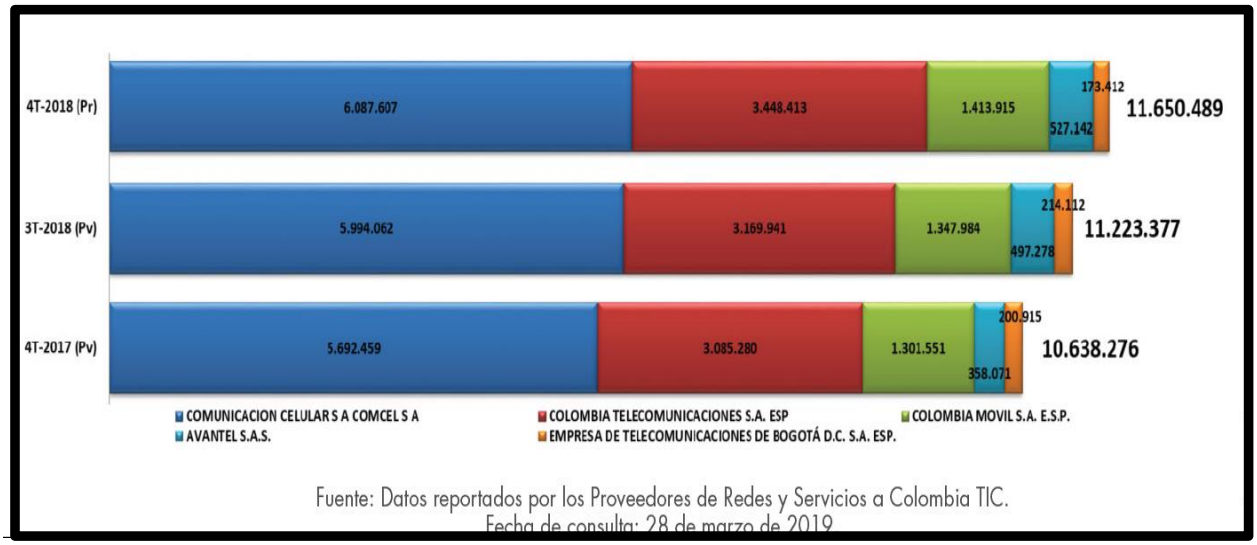


Ilustración no 17. Otras tecnologías de acceso a internet
fuente: datos reportados por los proveedores de redes y servicios a Colombia TIC.
Fecha de consulta: 6 de julio del 2018



Mapa No. 12. Índice de penetración de internet por departamentos en Colombia 2018
Fuente Cintel

En la ilustración 17 se observa que al finalizar el primer trimestre de 2018, las conexiones a Internet fijo en otras tecnologías de acceso alcanzaron los 235.895 accesos, los cuales representan el 3,7% del total de accesos fijos. Se destacaron, en términos de participación, las tecnologías de acceso inalámbricas, tales como Otras tecnologías inalámbricas (79%), WiFi (11%) y Satelital (4%). En



Fuente: Datos reportados por los Proveedores de Redes y Servicios a Colombia TIC.
Fecha de consulta: 28 de marzo de 2019

la ilustración 18, se detalla la cantidad de suscriptores comunicación móvil en Colombia.

Ilustración 18

6.4 Descripción, topología general de los servicios vitales de telecomunicaciones y sus elementos básicos. Rescatado de:

https://cintel.co/wp-content/uploads/2013/05/23.estudio_sectorial_2006_Estudio-del-Sector-de-la-Telecomunicaciones-en-Colombia-2006.pdf.

Los principales elementos físicos de la red del proveedor de telecomunicaciones, 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.

Servicio de Telefonía Local

El servicio de telefonía local pública 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 Ilustración 19 ilustra los principales elementos de la red de TPBCL.

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: Resolución 87 – CRC

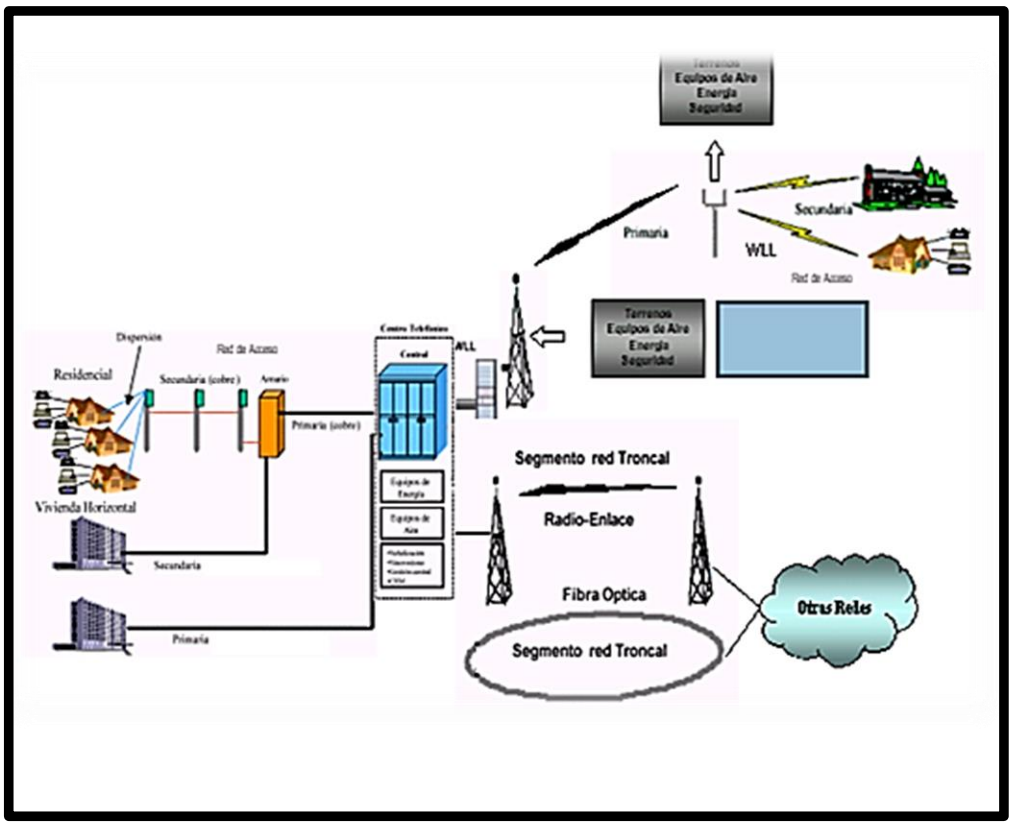


Ilustración no. 19. Elementos de una red telefonica
Fuente ilustración Cintel

Los centros telefónicos (centrales de conmutación), establecen la conexión física entre dos abonados de la Red telefónica 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 y otros operadores y los abonados existe un camino físico, el cual puede ser totalmente alámbrico o inalámbrico, según el diseño de red del operador, el cual está segmentado física

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

Tabla No 3 . Elementos de una red telefonica
Fuente ilustración Cintel

funcionalmente así:

Red Troncal: Es el segmento de red que une las diferentes centrales de una red o la red de telefónica 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. 148 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. 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. 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.

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.

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, 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.

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).

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 geográficos para cubrir un área. Los canales discretos son susceptibles de ser reutilizados en diferentes células dentro del área de cubrimiento.

La ilustración No 20 muestra el espectro radioeléctrico actualmente atribuido a comunicaciones móviles:

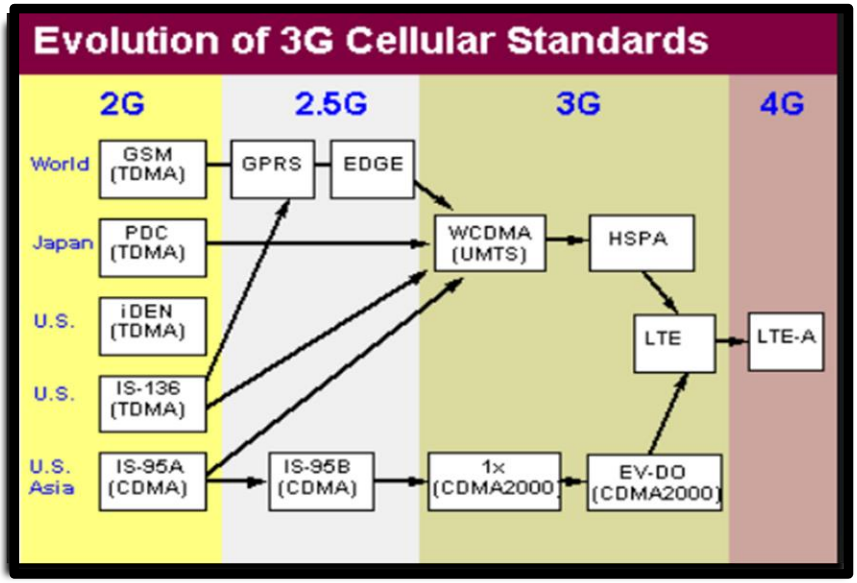


Ilustración No. 20. Evolución tecnología celular

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

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).

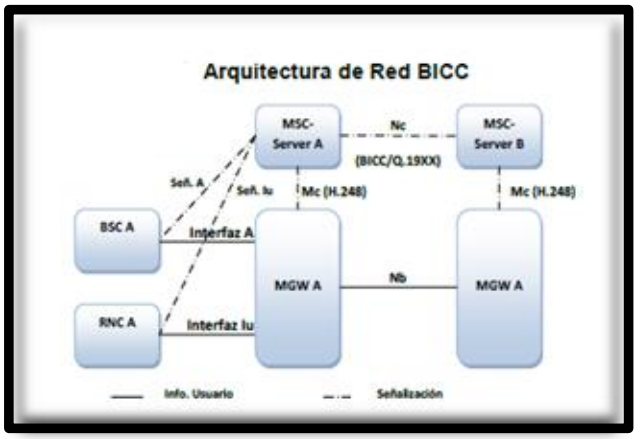


Ilustración no.21 Arquitectura de red BICC

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

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

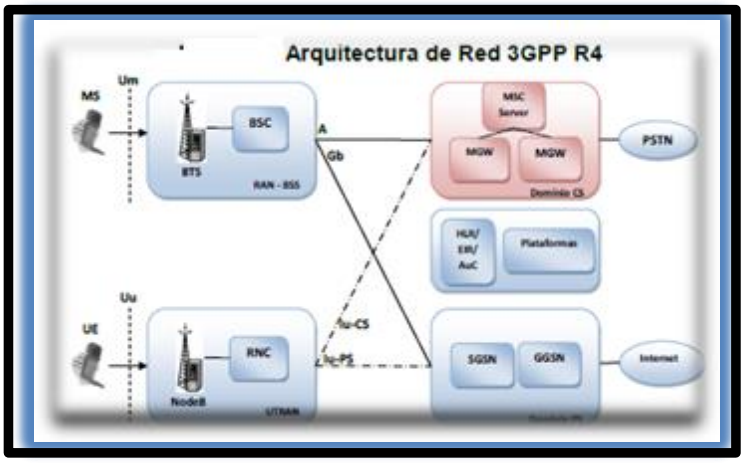


Ilustración No. 22 Arquitectura de Red BICC

En la arquitectura GSM, el tráfico se concentra en las BSCs y MGWs (únicamente el tráfico de señalización llega al softswitch). Estos nodos 161 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: 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 geoIlustración con capacidad de conmutación automática.

Para eventos de catástrofe en zonas geogràficas 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.

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 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.

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 penetraciónde 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.

Los componentes básicos de DSL son:

CPE: 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 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).

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 geográfica.

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 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.

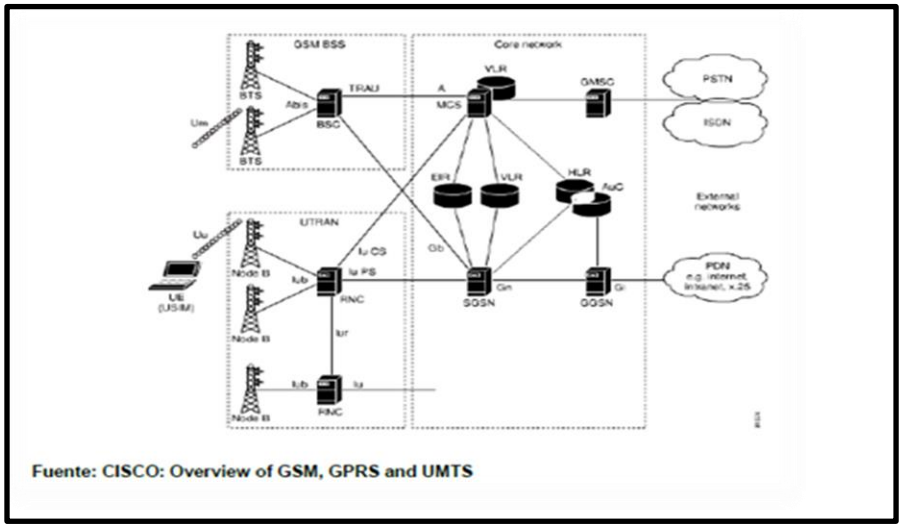


Ilustración No 23 Arquitectura UMTS

Vulnerabilidad de las redes vitales de telecomunicaciones.

La vulnerabilidad es una característica intrínseca de una infraestructura o sistema que lo hacen susceptible al daño al ser explotada por una amenaza, los componentes de una red desde este estudio 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.
- 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 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 organizados en la siguiente tabla

Componente de Infraestructura	Vulnerabilidades
Humano	Conocimiento (falta, distracción, engaño confusión)
	Etica (lealtades divididas, codicia, mal. intuición)
	Entorno del usuario (interfaz de usuario funciones, cultura corporativa)
Política	Intrpretación errada
	Excesiva regulación
	Desactualización

Componente de Infraestructura	Vulnerabilidades
Instalaciones físicas	Dependencia de otras infraestructuras
	Remotamente manejada
	No cumplimiento de protocolos y procedimientos establecidos
	Exposición a elementos
Energía eléctrica	Limitaciones del suministro
	Destrucción física
	Dependencia del combustible
Hardware	Al ambiente (temperatura, humedad, polvo, luz solar, inundaciones)
	ciclo de vida (repuestos, reemplazo de equipos, capacidad, envejecimiento y obsolescencia)
	Energía electromagética (EMI, EMC, ESD, RF, EMP, HEMP, IR)
Software	Complejidad de los programas
	Habilidad para controlar
	Errores en los códigos
Tráfico	Autenticación erronea
	Encapsulación de contenido malicioso
	Insuficiente inventario de componentes críticos
	Encriptación
Redes	Interconexión (interoperabilidad, interdependencia, conflictos)
	Complejidad

TABLA No. 4 Componentes de infraestructura y sus vulnerabilidades.

Fuente MINTIC

7. PROPUESTA METODOLÓGICA

7.1 Propuesta metodológica para el desarrollo de proyectos de gestión de riesgos de desastre DRP para proveedores de Telecomunicaciones

Definiciones. Se toman como referencia las siguientes definiciones de la norma ISO 31000, las cuales servirán de base para el desarrollo de esta Metodología:

Aceptación del riesgo: Decisión informada de asumir un riesgo concreto.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de mismo.

Causa: Origen, comienzo de una situación determinada que genera un efecto o consecuencia.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.

Control: Medida que modifica el riesgo.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Fuente de riesgo: Elemento que solo o en combinación tiene el potencial de originar un riesgo.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Identificación de riesgos: Proceso de encontrar, reconocer y describir riesgos.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su probabilidad

Política para la gestión del riesgo: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo

Proceso: Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos (Tomada de la ISO 31000:2009).

Valoración del riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Riesgo Operativo: posibilidad de incurrir en pérdidas por deficiencias como fallas o inadecuaciones en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos (incluye el riesgo legal y riesgo reputacional).

RTO: Recovery Time Objective: Es el máximo tiempo permitido que un proceso puede estar caído como consecuencia de un evento catastrófico.

RPO: Recovery Point Objective: Son los primeros datos que permiten volver a ofrecer el servicio. Identifica si para la recuperación del proceso que se haya visto afectado se necesita disponer de la información que se tenía justo antes de que sucediera el incidente, o si, por el contrario, se puede utilizar la información anterior (hasta qué Momento: una hora, un día, dos días…)

Política asociada. Los riesgos de desastres serán evaluados y mitigados acorde con su probabilidad de ocurrencia e impacto en el negocio, bajo los requerimientos legales del decreto 2137 de 2017.

Comité de Riesgos Se debería crear un Comité de gestión de riesgos definido por el proveedor de Telecomunicaciones, quier será el responsable del cumplimiento de la gestión de todas las actividades concernientes a la identificación, planeación, administración, seguimiento, control y comunicación de los riesgos dentro de sus sedes críticas. Adicionalmente, son funciones del Comité las siguientes:

- Validar y aprobar los criterios para aceptación del riesgo, los niveles de riesgo aceptables y los riesgos residuales del Sistema de Administración de Riesgos.

- Validar y aprobar el plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para administrar y gestionar los riesgos del sistema de administración de riesgos.
- Garantizar que el tratamiento definido para cada uno de los riesgos estén alineados con los objetivos del negocio.

Se debería establecer una periodicidad mínima trimestral para la realización de los comités ordinarios. Sin embargo, cualquiera de sus integrantes puede citar a reunión extraordinaria cuando se presenten una o varias de las siguientes situaciones:

Cambios considerables en los negocios, infraestructura tecnológica, infraestructura física, Personal o cualquier modificación que pueda alterar el Sistema de Administración de Riesgos de desastres.

Ante la evidencia de incumplimiento en la ejecución de planes de tratamiento de riesgos o cualquier situación que impida o dificulte la ejecución de los objetivos del negocio que requieran la intervención y toma de decisiones por parte de la alta Dirección.

Propietario de los Riesgos

Con base a los procesos incluidos en la gestión de riesgos, se define a un líder por sede o infraestructura crítica.

Se deben identificar y valorar los riesgos asociados a cada sede crítica y realizar seguimiento periódico (mínimo cada tres meses), al estado de avance de las actividades definidas en los diferentes planes de acción que establezca en el marco del plan de tratamiento del riesgo.

En todo caso, los propietarios de los riesgos velarán por la implementación y mejora de controles necesarios y suficientes para el tratamiento de los riesgos conforme a los planes establecidos.

Toda vez que se haya dado cierre o ejecución del tratamiento para mitigar los riesgos identificados, los propietarios del riesgo deben actualizar su matriz de riesgos e informar de

manera formal escrita a los administradores de riesgo (de desastre operativo, desastre natural siniestro) el estado de los mismos, para así disponer de una gestión sincronizada y actualizada, con el fin de determinar la efectividad del control en la mitigación de dichos riesgos.

Administradores de Riesgo.

Las empresas de telecomunicaciones deben definir un responsable o administrador de riesgo que acompañe a los dueños de procesos y propietarios de riesgos en la consolidación de los riesgos identificados, analizados, evaluados y tratados, así como realizar seguimiento a la ejecución de los planes de acción reportadas por los propietarios de los riesgos.

Para el caso de los riesgos relacionados con Desastres, debe haber un administrador de riesgos por ciudad, el cual debe asesorar a los responsables de los riesgos por sede o infraestructura crítica.

Es responsabilidad de los administradores de riesgo mantener actualizada las respectivas matrices, conforme a lo suministrado por los propietarios de riesgo.

Así mismo, generar los reportes del estado de la administración de los riesgos de los procesos y presentar el mismo al Comité de riesgos de desastres del proveedor.

Área de Control Interno.

Las funciones del área de Control Interno o quien haga sus veces en cada sede crítica del proveedor, frente a la administración y gestión de riesgos de desastres, están orientadas a evaluar a través de Auditorias Periódicas a los procesos definidos en el alcance de su revisión con el fin de validar la efectividad y cumplimiento de los controles, tomando como mínimo los criterios de evaluación de controles definidos previamente a este procedimiento, e informando a la Gerencia encargada de desastres del Proveedor y a sus Administradores de Riesgo los hallazgos identificados.

Adicionalmente realizará seguimiento a los planes de tratamiento definidos por cada Propietario de Riesgo para los riesgos identificados y los hallazgos evidenciados por Control Interno o quien haga sus veces en cada empresa, utilizando un formato único definido por el comité de riesgos o el que se disponga por las áreas de Calidad de cada compañía**.**

Es responsabilidad del área de control interno o de quien haga sus veces en cada empresa dar cierre a las acciones correctivas en conjunto con el propietario de riesgos, cuando los controles dispuestos para mitigar el riesgo asociado sean puestos en marcha, con el fin de determinar la efectividad del mismo.

Procedimiento

Tipos de riesgo de desastre. Desastre operativo, la provisión de los servicios de Internet colapsa ya sea telefonía local o celular, ocasionando la perdida de suministro de servicios públicos.

Desastre natural: enormes pérdidas materiales y vidas humanas ocasionadas por eventos o fenómenos **naturales**, como terremotos, inundaciones, tsunamis, deslizamientos de tierra, y otros.

Desastre por Siniestro: Causado intencional o accidentalmente por personas.

Fuentes de riesgo. Es muy importante identificar las fuentes generadoras de los riesgos y categorizarlos para su eficiente gestión, para efectos de implementar esta metodología se tomaran los siguientes:

Cada riesgo identificado deberá categorizarse en alguno de estos grupos:

Recurso Humano: Eventos de riesgo cuyo origen está asociado a actos que son incompatibles con la legislación laboral, con los acuerdos internos de trabajo, políticas, procedimientos y en general, la legislación vigente.

Tecnológicos: Eventos de riesgo derivados de incidentes por fallas tecnológicas. Dentro de esta clasificación están incluidos todos los eventos que causen daños, datos e información de calidad inapropiada, interrupción, alteración o fallas derivadas del uso o dependencia en el hardware, software, sistema, aplicaciones, redes, equipos de telecomunicaciones y cualquier otro canal de distribución de información en la prestación de servicios de la compañía.

Externos: Eventos de riesgo debidos a actos realizados por agentes externos a la entidad, tales como clientes, proveedores, asonadas, orden público, medio ambiente, ataques informáticos, espías financieros, etc., que buscan, apropiarse indebidamente o destruir los recursos y activos de la organización, así como incumplir normas o leyes. Adicionalmente, corresponde a riesgos asociados al uso indebido de información de la Compañía por parte de terceros.

Infraestructura y ambiental: es la posibilidad de presentarse daño o afectación sobre la infraestructura física, inclusive la infraestructura como suministro eléctrico, así como aquellos relacionados con daño o afectación por inundaciones, incendios, tormentas, animales, entre otros.

Operativos: Es la posibilidad de pérdidas ocasionadas en la ejecución de los procesos y funciones de la Compañía por fallas en procesos, sistemas, procedimientos, modelos o personas que participan en dichos procesos. *Fases para la administración de riesgos.*

A continuación se describen las fases que se tiene en cuenta para realizar la valoración de los riesgos acorde con las recomendaciones dadas por la norma ISO 31000.

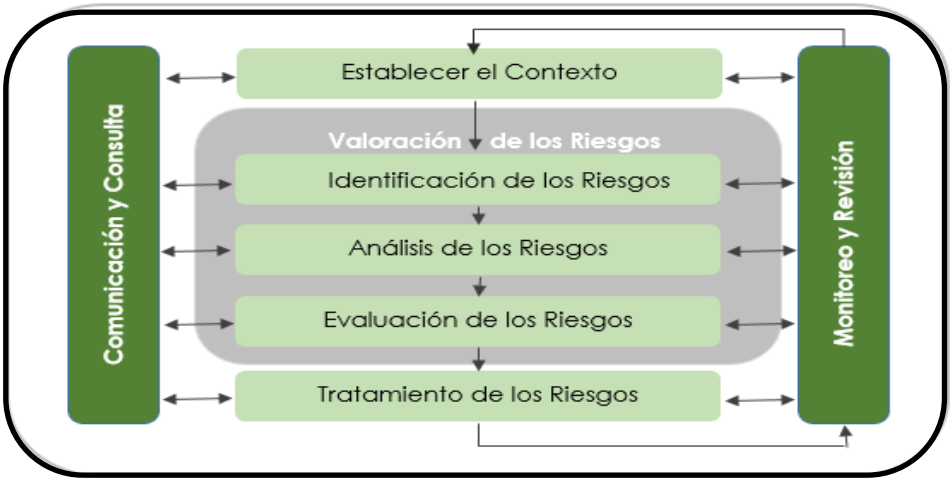


Ilustración No 25 Componentes de Infraestructura y sus vulnerabilidades
FUENTE ISO 31000

Cada una de las fases descritas deben ser formalizadas por medio de actas por los responsables de los riesgos.

El ciclo descrito para la administración y gestión de riesgos se deberá ejecutar por lo menos una vez al año o cada vez que se presenten algunos de los siguientes eventos:

- Cambios en la Organización
- Cambios en los Objetivos y procesos de negocio
- Cambios en los terceros que administran procesos críticos.
- Cualquier cambio o circunstancia que pueda incidir directamente en los niveles de riesgo.

- Cumplimiento de normativa regulatoria vigente.

FASE 1 – Establecer el contexto

Esta etapa consiste en definir los parámetros internos y externos que se han de tener en cuenta cuando se administra y gestiona el riesgo.

Contexto externo: Ambiente externo en el cual la organización busca alcanzar sus objetivos. Son situaciones del entorno; pueden ser de carácter Social, cultural, económico, tecnológico, político, legal, etc.

Contexto interno: Ambiente interno en el cual la organización busca alcanzar sus objetivos. Son situaciones internas que están relacionadas con: la estructura, cultura organizacional, el modelo de operación, el cumplimiento con los planes y programas, los recursos humanos y económicos, etc.

Nota: La definición del contexto interno y externo de cada Empresa, se deberá realizar en función de las características de cada negocio.

FASE 2 - Identificar el riesgo. Esta etapa consiste en identificar los riesgos asociados al proceso y determinar las fuentes, causas y consecuencias potenciales que puedan afectar el cumplimiento de los objetivos planteados para las sedes Críticas**.**

El proveedor de telecomunicaciones debería indicar cuales son las sedes críticas según la cantidad de ciudadanos que afecte en caso de desastre, ya sea porque su infraestructura colapse operativamente o porque la infraestuctura ocasione daños sobre un valor de

población expuesta, en el que se considere que la amenaza ocasione pérdida de vidas humanas al colapsar.

Estas sedes críticas se deben escoger también en un estudio de interposición de capas de amenazas e infraestructuras, las sedes que estén dentro de las zonas de alta probabilidad de amenaza natural o antrópica deben incluirse dentro de las infraestructuras expuestas que deben entrar en la Gestión de Riesgo de Desastres del proveedor.

Para la realización de esta metodología se propone el diseño de un aplicativo de superposición de capas en el que estén todas las capas de amenazas, y las áreas de influencia con mayor impacto, áreas de población aglomeradas que ya provee IDEAM, Ingeominas o El instituto Agustin Codazzi, puedan superponerse con las sedes criticas operativas de la infraestructura del proveedor, de esta manera, se puede modelar el impacto de la amenaza y definir con claridad las sedes donde se debería invertir en los planes de tratamiento de riesgos por desastre.

Las Sedes que defina el operador por Criticas operativamente debería realizar planes de contingencia Operativa y plan de Continuidad de Negocio de acuerdo a ISO 23001

Una adecuada identificación del riesgo debe considerar los siguientes parámetros, de acuerdo con los campos a registrar en el formato **Análisis y Evaluación de Riesgos:**

Sede Crítica a la que pertenece el riesgo: Los riesgos de desastres son caracterizados por sede, cada sede crítica posee condiciones particulares, característica de

entorno diferentes, por tanto se debe realizar un análisis de entorno diferente por cada sede.

Información general de la Sede Crítica Determinar ubicación, vías de acceso, actividad principal y complementaria, descripción de producción o servicio resaltando la actividad que pueda generar riesgo de desastre para la sociedad, listado general y la descripción, cantidad de procesos, de sustancias químicas, de maquinaria que pueden ser fuente de desastres, área total construida, área libre, disposición de edificaciones, número de pisos, año de licencia de construcción, tipo de espacios y número, espacios comunitarios y equipamiento para emergencias existente, horario de funcionamiento, población expuesta al interior de la instalación evaluada.

Tipo de riesgo: Se tipificarán los riesgos como desastre operativo, desastre natural o siniestro.

ID Riesgo: es el código con el cual se debe identificar un riesgo, teniendo en cuenta el estándar RDO###.Para Desastre Operativo (RDO001); RDN### para Riesgo de desastre natural, RDS## Desastre por siniestro.

Descripción del Riesgo: breve descripción del riesgo identificado frente al subproceso o activo involucrado, cuya finalidad es contextualizar la relación riesgo vs causa vs consecuencia.

Amenazas: Se definen los siguientes tipos de amenazas:

Hidrometeorológicas: inundaciones, deslizamientos, granizadas, avalanchas, vendavales, mares de leva, tormentas, huracanes, tornados, sequías, incendios forestales.

Geológicas: Fallas, sismos, tsunamis.

Volcánicas: 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.

Amenazas Antrópicas: 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.

Consecuencias: El propietario del riesgo, debe determinar los posibles resultados indeseados que se pueden generar con la materialización del riesgo.

Propietario del riesgo: Asignar el Propietario del riesgo, quien será el responsable de diligenciar completa y oportunamente, los aspectos relacionados con las fases de la gestión de riesgos.

FASE 3 – Analizar el riesgo. Esta etapa implica el desarrollo y la comprensión del riesgo, brindando una entrada para su evaluación, así como criterios para determinar si es necesario no tratar los riesgos, al igual que las estrategias adecuadas para su tratamiento.

Probabilidad. Para cada riesgo se debe estimar la probabilidad de que ocurra, considerando las causas establecidas, la probabilidad se asigna de manera cualitativa en una primera instancia utilizando la siguiente tabla:

PROBABILIDAD			
NIVEL	**DESCRIPTOR**	**FRECUENCIA**	**PERIODO**
1	Muy baja	Puede ocurrir	Difícilmente ocurriría
2	Baja	Ha ocurrido en la industria	Imaginable pero difícilmente ocurriría
3	Moderada	Ha ocurrido en la organización por lo menos una vez	No se espera que ocurra
4	Alta	Ha ocurrido en nuestra organización por lo menos una vez cada 3 meses	Puede ocurrir
5	Muy alta	Ha ocurrido en nuestra organización por lo menos una vez al mes	Va a ocurrir

TABLA 5 Escalas de probabilidad

Fuente propia

Para los casos en que un riesgo no ha ocurrido, se estima la probabilidad frente al descriptor del período, y en los casos en que ha ocurrido se establece con base en la frecuencia y cantidad de los hechos conocidos.

Impacto. Para cada riesgo se debe estimar el impacto de las consecuencias en caso de que ocurriera, considerando las consecuencias establecidas en la etapa de identificación; el nivel de impacto se asigna para cada riesgo utilizando como referencia la siguiente tabla:

FASE 4 – Evaluación del Riesgo **Para cada uno de los riesgos identificados en la primera fase, se debe estimar el nivel de riesgo. Es importante recordar que el nivel de riesgo está asociado a la relación de las consecuencias (impacto) y el factor de ocurrencia (probabilidad),** Para realizar este cálculo, los valores obtenidos a nivel de impacto y probabilidad son representados en la matriz de calor relacionada a continuación, que en conjunto permiten determinar la zona de riesgo.

Con base en esta primera evaluación de la probabilidad y el impacto (de la fase del análisis del riesgo) se determina el **riesgo inherente**, el cual se define como el riesgo intrínseco de una

actividad o un conjunto de ellas, sin considerar el efecto de medidas de tratamiento o controles que permitan llevarlo a los niveles aceptables para el Proveedor de Telecomunicaciones.

NIVEL		IMPACTO		
		SOBRE POBLACIÓN EXPUESTA	ECONOMICO	AMBIENTAL
1	Inferior	Se afecta un minimo de la población expuesta interna .	Requiere la revisión y ajuste de términos contractuales o la alineación de protocolos con el marco normativo interno.	La materialización del riesgo conlleva a una pérdida o sobrecosto menor o igual a *** **SMLV**
2	Menor	Se afecta un minimo de la población expuesta interna y externa .	Glosas por parte de órganos de control interno.	La materialización del riesgo conlleva a una pérdida o sobrecosto entre *** y *** **SMLV**.
3	Importante	Se afecta un 40 % de la población expuesta interna y externa .	Glosas por parte de órganos de control externo (Clientes o Entes Regulatorios).	La materialización del riesgo conlleva a una pérdida o sobrecosto entre *** y *** **SMLV**.
4	Mayor	Se afecta un 60 % de la población expuesta interna y externa .	Implica sanciones de entes regulatorios o la aplicación de cláusulas contractuales o demandas en contra.	La materialización del riesgo conlleva a una pérdida o sobrecosto entre *** y *** **SMLV**
5	Superior	Se afecta un 80 % o mas de la población expuesta interna y externa .	Implica intervención o control de la entidad por parte de los entes regulatorios y de control. Aplicación de sanciones que impactan negocios futuros.	La materialización del riesgo conlleva a una pérdida o sobrecosto mayor a *** **SMLV**, lo cual puede afectar la viabilidad o continuidad del negocio.

Tabla 6 IMPACTO DE DESASTRES FUENTE PROPIA

	IMPACTO				
PROBABILIDAD			**Importante(3)**	**Mayor (4)**	**Superior (5)**
Muy alta (5)			15 (Z. ALTA)	20 (Z. CRÍTICA)	25 (Z. CRÍTICA)
Alta (4)	4(Z. MODERADA)	8 (Z. MODERADA)	12 (Z. ALTA)	15 (Z. ALTA)	20 (Z. CRÍTICA)
Moderada (3)	3 (Z. BAJA)	6 (Z. MODERADA)	9 (Z. ALTA)	12 (Z. ALTA)	15 (Z. ALTA)
Baja (2)	2 (Z. BAJA)	4 (Z. MODERADA)	6 (Z. MODERADA)	8 (Z. MODERADA)	10 (Z. ALTA)
Muy baja (1)	1 (Z. BAJA)	2 (Z. BAJA)	3 (Z. BAJA)	4(Z. MODERADA)	5 (Z. MODERADA)

Tabla No 7 MATRIZ DE CALOR Elaboración propia

ZONA DE RIESGO	
Zona Baja	Riesgos de baja exposición y severidad, para lo cual se recomienda monitoreo permanente.
Zona Moderada	Dada su menor intensidad, se recomienda que estos riesgos sean gestionados en niveles básicos de la Organización, pero con supervisión directa del responsable.
Zona Alta	Riesgos que requieren de controles y alertas permanentes que permitan su gestión constante.
Zona Crítica	Riesgos de alta severidad y exposición, para los cuales se deben implementar sistemas de control para su adecuado tratamiento, los cuales por su importancia y criticidad son de máxima prioridad para la Organización.

TABLA No 8 ZONA DE RIESGO

Análisis de la efectividad de los controles y evaluación de riesgo residual. Para tratar o gestionar los riesgos identificados, se deberán implementar los controles suficientes para disminuir su probabilidad o impacto con base a las siguientes tipologías:

Controles Preventivos: Son controles que actúan sobre las causas del riesgo, con el fin de disminuir la probabilidad de ocurrencia, en general este tipo de controles son considerados como la primera barrera de seguridad que se establece para reducir un riesgo.

Controles Correctivos: Permiten corregir la desviación de los resultados en un proceso y prevenir de nuevo su ocurrencia. Este tipo de control toma las acciones necesarias una vez se ha materializado el riesgo y busca mejorar los demás controles. Con frecuencia corresponden a controles administrativos y son soportados por políticas y procedimientos para su correcto funcionamiento

Calificación del control

¿El control está documentado y se aplica?

PUNTAJE	DESCRIPCION
0	No está documentado ni se aplica
5	Está documentado pero no se aplica
15	No está documentado pero se aplica
20	Está documentado y se aplica

Dispone de monitoreo oportuno que permita identificar Posibles fallas?

PUNTAJE	DESCRIPCION
5	No
20	Si

¿Están definidos los responsables?

PUNTAJE	DESCRIPCIÓN
0	No
20	Si

¿La frecuencia de ejecución del control es adecuada?

PUNTAJE	DESCRIPCION
0	No
20	Si

Posterior al análisis y calificación de los controles, se debe determinar el nivel de incidencia en la mitigación de los riesgos, con base a los rangos definidos en la siguiente tabla:

Nota: Dado el caso que se considere más de un control para la mitigación de un riesgo, la afectación en la probabilidad o impacto del mismo se realizará en función del promedio de los rangos de calificación de cada uno de los controles.

El resultado del riesgo obtenido después de confrontar los controles se denomina, **riesgo residual**.

Dependiendo si el control afecta la probabilidad o el impacto, el (los) riesgos se desplazan en la matriz de calificación		
Rango de calificación en los controles	**Control Preventivo Cuadrantes a disminuir en la probabilidad**	**Control Correctivo Cuadrantes a disminuir en el impacto**
0 – 25	0	0
26 – 50	1	1
51 – 75	2	2
76 - 100	3	3

TABLA 13 RANGO DE CALIFICACIONES EN CONTROLES

FUENTE PROPIA

Se debe tener en cuenta que la calificación obtenida de los controles es una entrada para definir las actividades de los planes de tratamiento.

FASE 5 – Tratamiento de riesgos. Una vez calificados los controles y evaluado su nivel de incidencia en la mitigación de los riesgos, si el riesgo residual se ubica en una zona de riesgo que requiera tratamiento, este se deberá realizar en función de las siguientes opciones:

Los responsables de los riesgos deben formular los planes de implementación o mejora de

controles necesarios para el tratamiento de los riesgos residuales según su zona de criticidad, los cuales deben registrarse en un formato diseñado para tal fin.

OPCIONES DE TRATAMIENTO DE RIESGO	
Evitar el Riesgo	Implica tomar medidas encaminadas a la cancelación de una actividad dentro de un proceso o modificar las condiciones de negocio. (Eliminar la fuente de riesgo).
Reducir el Riesgo	Implica tomar medidas encaminadas a disminuir tanto la probabilidad, como el impacto, a través de la optimización de los procedimientos y la implementación de controles eficientes, eficaces y efectivos.
Compartir o Transferir el Riesgo	Implica reducir su efecto a través del traspaso de posibles impactos a otras organizaciones, como el caso de los seguros o a través de otros medios que permitan distribuir una porción del riesgo con otra entidad.
Asumir el Riesgo	Una vez el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el Comité de Seguridad de la Información o de Riesgos, puede aceptar el riego residual.

TABLA 14 Opciones de tratamiento de riesgo.
FUENTE PROPIA

Nota: El comité de Riesgos deben definir cuáles de estas zonas serán susceptibles de tratamiento y gestión.

TRATAMIENTO DE RIESGOS	
ZONA	**TRATAMIENTO**
Crítica	Riesgo crítico, se requiere atención inmediata de la alta Dirección, se debe reducir, evitar, compartir o transferir.
Alta	Riesgo Alto, es necesario atención de la alta Dirección, se debe reducir, evitar, compartir o transferir.
Moderada	Riesgo Moderado, se debe reducir, evitar, compartir, transferir o asumir, acorde a lo que estipule alta Dirección.
Baja	Riesgo Menor, asumir el riesgo o gestionar mediante procedimientos de rutina, acorde a lo que estipule alta Dirección.

TABLA 15 Opciones de tratamiento de riesgo
FUENTE PROPIA

Cuando el costo de gestionar el riesgo es mayor al beneficio de mitigarlo, el Comité de Riesgos debe evaluar las consecuencias y decidir si acepta o asume el riesgo, para lo cual, se debe elaborar un acta, documentando la aceptación los riesgos identificados y estableciendo un periodo de revisión para evaluar su pertinencia.

Los planes de riesgo definidos deben tener en cuenta la disponibilidad de recursos tecnológicos, humanos y financieros y las acciones a realizar para llevar a cabo su implementación.

En todo caso el Comité de Riesgos deberá conocer los riesgos inherentes y residuales, así como aprobar los correspondientes planes de tratamiento de riesgos.

FASE 6 Monitoreo y seguimiento de los riesgos. El Comité Riesgos hacer control y tomar decisiones respecto a cada uno de los riesgos evaluados con nivel mayor y crítico, para validar la ejecución oportuna y eficacia de las acciones planificadas en los diferentes planes de tratamiento definidos por los responsables de los riesgos.

FASE 7 Comunicación y consulta. Se deben establecer las siguientes acciones para la comunicación de los riesgos a las partes internas y externas involucradas:

Documentación de las matrices consolidadas de riesgos.

Divulgación de las matrices consolidadas de riesgos a los propietarios.

7.1.2. Plan de continuidad de Negocio BCP

El plan de continuidad de negocio debe ser estructurado bajo la norma ISO 22301, tal plan debe ser realizado para sostener en niveles previamente definidos de prestación de servicios críticos del negocio a través de la estructuración de procedimientos, los cuales son desarrollados, compilados y mantenidos en preparación para su uso durante y después de una interrupción o desastre, con el fin de proteger los intereses del proveedor de telecomunicaciones y las partes interesadas, la reputación, las finanzas y los activos críticos.

Previamente se debe identificar los activos críticos ya que ellos son la razón de ser de toda organización productiva. A del plan de continuidad de negocios, el proveedor de telecomunicaciones será capaz de reconocer qué necesita para garantizar la prestación de los servicios, cuidar del talento humano, edificaciones, tecnología, la información, proveedores, partes interesadas y reputación.

Actividades de gestión de continuidad de negocios:

1. Identificar servicios críticos e infraestructura y aplicaciones relacionadas.
2. Priorizar actividades y recursos críticos.
3. Evaluar riesgos asociados a la continuidad de servicios, actividades y recursos críticos.
4. Contar con procedimientos de recuperación
5. Verificar la efectividad de los procedimientos.

Plan complementario al plan de continuidad de negocio: Este plan incluye:

1. Plan de recuperación de desastres DRP

2. Plan de comunicaciones de Crisis
3. Plan de evacuación por estructuras, edificios y zonas aledañas a infraestructura de telecomunicaciones
4. Respuesta a ciber-incidentes.
5. Planes de contingencia.

Plan de comunicación de crisis: este documento debe describir los procedimientos y comunicados al público que el proveedor de telecomunicaciones debe preparar para responder ante un incidente de manera correcta.

Planes de evacuación por edificio e infraestructuras críticas: estos planes, contienen los procedimientos a seguir en o alrededor de una infraestructura crítica, en caso de eventos que puedan oncluir fuego, terremoto, huracán, ataque criminal o una emergencia médica

Plan de respuesta a ciber-incidentes: este plan establece los procedimientos para responder a los ciber- ataques contra los sistemas de información.

Planes de contingencia: Los planes de contingencia representan actividades enfocadas a sostener y a recuperar los servicios críticos de TI después de una emergencia en un tiempo mínimo.

Es posible en algunos casos contar con múltiples planes de contingencia, uno por cada componente, sistema o servicio crítico. Los planes de contingencia son de rápida activación y se puede asumir un RTO o tiempo de recuperación objetivo, muy cercano a cero. Los planes de contingencia son propios de estructuras o equipos que trabajan con equipos espejo o de respaldo.

Realización BIA: Se deben tomar los procesos (relacionados a servicios) críticos para el proveedor de telecomunicaciones y desarrollar un análisis de impacto de los riesgos que afecten la normal prestación de los servicios del proveedor.

Para realizar el análisis de impactos se debe tener e cuenta los siguientes puntos;

Análisis de impactos

- Definir los tipos de impactos
- Identificar las funciones criticas
- Identificar el impacto de cada una de las causas de desastre
- Identificar los recursos necesarios
- Identificar las causas de interrupción como:
    1. Fallos de los sistemas o aplicaciones
    2. Fuego
    3. Software
    4. Inundación
    5. Rayo
    6. Sabotaje
    7. Terrorismo
    8. Ciberataque

Identificar las unidades de negocio, procesos y subprocesos

- Identificar servicios clave a nivel externo e interno
- Identificar las unidades de negocio que son vitales
- Restricciones derivadas de capacidades, mercado y estrategia

- Definir los RTO y RPO de las unidades de negocio
- Clasificarlas según la prioridad del negocio

Estrategias y Alternativas

- Evaluar las necesidades de infraestructura externa
- Alternativas disponibles para las unidades de negocio criticas
- Análisis de procedimientos alternativos o centros alternos con:
    1. Centros espejo
    2. Acuerdos entre organizaciones
    3. Outsourcing

Componentes del Plan

1. Definir los equipos de recuperación
2. Definir los procesos que permiten la vuelta a la normalidad
3. Definir los procesos de logística

Informe BIA El informe debe indicar si se utilizaron cuestionarios con los encargados de los procesos, número de procesos encuestados, fecha y quien lidero el grupo de encuestadores.

Los entregables del BIA son:

1. Resultados de cada unidad o proceso de negocio: en esta parte se describe cada proceso o unidad de negocio, informe de quien realizo las encuestas y además muestra la siguiente información por cada proceso o unidad de negocio:
    a. Proceso de negocio y RTO de forma tabulada por cada subproceso de la unidad de negocio.
    b. Recursos requeridos por cada proceso de negocio, aplicaciones necesarias, equipo, registros vitales o reportes, personas que los requieren.
    c. Procedimientos manuales de recuperación, porcentaje que se puede hacer manualmente y RPO.
    d. Impacto financiero identificado en términos de costo/ ingresos por cada proceso o unidad de negocio calificado como ninguno, bajo, medio, alto.
    e. Impacto operacional (imagen ante el cliente) calificado como ninguno, bajo, medio, alto.
    f. Impacto legal identificado por cada proceso calificado como ninguno, bajo, medio, alto.
    g. Resumen y conclusiones del proceso evaluado: se debe enunciar cual es subproceso más crítico en orden de impactos y sobre todo cuales son los reportes más vulnerables.

Gráficos de Impactos

- Impacto financiero combinado: se debe mostrar día a día la perdida financiera, se debe describir cual es el valor del primer día, la primera semana y el primer mes. Con un resumen que comprenda como ocurren los impactos y desde que proceso, subprocesos o unidades de negocio se originan.
- Impacto operacional combinado: generalmente el impacto operacional es un intangible y tiene que ver con la moral de los empleados, el valor de la acción si se cotiza en la bolsa, el flujo de trabajo y finalmente el servicio al cliente.
- Impacto combinado legal: el impacto legal o de regulación tiene que ver con las unidades de negocio que deben cumplir obligaciones contractuales. Incluye deberes para con las entidades de vigilancia gubernamentales, contratos y niveles de servicio pactados con los clientes, vendedores y agencias.
- Requerimientos de personal para la recuperación
- Complejidad de la recuperación por unidad de negocio o subproceso. cada unidad de negocio o proceso se debe encuestar con el fin de conoces a que rango pertenece según la lista:

a. **Fácilmente recuperable:** los procesos que tenga procedimientos manuales de recuperación, locaciones alternas para poder trabajar, tecnología y estrategias de recuperación.
b. **Razonablemente recuperable:** unidades de negocio que se pueden recuperar con pocos recursos en un tiempo razonable como el recurso humano, la contabilidad.

c. **Difícilmente recuperables:** muchas de las necesidades esenciales de la unidad de negocio puedes ser difíciles de remplazar o recuperar en tiempos razonables, como sistemas de seguridad.

d. **Muy difíciles de recuperar:** normalmente son elementos con una dificultad alta para ser recuperados y con tiempos de recuperación muy largos como lo son laboratorios, desarrollos, planta física.

Propuesta de solución: descripción de recomendaciones y alternativas que permitan la continuidad del negocio

Conclusiones finales: lista de una serie de actividades y sus recursos necesarios.

8. CONCLUSIONES

1. La gestión de Riesgo de desastres DRP es de obligatorio cumplimiento para empresas que prestan servicios públicos.
2. En el presente trabajo se propuso una metodología basada en los trabajos previos en Gestión de Riesgos de desastres propuestas por MINTIC, adicionalmente se propuso una metodología de gestión de riesgos de desastres fundamentada en la NORMA ISO 31000 y una metodología para la realización del plan de continuidad de Negocio basada en ISO 22301.
3. Esta metodología se puede aplicar a otras compañías de proveedores de Telecomunicaciones y prestadores de servicios públicos.
4. El proveedor de telecomunicaciones debería indicar cuales son las sedes críticas según la cantidad de ciudadanos que afecte en caso de desastre, ya sea porque su infraestructura colapse operativamente o porque la infraestuctura ocasione daños sobre un valor de población expuesta, en el que se considere que la amenaza ocasione pérdida de vidas humanas al colapsar.
5. Cada sede del proveedor de telecomunicaciones tiene sus propios riesgos de desastres que son directamente relacionados a las condiciones propias naturales de la zona, para determinar estos riesgos es necesario consultar las bases de datos de riesgos de desastres naturales.

6. Las sedes críticas se deben escoger también en un estudio de interposición de capas de amenazas e infraestructuras, las sedes que estén dentro de las zonas de alta probabilidad de amenaza natural o antrópica deben incluirse dentro de las infraestructuras expuestas que deben entrar en la Gestión de Riesgo de Desastres del proveedor.

7. Dentro de los planes de Organización territorial se encuentran bases de datos de usos permitidos para cada zona y es importante consultar esos usos permitidos y su cumplimiento.

8. Para la realización de esta metodología se debería diseñar un aplicativo para superposición de capas de mapas con coordenadas GPS, en el que estén todas las capas de amenazas, y las áreas de influencia con mayor impacto, áreas de población aglomeradas que reposan en las bases de datos IDEAM, Ingeominas o El instituto Agustin Codazzi, tales capas puedan superponerse con las sedes críticas e infraestructuras críticas operativas de la infraestructura del proveedor, de esta manera, se puede modelar el impacto de la amenaza y definir con claridad las sedes donde se debería invertir en los planes de tratamiento de riesgos por desastre.

9. Las Sedes que defina el operador por Criticas operativamente deberían realizar planes de contingencia Operativa y plan de Continuidad de Negocio de acuerdo a ISO 23001.

BIBLIOGRAFÍA

1. Ley 1523 2012, ideam, recuperado de: http://www.ideam.gov.co/documents/24189/390483/11.+ley+1523+de+2012.pdf/4e93527d-3bb8-4b53-b678-fbde8107d340?version=1.2
2. Decreto 2157 de 2017. Presidencia de la República, recuperado de: http://es.presidencia.gov.co/normativa/normativa/decreto%202157%20del%2020%20de%20diciembre%20de%202017.pdf
3. Análisis del documento estudio de vulnerabilidad y riesgo de las redes e infraestructura de telecomunicaciones en zonas vulnerables expuestas a eventos naturales desastrosos, Mintic, Recuperado de https://colombiatic.mintic.gov.co/679/w3-article-73949.html
4. Análisis del documento diseño de la red nacional de telecomunicaciones de emergencia en Colombia. MINTIC, Recuperado de https://colombiatic.mintic.gov.co/679/w3-article-73949.html
5. https://colombiatic.mintic.gov.co/679/articles-73953_recurso_1.pdf diagnóstico sobre el estado actual del entorno nacional en relación con la prevención y atención de emergencias y desastres y del estado actual de la red nacional de telecomunicaciones de emergencia (RNTE) en Colombia.
6.

7. https://cintel.co/wp-content/uploads/2013/05/23.estudio_sectorial_2006_Estudio-del-Sector-de-la-Telecomunicaciones-en-Colombia-2006.pdf. Estudio de las telecomunicaciones en Colombia. Cintel.

8. https://colombiatic.mintic.gov.co/679/articles-73955_recurso_02.pdf . Diseño de la Red Nacional de Telecomunicaciones de Emergencias y Establecimiento de un Marco Normativo para el Fortalecimiento del Sistema Nacional de Telecomunicaciones de Emergencias en Colombia

ANEXO 1:

TABLAS DE GESTION DE LA INFORMACIÓN DEL RIESGO

1. ESTABLECIMIENTO DEL CONTEXTO				
FECHA DE ELABORACION	Día:	0	Año:	0
PROCESO				
OBJETIVO DEL PROCESO				

FACTORES INTERNOS GENERADORES DE RIESGO			
AMENAZAS SOBRE LA INFRAESTRUCTURA EXPUESTA		VULNERABILIDADES SOBRE LA INFRAESTRUCTURA EXPUESTA	
AI-1		DI-1	

FACTORES EXTERNOS GENERADORES DE RIESGO	
FORTALEZAS	OPORTUNIDADES

AREAS DE AFECTACIÓN PROBABLES Y ELEMENTOS EXPUESTOS DENTRO DEL AREA DE AFECTACION			
CON IMPACTO ALTO		CON IMPACTO MEDIO	
AI-1		DI-1	

FACTORES INTERNOS GENERADORES DE RIESGO			
AMENAZAS SOBRE LA INFRAESTRUCTURA EXPUESTA		VULNERABILIDADES SOBRE LA INFRAESTRUCTURA EXPUESTA	
AI-1		DI-1	

TERCEROS RELACIONADOS CON LAS POSIBLES AMENAZAS			
TERCEROS RELACIONADOS CON AMENAZAS HIDROMETEREOLÓGICAS		TERCEROS RELACIONADOS CON AMENAZAS SISMICAS	
AI-1		DI-1	

TABLA No. 5 ESTABLECIMIENTO DEL CONTEXTO

FUENTE PROPIA

INFORMACIÓN GENERAL DE LA ACTIVIDAD						
NOMBRE INFRAESTRUCTURA						
TIPO DE INFRAESTRUCTURA	OMINISTRATIVA		DE COMUNICACIONES			
CRITICIDAD DE LA INFRAESTRUCTURA	ALTA		MEDIA		BAJA	
ACTIVIDAD PRINCIPAL DE LA INFRAESTRUCTURA QUE PRODUCE RIESGO SOBRE LA SOCIEDAD						
UBICACIÓN						
PRINCIPAL AMENAZA DEL ENTORNO						
LINDEROS	Norte					
	Sur					
	Oriente					
	Occidente					
PROCESOS DE LA INFRAESTRUCTURA						
AREA TOTAL CONSTRUIDA			CUENTA CON CERTIFICADO ANTISISMICO?			
AÑO DE LICENCIA DE CONSTRUCCION						
CUMPLE CON EXIGENCIAS PLAN DE ORGANIZACIÓN TERRITORIAL POT ?						
EQUIPAMIENTO DE EMERGENCIAS EXISTENTE						
TIPO DE POBLACION EXPUESTA AL INTERIOR DE LA INFRAESTRUCTURA			TIPO DE POBLACION EXPUESTA AL EXTERIOR DE LA INFRAESTRUCTURA			

TABLA No. 6 INFORMACION GENERAL DE LA ACTIVIDAD

FUENTE PROPIA

TIPO DE POBLACION EXPUESTA AL INTERIOR DE LA INFRAESTRUCTURA			TIPO DE POBLACION EXPUESTA AL EXTERIOR DE LA INFRAESTRUCTURA			
TIPO DE POBLACION EXPUESTA AL INTERIOR DE LA INFRAESTRUCTURA			TIPO DE POBLACION EXPUESTA AL EXTERIOR DE LA INFRAESTRUCTURA			
Gas Domiciliario						
Ascensores						
Subestación eléctrica						
Número Pisos						
Shut Basuras						
Cafeterías						

VULNERABILIDAD SOCIAL						
AREAS AFECTADAS POR EVENTUAL DESASTRE						
NUMERO DE HABITANTES AFECTADOS AMENAZA HIDROMETEREOLÓGICA						
NUMERO DE HABITANTES AFECTADOS AMENAZA VOLCANICA						
NUMERO DE HABITANTES AFECTADOS POR SISMO						

TABLA No. 6A INFORMACION GENERAL DE LA ACTIVIDAD

FUENTE PROPIA

SISTEMA DE ALIMENTACIÓN ELECTRICA			
Generador Eléctrico		Ubicación Generador	
KwA / Hr		Marca	
Tanque Combustible (Capacidad en Galones)		Ubicación Tanque	
Tiene Dique Contención		Polo a Tierra	
Banco Baterías		Ubicación	
Tipo Baterías		Kit de Derrames	

PRODUCTOS QUIMICOS EN LA SEDE	Nombre		Cantidad	
	Nombre		Cantidad	
	Nombre		Cantidad	
	Nombre		Cantidad	
	Nombre		Cantidad	
	Nombre		Cantidad	
	Nombre		Cantidad	
EMERGENCIAS OCURRIDAS EN LOS ULTIMOS AÑOS			Perdidas	
			Perdidas	
			Perdidas	
			Perdidas	
			Perdidas	
			Perdidas	
			Perdidas	

TABLA No. 6B INFORMACION GENERAL DE LA ACTIVIDAD

FUENTE PROPIA

CONTEXTO EXTERNO		
Descripción del entorno (Condiciones biofísicas y de localización)		
Infraestructura que pueda generar Amenazas o contribuir con el desarrollo de una emergencia o Desastre (Dominó)		
PLAN DE ORDENACION Y MANEJO DE CUENCAS HIDROGRÁFICAS POMCA		
PLANES DE ORDENACIÓN Y MANEJO DE UNIDADES AMBIENTAES COSTERAS POMIUAC		
PLANES DE ORDENACIÓN Y MANEJO DE UNIDADES AMBIENTAES COSTERAS POMIUAC		

TABLA No. 6C INFORMACION GENERAL DE LA ACTIVIDAD

FUENTE PROPIA

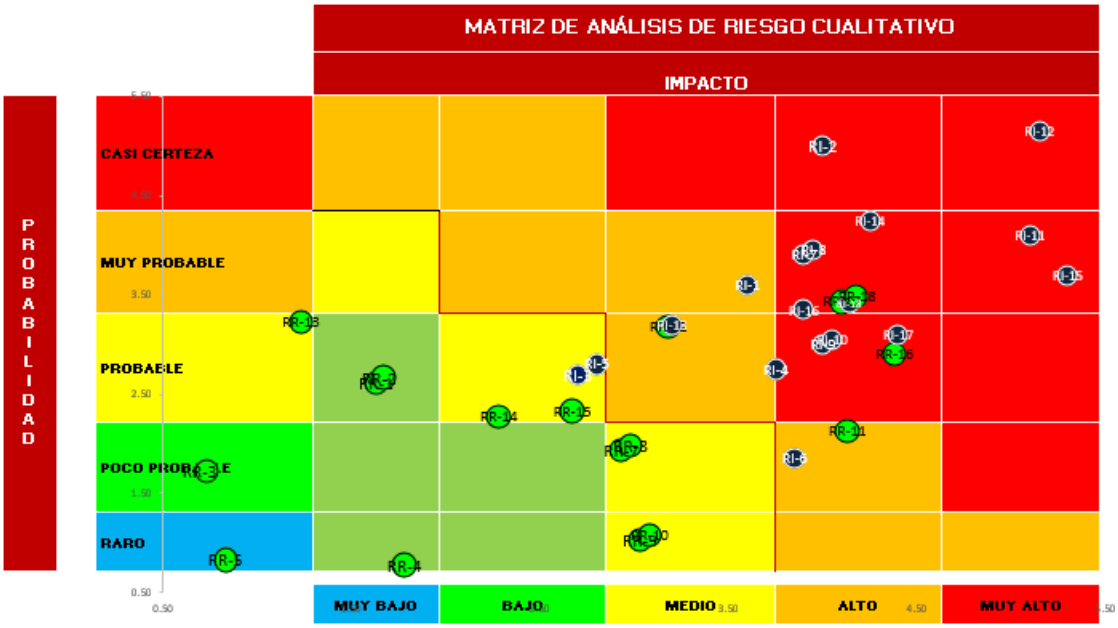


TABLA No. 6D MATRIZ ANÁLISIS RIESGO CUALITATIVO

FUENTE PROPIA

					FACTORES DE VULNERABILIDAD				AMENAZAS		
N°	CATEGORIA DEL RIESGO	AMENAZA	VULNERABILIDAD	METAS ESTRATÉGICAS	Recurso Humano	Procesos	Tecnología	Infraestructura Física	Deliberadas	Accidentales	Del entorno y/o equipos
RDC-1	De Desastre	Sismo	Ubicación en zona catalogada de alta sismicidad con una probabilidad de ocurrencia alta.	Rentabilidad	x	x	x	x			Externa
RDC-2	De Desastre	Inundaciones	Cambios meteorologicos que puedan ocasionar lluvias torrenciales causando inundaciones en el datacenter	Rentabilidad	x	x	x	x			Externa
RDC-3	De Desastre	Derrames	Fugas por falta o inadecuado mantenimiento	Rentabilidad	x	x	x	x			Externa
RDC-4	De Desastre	Incendios	Sobrecargas o cortos circuitos	Rentabilidad	x	x	x	x			Externa
RDC-5	De Desastre	Incendios	Generación y acumulación de residuos	Rentabilidad	x	x	x	x			Externa
RDC-6	De Desastre	Incendios	Manejos inadecuados de derrames de combustibles (ACPM)	Rentabilidad	x	x	x	x			Externa
RDC-7	De Desastre	Descargas Electricas	Ubicación en zonas de riesgo medio de niveles ceraunicos (Descargas electricas)	Rentabilidad	x	x	x	x			Externa
RI-8	De Desastre	Derrames	Fallas en la manipulación, transporte o almacenamiento de combustibles	Rentabilidad	x	x	x	x			Externa

TABLA No. 7 IDENTIFICACIÓN DEL RIESGO FUENTE PROPIA

5. TRATAMIENTO DEL RIESGO													
	NOMBRE DEL RIESGO	ZONA DE RIESGO INHERENTE	ZONA DE RIESGO RESIDUAL	OPCIONES DE MANEJO (1)				PLAN DE MANEJO DEL RIESGO					
								CONTROL PROPUESTO O ACCIONES A TOMAR	TIPO DE CONTROL		RESPONSABLE	CRONOGRAMA IMPLEMENTACIÓN	
				EVT	RE	TR	AS		P	C	CARGO	INICIA	TERMINA
R-1	Riesgo De Desastre : por Sismo Debido a Ubicaciòn en zona catalogada de alta sismicidad con una probabilidad de ocurrencia alta.	4-Extrema	2-Moderada										
R-2	Riesgo De Desastre : por Inundaciones Debido a Cambios meteorologicos que puedan ocasionar lluvias torrenciales causando inundaciones en el datacenter	4-Extrema	2-Moderada										
R-3	Riesgo De Desastre : por Derrames Debido a Fugas por falta o inadecuado mantenimiento	3-Alta	1-Baja										
R-4	Riesgo De Desastre : por Incendios Debido a Sobrecargas o cortos circuitos	4-Extrema	1-Baja										
R-5	Riesgo De Desastre : por Incendios Debido a Generaciòn y acumulaciòn de residuos	3-Alta	1-Baja										

TABLA No. 8 IDENTIFICACIÓN DEL RIESGO
FUENTE PROPIA

	NOMBRE DEL RIESGO	Probabilidad	Impacto	Valoración del Riesgo	CONTROLES EXISTENTES					EVALUACIÓN DE CONTROLES											
										PROBABILIDAD						IMPACTO					
					DESCRIPCIÓN	EVIDENCIA	FRECUENCIA	RESPONSABLE DE SU EJECUCIÓN	TIPO (C.D.P)	HC	MP	HE	EC	FE	TOTAL PROBABILIDAD	HC	MP	HE	EC	FE	TOTAL IMPACTO
R-1	Riesgo De Desastre : por Sismo Debido a Ubicación en zona catalogada de alta sismicidad con una probabilidad de ocurrencia alta.	Muy Probable	Alto	4-Extrema	Sede construida con máxima tolerancia ante fallas antisísmicas certificada por International Computer Room Experts Association (ICREA) Nivel 5	Certificado ICREA	Por demanda		Preventivo			30	15	25	70	15	15	30	15	25	100
R-2	Riesgo De Desastre : por Inundaciones Debido a Cambios meteorologicos que puedan ocasionar lluvias torrenciales causando inundaciones en el datacenter	Casi Certeza	Alto	4-Extrema	Se cuenta con techo a dos aguas y canaletas de acuerdo a normas internacionales y mantenimientos preventivos	Mantenimientos preventivos	Permanente		Preventivo	15	15	30	15	25	100	15	15	30	15	25	100
R-3	Riesgo De Desastre : por Derrames Debido a Fugas por falta o inadecuado mantenimiento	Probable	Medio	3-Alta	Tanques con valvulas de control certificadas, procedimientos seguros y certificados por fabricante	Mantenimientos preventivos	Semestral		Preventivo	15	15	30	15	25	100	15	15	30	15	25	100
R-4	Riesgo De Desastre : por Incendios Debido a Sobrecargas o cortos circuitos	Probable	Alto	4-Extrema	Tomas de corriente reguladas, existencia de brakers, canaletas	Mantenimientos, capacitaciones.	Permanente		Preventivo	15	15	30	15	25	100	15	15	30	15	25	100
					Capacitacion										0						0
					Cableado estructural										0						0
R-5	Riesgo De Desastre : por Incendios Debido a Generación y acumulación de residuos	Probable	Medio	3-Alta	Existencia de Progerama RESPEL	De recorrido	Permanente		Preventivo	15	15	30	15	25	100	15	15	30	15	25	100
					Frecuente reolección de basuras	De recorrido									0						0
					Capacitación a empleados sobre	Actas y de recorrido									0						0
															0						0
															0						0

TABLA No. 9 IDENTIFICACIÓN DEL RIESGO. FUENTE PROPIA