TESIS DE LA UNIVERSIDAD DE ZARAGOZA

2012

41

Gabriel Jaime Correa Henao

Identificación y evaluación de amenazas a la seguridad de infraestructuras de transporte y distribución de electricidad

Departamento

Instituto Universitario de Investigación Mixto CIRCE

Director/es

Yusta Loyo, Jose María

ISSN 2254-7606

Prensas de la Universidad Universidad Zaragoza

Universidad Zaragoza
1542

Tesis Doctoral

IDENTIFICACIÓN Y EVALUACIÓN DE AMENAZAS A LA SEGURIDAD DE INFRAESTRUCTURAS DE TRANSPORTE Y DISTRIBUCIÓN DE ELECTRICIDAD

Autor

Gabriel Jaime Correa Henao

Director/es

Yusta Loyo, Jose María

UNIVERSIDAD DE ZARAGOZA

Instituto Universitario de Investigación Mixto CIRCE

2012

Universidad Zaragoza
1542

Instituto Universitario de Investigación Mixto
circe
UniversidadZaragoza

TESIS DOCTORAL

IDENTIFICACIÓN Y EVALUACIÓN DE AMENAZAS A LA SEGURIDAD DE INFRAESTRUCTURAS DE TRANSPORTE Y DISTRIBUCIÓN DE ELECTRICIDAD

Autor:
Gabriel Jaime Correa Henao

Director:
José María Yusta Loyo, PhD

ZARAGOZA, ESPAÑA

JUNIO, 2012

Las naciones marchan hacia su grandeza al
mismo paso que avanza su educación
Simón Bolivar

A mi novia, Any,
Por su manifestación de amor, paciencia, apoyo, comprensión y orientación

A mi madre y a mis hermanos,
Porque me han servido de guía y de soporte en esta etapa de mi vida

GABRIEL JAIME CORREA HENAO

IDENTIFICACIÓN Y EVALUACIÓN DE AMENAZAS A LA SEGURIDAD DE INFRAESTRUCTURAS DE TRANSPORTE Y DISTRIBUCIÓN DE ELECTRICIDAD

Tesis doctoral presentada en el Programa de Doctorado en Energías Renovables y Eficiencia Energética, Instituto Universitario de Investigación Mixto CIRCE - Universidad de Zaragoza, como requisito para la obtención del título de Doctor por la Universidad de Zaragoza

Director de Tesis: José María Yusta Loyo, PhD

Zaragoza, España

Junio, 2012

IDENTIFICACIÓN Y EVALUACIÓN DE AMENAZAS A LA SEGURIDAD DE INFRAESTRUCTURAS DE TRANSPORTE Y DISTRIBUCIÓN DE ELECTRICIDAD

Tabla de Contenido

IDENTIFICACIÓN Y EVALUACIÓN DE AMENAZAS A LA SEGURIDAD DE INFRAESTRUCTURAS DE TRANSPORTE Y DISTRIBUCIÓN DE ELECTRICIDAD

Listado de Figuras

IDENTIFICACIÓN Y EVALUACIÓN DE AMENAZAS A LA SEGURIDAD DE INFRAESTRUCTURAS DE TRANSPORTE Y DISTRIBUCIÓN DE ELECTRICIDAD

Listado de Tablas

I. AGRADECIMIENTOS

El listado de personas y organizaciones que me han ayudado a la realización de esta tesis es considerable, y debo emitir mis disculpas en caso que no mencione a alguien, especialmente a toda esa gente maravillosa que haya influido y dado forma a mi visión y a mis ideas en los últimos años. Sin embargo, hay quienes deben ser reconocidos por su ayuda para esta investigación y tesis.

En primer lugar, tengo el inmenso privilegio de agradecer a Dios, que me ha concedido salud, motivación y bendición en el recorrido de este camino, una de las etapas más importantes de mi vida.

El desarrollo de esta tesis doctoral no hubiera sido posible sin la financiación otorgada en Colombia, tanto por parte de la Fundación *Colfuturo*, como por la Alcaldía de Medellín, a través del programa *Enlazamundos*. A ambas instituciones manifiesto mi profundo agradecimiento por el patrocinio que me otorgaron en estos años de estudios.

Mis agradecimientos a España, país que me acogió muy bien con excelente calidad de vida, y que llevaré siempre presente en mi memoria. Así mismo, a todas las personas con las que aquí me he relacionado, en la ciudad de Zaragoza, y que ciertamente puedo considerarlos como excelentes amigos de tantas nacionalidades: españoles, latinos, africanos y europeos.

Aprovecho esta oportunidad para agradecer a mi director, José María Yusta Loyo, por convertirse en guía y apoyo durante mis estudios de doctorado. Él me extendió su mano en un momento crucial del programa de doctorado que nunca voy a olvidar. Su guía ha significado una gran fuente de conocimiento e inspiración. Gracias a su orientación, ha sido posible materializar el desarrollo de esta tesis doctoral, así como los aportes científicos que de ella se derivan.

Quiero agradecer al Centro de Investigación de Recursos y Consumos Energéticos (CIRCE), a su director, Antonio Valero Capilla, y empleados de la

Fundación. A través del CIRCE desarrollé gran parte de mi formación por medio de sus programas oficiales de máster y doctorado. Mi reconocimiento al Departamento de Ingeniería Eléctrica, representado por su director, José Antonio Domínguez Navarro, por su dinamismo y excelencia, les agradezco la orientación y la dedicación profesional.

Una gran inspiración me la ha brindado mi novia, Ana Isabel Soto Parra; su amor, paciencia, comprensión y apoyo me han sostenido a lo largo de estos años de estudios en el programa de doctorado. También quiero agradecer a mi madre, Magdalena, por su constante aliento y buenos deseos, quien influyó en mi vida de manera significativa. También agradezco a mis hermanos, Diana Cristina y Jorge Mario, quienes me brindaron toda su orientación y consuelo para compartir mis penas y alegrías de todos los momentos de mi investigación.

Sin duda, la asesoría y consejos académicos de Beatriz López Valencia (*ISA*, Colombia), Roberto Lacal Arántegui (*JCR*, *Institute for Energy – Comisión Europea*) y todas aquellas personas que hemos contactado a lo largo de la investigación, han sido fundamentales para definir los aportes científicos y los resultados de esta tesis.

También agradezco a todos mis colegas, de los distintos países, que aquí compartieron conmigo los logros, así como los momentos difíciles en el transcurso del doctorado: Alberto, Carmen, Nourou, Atencio, Abebe, Ponce, Hans, Lujano, Eva, Juan Daniel, Juan Carlos, John Fabián y en general, a todas aquellas personas que con su amistad y compañerismo han facilitado mi estadía en España.

A todas aquellas personas e instituciones que me han servido de apoyo, y que no he alcanzado a mencionar en estos renglones, mis mayores agradecimientos por haber creído en mí, por su paciencia y por sus valiosos aportes y orientaciones.

II. RESUMEN

El tema de aseguramiento del suministro energético, especialmente en lo concerniente a la protección de las infraestructuras energéticas, ha suscitado especial interés en los países de la OCDE en los últimos años. Al respecto, el Consejo de la Unión Europea ha aprobado la Directiva 2008/114/CE (sobre la identificación y designación de infraestructuras críticas europeas) y el Departamento de Seguridad Nacional de EE.UU ha publicado el NIPP en 2009 (National Infrastructure Protection Plan). Dichos planes contemplan el establecimiento de procedimientos para la protección y seguridad de las infraestructuras críticas, en el marco de estrategias de gestión de riesgos.

A partir de los conceptos establecidos en ambos programas, en esta tesis se presentan propuestas metodológicas aplicables a la identificación de riesgos y a la evaluación de amenazas en la red de infraestructura eléctrica. Se propone el uso de *mapas interconectados de riesgos*, complementados con la determinación de componentes de riesgo en el sistema de infraestructura. Así mismo, se propone el uso de las *cartas de riesgos*, mediante las cuales se obtiene una representación gráfica e intuitiva de la evaluación semicuantitativa de los riesgos más relevantes.

Por otro lado, se formulan y validan estrategias metodológicas para la evaluación de la vulnerabilidad estructural en redes de transporte de alta tensión, a partir de la combinación de modelos de flujos de carga y medidas de grafos de libre-escala. De esta manera, es posible estudiar los escenarios de riesgos en función de los eventos que pueden desencadenar fallos en cascada dentro de un sistema eléctrico de potencia. Se demuestra la utilidad de las técnicas de teoría de grafos para analizar las respuestas de los sistemas eléctricos de potencia y evaluar la vulnerabilidad de las redes de transporte. Un ejemplo de dicha evaluación se desarrolla mediante valoración de la tolerancia de redes de prueba IEEE contra fallos aleatorios y contra ataques deliberados. Adicionalmente, se ha realizado una

aplicación de la propuesta metodológica para evaluación de vulnerabilidad en los sistemas eléctricos de alta tensión en Colombia y España.

Como resultado, los trabajos desarrollados en la tesis aportan nuevos instrumentos para la gestión de riesgos en infraestructuras eléctricas, en particular en redes de transporte en alta tensión.

III. ABSTRACT

The issue of securing energy supply, especially concerning the protection of critical energy infrastructures, has attracted particular attention in OECD countries during the last few years. In this regard, the European Council has issued the EU Directive 2008/114/EC (On the identification and designation of European critical infrastructures) and the U.S. Department of Homeland Security has issued the NIPP (National Infrastructure Protection Plan) in 2009. These plans include the establishment of the required steps within a risk management framework, in order to protect and secure critical infrastructures.

Based upon the definitions established in both programs, this thesis seeks to develop several methodological proposals applicable to both risk identification and threat assessment in electric infrastructures. One of the proposals concerns to the use of *interconnected risk maps* that are supplemented with the estimation of risk components in the infrastructure system. Furthermore, the application of *risk charts* is propositioned as a technique that leads the establishment of a more intuitive graphical representation of the most significant risks affecting the infrastructure system, based upon semi-quantitative assessment.

Additionally, some methodological strategies are formulated and validated in order to perform structural vulnerability assessment in high voltage transmission networks combining power flow models and scale-free graph measures. Thus, it is possible to study risk scenarios based on events that can trigger cascade failures in electric power systems. Moreover, a demonstration of the usefulness of graph theory methods is performed in order to analyze technical responses as well as vulnerability assessment in transmission networks. An example of such evaluation is exploited through tolerance assessment on IEEE testing networks to both random errors and deliberate attacks. Furthermore, the methodological approach has been applied in order to assess vulnerability within high voltage electric power systems in Colombia and Spain.

The results of this thesis seek to contribute new methodological tools in order to perform risk management in electric infrastructures, particularly within high voltage transmission networks.

1 INTRODUCCIÓN

En este capítulo se presenta el tema de la investigación, justificado por la preocupación creciente en los últimos años sobre la seguridad de las infraestructuras críticas, en especial, las redes eléctricas. Se pone en valor la necesidad de involucrar los componentes de las infraestructuras en un marco de gestión de riesgos, a partir de los procedimientos de identificación y evaluación, que a su vez conduzcan al análisis de vulnerabilidad de dichos sistemas. Se establecen los objetivos de la investigación, la relevancia de las aportaciones realizadas y la estructura del trabajo planificado en la tesis doctoral.

1.1 JUSTIFICACIÓN Y MOTIVACIÓN

La problemática de la seguridad energética constituye en la actualidad uno de los temas centrales mundiales que afectan de forma esencial a las economías y las políticas de seguridad en todos los Estados. Dentro de este contexto, se hace evidente la estrecha relación entre la seguridad global de las infraestructuras energéticas con los otros sectores de la economía y de éstos con la sociedad de un país. A su vez, las metas de sostenibilidad energética, los objetivos económicos, los planes de desarrollo y bienestar social en todos los países forman parte del entorno de interdependencia entre los países y sus infraestructuras críticas.

Precisamente el interés estratégico asociado a la seguridad de las infraestructuras energética de las naciones, específicamente en el sector de transporte de energía eléctrica, ha constituido la motivación para abordar este trabajo de investigación. Los procesos de consulta y exploración de referencias bibliográficas que permitieron definir el tema de investigación, han dejado en evidencia la existencia de un área de pendiente por explorar y desarrollar, consistente en la aplicación de metodologías, técnicas y herramientas cuantitativas que permitan evaluar la vulnerabilidad de las infraestructuras de energía eléctrica.

Por tal razón, esta investigación involucra la concepción de una propuesta metodológica para la identificación y evaluación de riesgos en el ámbito de la infraestructura del suministro energético, así como el desarrollo de una metodología para la valoración de vulnerabilidad estructural en redes de transporte de energía eléctrica de alta tensión.

1.2 PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS (PIC)

La infraestructura crítica se describe por parte de muchos gobiernos como el conjunto de activos que son esenciales para el funcionamiento de una sociedad y de su economía. En años recientes, tanto la *Comisión Europea* (CE), el Departamento de Seguridad Nacional de los EEUU, y muchas otras entidades gubernamentales en varios países del mundo, han liderado la puesta en marcha de *programas de protección de infraestructura crítica*, como mecanismo de aseguramiento del suministro energético y de su defensa nacional. En el año 2008 el Consejo de la Unión Europea adoptó la Directiva 114/08/CE [CUE, 2008], que dio origen al *Programa Europeo de Protección de Infraestructura Crítica* (PEPIC). En el 2009 fue publicado el *Plan de Protección de Infraestructura Crítica de los EEUU* [NIPP, 2009].

En general, estos programas pueden asociarse a estrategias de gestión de riesgos que incluyen seis etapas: definición de los objetivos de seguridad, identificación de recursos y de riesgos, evaluación de riesgos, priorización de acciones para mitigación de riesgos, implementación de programas de mejora y medición de su efectividad, como puede apreciarse en la Figura 1.1. En el caso particular de España, mediante la Ley 8/2011 [BOE, 2011a] se legisla el cumplimiento de la Directiva 2008/114/CE y se delega en el *Centro Nacional para la Protección de las Infraestructuras Críticas* (CNPIC) la coordinación y supervisión de los planes y agentes involucrados en la protección de las infraestructuras críticas nacionales y transnacionales.

Estos programas proporcionan a los gobiernos y al sector privado la oportunidad de definir más claramente los sistemas de alertas en infraestructuras energéticas críticas, sus recursos claves, su protección, su planificación para garantizar la continuidad y fiabilidad de dichas infraestructuras. También se desarrollan los procesos de mejora continua y retroalimentación, en un marco flexible y adaptable al panorama de riesgos de cada sector. En ese sentido, las experiencias de algunos países que se consideran como referentes internacionales, han definido las estrategias metodológicas para implementar los programas de *protección de infraestructura crítica* (PIC), de acuerdo con la funcionalidad de las mismas, siempre en el marco de las metodologías organizacionales para la gestión de riesgos.

Para el interés de esta investigación, se procura hacer énfasis en las primeras etapas requeridas por el programa NIPP, según se ilustra en la Figura 1.1. El enfoque que se describe en la presente tesis tiene que ver con los procesos de *definición*, *identificación* y *evaluación* de riesgos en los sistemas de infraestructuras críticas, los cuales se desarrollan en los capítulos 3 y 4.

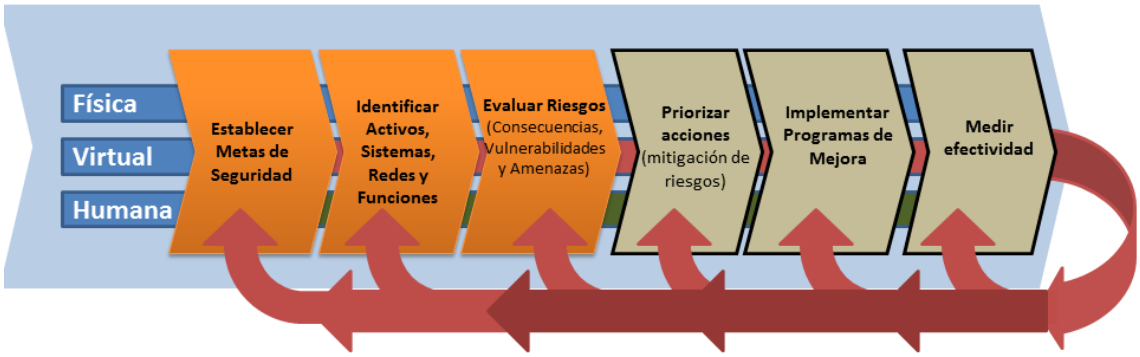


Figura 1.1: Marco de gestión de riesgos con énfasis en las etapas objeto de la investigación

En todos los casos, los sistemas eléctricos de potencia siempre están considerados dentro de los grupos de infraestructuras críticas más importantes por su relación con los asuntos sociales, económicos y militares dentro de un país. Se evidencia la necesidad de incorporar la cuantificación de las amenazas dentro de las etapas de identificación y evaluación, como requisito en la administración de aquellos riesgos que impactan las operaciones de estas infraestructuras, los cuales pueden variar desde las perturbaciones ocasionadas por fallos técnicos en los activos, los fenómenos naturales, las condiciones meteorológicas, hasta los sabotajes y los actos de terrorismo.

Esta línea de investigación ha despertado un notable interés por parte de instituciones públicas y privadas en todo el mundo, especialmente por la necesidad de aplicar los descubrimientos académicos en la formulación de políticas para los programas de PIC. Una revisión completa de las actuales metodologías, modelos y aplicaciones de simulación en torno a la protección de infraestructuras eléctricas, como la que se presentan en el capítulo 2 de esta tesis, revela la existencia de líneas de investigación que tienen en cuenta la descripción del estado del sistema (diagramas, matrices de valoración, bases de datos, etc), así como el desarrollo de modelos de simulación para estudiar el comportamiento dinámico de las redes de infraestructura (técnicas Montecarlo, dinámica de sistemas, multiagentes, teoría de grafos, etc).

Usualmente la valoración de la vulnerabilidad de la red de transporte en alta tensión (tanto a nivel local, como nacional) está supeditada al interés de las organizaciones propietarias y operadoras del sistema de infraestructura. La mayor parte de los estudios de vulnerabilidad suelen desarrollarse después de la ocurrencia de eventos de alto impacto (por ejemplo, un *blackout* o apagón con gran alcance geográfico), con la finalidad de determinar las causas que generan los eventos de fallos en cascada en un sistema de potencia específico. Estos estudios se desarrollan mediante análisis estructural de vulnerabilidad en redes de transporte, los cuales requieren metodologías bien definidas que permitan guiar la toma de decisiones en acciones de prevención y recuperación de la normalidad en la red. Por ejemplo, a través de estudios de contingencias N-1 y N-*t* que están considerados entre los criterios más aceptados por la industria eléctrica.

Como alternativa a las herramientas clásicas de análisis de contingencias, se presentan en los capítulos 5 y 6 las técnicas de teoría de grafos y redes complejas, que en los últimos años se han propuesto como métodos útiles en el análisis del comportamiento físico de las redes de potencia, especialmente su respuesta ante

fallos en cascada. Esto permite realizar una valoración de la vulnerabilidad del sistema, así como estudiar su comportamiento ante riesgos de tipo aleatorio o ante ataques deliberados.

La utilidad práctica de las técnicas de teoría de grafos en redes eléctricas es un tema que todavía está sujeto al desarrollo de más investigaciones y aplicaciones. Permiten evaluar la vulnerabilidad de redes, sin la necesidad de utilizar parámetros eléctricos. Los resultados obtenidos en esta investigación permiten concluir que el uso de las redes complejas, cuando se utilizan los parámetros adecuados, puede ser apropiado para el análisis de contingencias.

1.3 OBJETIVOS DE LA INVESTIGACIÓN

Con la realización de esta investigación se procura contribuir a los procesos de planificación de estrategias para garantizar la seguridad y protección del sistema de infraestructura crítica. Estos desafíos surgen de un conjunto de acontecimientos internos y externos de origen técnico, geopolítico y económico en torno al sistema de infraestructura.

Los objetivos propuestos pretenden cubrir las etapas de identificación y evaluación de riesgos en el sistema de suministro energético en un país, específicamente, la red de transporte de electricidad en alta tensión. Bajo estos argumentos, en este trabajo de investigación se definen los siguientes objetivos:

1. Proponer y validar una aproximación metodológica para la identificación de riesgos en redes de infraestructura energética.
2. Realizar una aproximación metodológica para la valoración de riesgos que permita planificar la seguridad de las infraestructuras frente a amenazas técnicas y no técnicas.
3. Realizar la identificación, análisis y evaluación de los riesgos de la infraestructura del suministro energético en un país, como aplicación.
4. Investigar la efectividad de las metodologías de redes complejas para evaluar la vulnerabilidad estructural de los sistemas eléctricos de potencia, mediante la comparación de los índices obtenidos a través de los flujos de carga, con las medidas estadísticas alternativas proporcionadas por la teoría de grafos.
5. Aplicar la metodología propuesta de evaluación de vulnerabilidad mediante redes complejas sobre redes de transporte en alta tensión en Colombia y España,

considerando los planes orientativos de expansión de las redes eléctricas expedidos por los respectivos gobiernos.

1.4 RELEVANCIA Y APORTES DE LA INVESTIGACIÓN

En la investigación se analiza, desde una perspectiva global, el tratamiento de riesgos y amenazas al sistema de infraestructura eléctrica, de conformidad con el marco sugerido en los programas de protección de infraestructura crítica, con especial utilidad para las empresas propietarias y operadoras de la red de transporte de alta tensión. Este tratamiento incluye la implementación de metodologías de *mapas interconectados de riesgos*, cuyos esquemas permiten identificar los panoramas de riesgos en el sistema. El proceso de calificación de riesgos se efectúa mediante la generación de *cartas de riesgos*, para determinar aquellos riesgos y amenazas más críticas e importantes.

Adicionalmente, el desarrollo de la propuesta metodológica para evaluación estructural de la vulnerabilidad de las redes eléctricas constituye una técnica eficiente y sencilla comparada con las herramientas clásicas de análisis de contingencias. La aplicación de esta técnica permite valorar la efectividad de los planes orientativos de expansión de la red, en la medida que se evalúa la respuesta de la red ante posibles fallos en cascada.

Los trabajos y resultados de la tesis han sido compartidos mediante entrevistas y contactos con el Centro Nacional de Infraestructuras Críticas del Ministerio del Interior español, con la empresa Red Eléctrica de España, con la Comisión Europea, con la empresa ISA operadora de redes de alta tensión en Colombia y con otras organizaciones.

Se ha realizado un esfuerzo para difundir las principales propuestas y aportaciones de esta tesis doctoral. A la fecha de entrega de esta tesis, algunos artículos han sido aceptados para publicación en revistas, en tanto que otros aún se encuentran en proceso de revisión, según se mencionan a continuación:

YUSTA, José María, CORREA, Gabriel Jaime, LACAL-ARÁNTEGUI Roberto. (2011). "*Methodologies and applications for critical infrastructure protection: State-of-the-art*". En: Energy Policy. Vol. 39. N° 10. pp 6100-6119. Ed. Elsevier (ISSN 0301-4215). Estado: PUBLICADO

YUSTA LOYO, José María, CORREA HENAO, Gabriel Jaime (2012). "*Seguridad energética y protección de infraestructuras críticas*". En: Inteligencia y seguridad. Revista de análisis y prospectiva. Ed. Plaza y Valdés (ISSN 1887-293X-n6). Estado: EN PROCESO DE REVISIÓN (fecha envío: 4 Febrero 2012)

CORREA, Gabriel Jaime, YUSTA, José María, LACAL-ARÁNTEGUI Roberto. (2012). "*Interconnected risk maps for threat assessment in electric critical infrastructure*". En: International Journal of Critical Infrastructure Protection. Ed. Elsevier (ISSN 1874-5482). Estado: EN PROCESO DE REVISIÓN (fecha envío: 14 Diciembre 2011)

CORREA, Gabriel J., YUSTA, José M. (2012). "*Grid Vulnerability Analysis Based on Scale-Free Graphs versus Power Flow Models*". En: Electric Power Systems Research. Ed. Elsevier. (ISSN 0378-7796). Estado: EN PROCESO DE REVISIÓN. (fecha envío: 8 Junio 2012)

Entre otros, se destacan los siguientes aportes de la tesis doctoral:

- Definición del problema de Protección de Infraestructura Crítica como tema de investigación académica, generando resultados en aspectos como: estado del arte, integración de riesgos, análisis de vulnerabilidad, redes de apoyo académico con otras instituciones y empresas.
- Para la etapa de identificación se ha desarrollado la propuesta metodológica de *mapas interconectados de riesgos*, que permiten obtener una visión general del estado del sistema. Estos se complementan con una base de componentes de riesgo.
- Se ha desarrollado la metodología de *cartas de riesgos* para la evaluación semicuantitativa de las amenazas y riesgos que afectan a las infraestructuras técnicas, el cual depende de las componentes de riesgo del sistema y de los recursos organizacionales sobre los cuales se realiza la evaluación.
- Se ha demostrado la utilidad de combinar modelos de flujos de carga y mediciones estadísticas de los grafos de libre escala. Estos últimos, corresponden a herramientas computacionales más rápidas para evaluar la vulnerabilidad estructural de cualquier red eléctrica, en función de los eventos que desencadenan fallos en cascada.
- Se ha validado la propuesta metodológica en sistemas eléctricos de potencias, en los que sólo se requiere conocer la topología de las redes de transporte en alta tensión, para cuantificar la vulnerabilidad del sistema.
- Se han efectuado ejemplos de aplicación de la propuesta metodológica mediante la evaluación de vulnerabilidad en sistemas de infraestructura energética de países como Colombia y España.
- Como resultados complementarios, se exponen aspectos en la priorización de acciones y toma de decisiones para la prevención y mitigación de riesgos del suministro energético.

La investigación también puede considerarse, desde el punto de vista conceptual, como una guía para facilitar la evaluación de la vulnerabilidad de las infraestructuras técnicas, tomando el ejemplo de los casos de estudio.

1.5 ESTRUCTURACIÓN DEL TRABAJO DE TESIS

A partir de los objetivos expuestos previamente en la sección 1.3, se construyen los argumentos que conducen el trabajo de investigación. La tesis se apoya en las teorías existentes alrededor de las estrategias de gestión de riesgos, tomando las directrices inicialmente establecidas en [NIPP, 2009], haciendo especial énfasis en las etapas de identificación y evaluación de riesgos y combinando técnicas de análisis entre redes complejas y herramientas de ingeniería eléctrica.

La tesis se compone de seis capítulos y tres anexos. Claramente se distinguen dos secciones. La primera parte está conformada por los capítulos 2, 3 y 4. En esta primera sección se aborda el problema de identificación y evaluación de riesgos mediante metodologías cualitativas y semicuantitativas. Los anexos A y B constituyen un complemento de estos capítulos.

Esta primera parte también contiene una descripción detallada sobre el estado del arte, en los temas de PIC, así como la identificación, evaluación de riesgos, programas de protección de infraestructura, políticas, regulaciones y estándares de gestión de riesgos. Esta parte del trabajo de investigación está soportada en una exhaustiva revisión bibliográfica.

Por su parte, los capítulos 5 y 6 presentan una estrategia de evaluación de la vulnerabilidad estructural en las redes eléctricas de transporte. El anexo C constituye un complemento y contiene la descripción de la metodología para futuras líneas de investigación que requieran la identificación de los activos más críticos en la infraestructura.

Idealmente, el documento de la tesis debe leerse en el orden que se recomienda en la Figura 1.2. En cada uno de los capítulos, se realiza una revisión de los respectivos conceptos, relacionados con el tema de protección de infraestructura crítica, vulnerabilidad estructural y redes complejas.

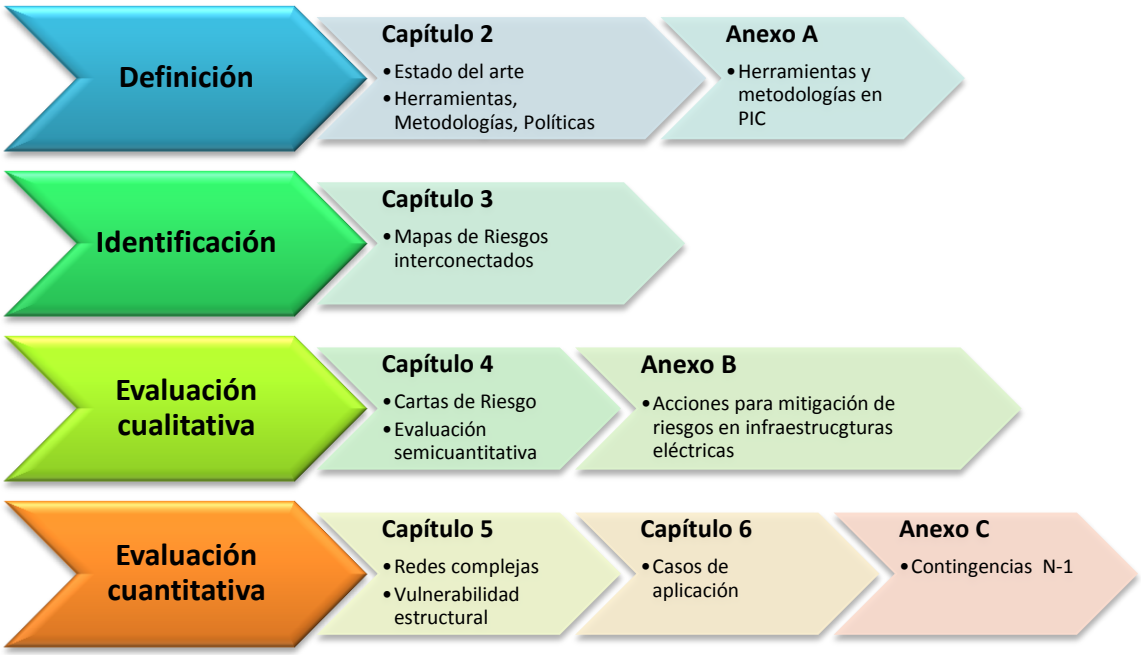


Figura 1.2: Estructura del documento de tesis

El capítulo 2 presenta una actualización del **estado del arte** en el tema de seguridad energética y específicamente en lo que respecta a la protección de infraestructuras críticas. Para el efecto, esta revisión se fundamenta en la visión conceptual de los países de la OCDE, y en concreto, de conformidad con la Directiva 2008/114/CE de la UE relativa a la identificación y designación de infraestructuras críticas europeas, y en el Plan Nacional de Protección de Infraestructuras de EE.UU del 2009.

La revisión se centra en las diferentes definiciones de la seguridad energética, infraestructura crítica y recursos clave, presentando las experiencias en países considerados como de referencia internacional sobre el tema. Adicionalmente, se lleva a cabo una revisión completa de las actuales metodologías, modelos y aplicaciones de simulación en torno a la protección de infraestructuras críticas, de acuerdo con su funcionalidad dentro de un marco de gestión de riesgos, cuya descripción se encuentra en el anexo A.

El capítulo 3 presenta una propuesta metodológica aplicable a la **identificación de riesgos** en infraestructuras críticas del sector eléctrico. Se realiza una revisión completa de las actuales metodologías, modelos y aplicaciones de simulación en torno a la identificación de riesgos para la protección de infraestructuras eléctricas críticas, dentro de un marco de gestión de riesgos.

La propuesta de trabajar con mapas de riesgos se sustenta a partir del análisis de la revisión bibliográfica y el diagnóstico del estado del arte. De esta manera, se confirma la robustez que en la etapa de identificación ofrece la mencionada metodología. Finalmente, se propone realizar la tarea de identificación de amenazas mediante el uso de *mapas interconectados de riesgos*, los cuales constituyen la base para obtener las componentes de riesgo que afectan a cada una de los elementos en la cadena de valor en las redes de infraestructuras eléctricas.

En el capítulo 4 se realiza la propuesta de una aproximación metodológica para la **evaluación de amenazas** en infraestructuras energéticas, mediante la utilización de metodologías semicuantitativas de evaluación de riesgos. Como resultado, se obtiene una *carta de riesgos*, en la cual se determinan las amenazas más críticas e importantes. Se presenta un caso de estudio que contiene la información de fuentes humanas, relacionadas especialmente con un caso de estudio en Colombia. Este capítulo se complementa con el anexo B, el cual contiene una propuesta de acciones requeridas para la mitigación de cada uno de los riesgos identificados. La base de datos generada con estas recomendaciones puede ser de utilidad para las empresas propietarias y operadoras del sistema de infraestructura crítica.

La segunda parte de la tesis hace énfasis en estrategias cuantitativas de evaluación de vulnerabilidad, así como su aplicación a casos reales.

El capítulo 5 presenta una metodología novedosa para el **cálculo de la vulnerabilidad estructural** de los sistemas de potencia. La demostración de la efectividad de esta propuesta se realiza mediante el estudio de las diferentes redes de prueba IEEE. Se realiza una comparación entre los resultados de las herramientas tradicionales en ingeniería eléctrica, como son los flujos de carga, con las mediciones estadísticas de indicadores en redes complejas. Adicionalmente, se demuestra la versatilidad de la propuesta, tanto por la rapidez de ejecución de los algoritmos asociados, como por la capacidad de procesar datos cuando se dispone de información incompleta.

El capítulo 6 refleja una **aplicación práctica** de la metodología desarrollada, a través del caso de estudio en las redes de transporte de alta tensión en Colombia y en España. Además, se realiza un análisis de la efectividad sobre aquellas inversiones contempladas en los documentos de planificación de los respectivos gobiernos tendientes a mejorar la robustez del sistema, así como la expansión de la red.

El anexo complementario C se desarrolla a partir de la metodología formulada en el capítulo 5. Empleando una red de prueba, se propone la valoración de vulnerabilidad en cada uno de los elementos del sistema, empleando indicadores característicos de la red de infraestructura (índices de severidad, desconexión de cargas y conectividad de la red), a través del método de análisis de contingencias N-1.

2 ESTADO DEL ARTE EN LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

En este capítulo se estudian las diferentes propuestas contempladas a nivel internacional para la implementación de los Planes de Protección de Infraestructuras (PIC), que incluyen los programas estratégicos de los diferentes gobiernos y estamentos supranacionales, así como las líneas de investigación que se han abierto alrededor de los PIC, especialmente aquellos orientados al sector eléctrico.

El estudio de las amenazas y vulnerabilidades en los sistemas de infraestructura crítica muestra dos tendencias importantes. Una primera tendencia se refiere a la identificación de métodos, técnicas, herramientas y esquemas para describir el estado actual de las infraestructuras a través de técnicas de matrices de riesgo, o mediante descripciones topológicas de teoría de grafos. La otra tendencia tiene en cuenta el comportamiento dinámico de los sistemas de infraestructuras por medio de técnicas de simulación, incluyendo la dinámica de sistemas, simulación de Monte Carlo, sistemas multiagente, etc.

2.1 OBJETIVO DEL CAPÍTULO

En este capítulo se presenta el estado del arte de los conceptos de seguridad del abastecimiento energético, protección de infraestructuras energéticas y recursos claves, en un marco de gestión de riesgos. En general, se pretende cumplir con los siguientes objetivos:

- Realizar una revisión bibliográfica, que incluya artículos de revistas internacionales, informes, estándares y políticas gubernamentales, que aparecen durante la última década (1999-2012).
- Realizar un análisis crítico de los enfoques metodológicos y las consideraciones específicas sobre infraestructuras eléctricas, de acuerdo a la selección de literatura sobre la base de su aplicabilidad y la documentación de las mejores prácticas.
- Presentar y analizar las definiciones y las experiencias internacionales sobre la seguridad energética e infraestructuras críticas, así como la importancia que ha tenido este problema en la investigación pública actual.
- Generar una visión de las metodologías actuales, modelos y aplicaciones de simulación, que apoyan la investigación científica en materia de protección de infraestructuras críticas, con énfasis en su clasificación y la funcionalidad. Lo anterior, según las etapas de gestión de riesgos que están incluidos en los programas NIPP y PEPIC: identificación, evaluación de riesgos, priorización e implantación de acciones y medición de efectividad.

Con el cumplimiento de estos objetivos, se presenta una discusión posterior destinada a orientar la investigación de la tesis en esta área específica. La evaluación de amenazas al sistema de abastecimiento energético cubre una amplia gama de temas, que incluyen **definiciones**, **evaluación de recursos**, **indicadores**, **gestión de riesgos**, entre otros aspectos. En consecuencia, en esta revisión del estado del arte, se procura enriquecer el debate científico y político en torno a los intereses estratégicos relacionados con la seguridad de las infraestructuras críticas de una nación, para lo cual se incluyen algunas aplicaciones metodológicas, clasificadas en un marco de gestión de riesgos.

2.2 PROGRAMAS DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS (PIC)

Como preámbulo al marco conceptual de las estrategias y metodologías en materia de protección de infraestructuras críticas, se discuten los conceptos y

definiciones de la seguridad energética. En general, una revisión de la literatura científica y política proporciona información relativa a la definición de este término en áreas como: indicadores de oferta de energía, diversificación de las fuentes de suministro energético, herramientas para la toma de decisiones, geopolítica y el pensamiento militar, etc.

Tradicionalmente, el enfoque de la ***seguridad energética*** se había concentrado en la prevención de accidentes y la respuesta frente a desastres naturales. A partir de los hechos acontecidos el 11 de septiembre 2001, los gobiernos de los países que conforman la OCDE y sus respectivas asociaciones industriales, también consideran incluir la noción de ***seguridad energética*** desde el punto de vista de la infraestructura crítica y recursos clave [BELLUCK, HULL *et al.*, 2007; GIROUX, 2010]. Aunque la posibilidad de un ataque informático a las infraestructuras críticas ya se había identificado desde principios de la década de 1990, los riesgos en la infraestructura energética se hicieron más prominentes, debido a los acontecimientos que durante el siglo XXI han afectado significativamente a la opinión pública (ataques terroristas y desastres naturales). Adicionalmente, el accidente nuclear de nivel 7 en la planta de energía nuclear Fukushima en Japón en marzo 2011 ha ubicado el tema de la infraestructura crítica de energía en las agendas políticas [YUSTA, CORREA *et al.*, 2011].

En primer lugar, se reconoce el término "***infraestructura crítica"***, definido como cualquier elemento, sistema o parte del mismo, situado en un país y que se considera esencial para el mantenimiento de sus funciones sociales vitales: la salud, la integridad física de sus habitantes, la seguridad, el bienestar económico, el funcionamiento de la sociedad [US Dept Home Security, 2003].

La literatura coincide en definir al sistema energético de un país, como una red interconectada y compleja. La interrupción en una parte de la infraestructura puede causar perturbaciones en otras partes del sistema. A esta definición se le denomina ***interdependencia*** [CONSOLINI, 2009].

2.2.1 ASEGURAMIENTO ENERGÉTICO

El concepto de suministro de energía abarca nociones diferentes, que son analizados en diversos escenarios. Como consecuencia, la definición clásica de la seguridad energética basado inicialmente en el suministro de energía lo suficientemente asequible, también requiere la adición de nuevos conceptos, incluyendo la estabilidad de precios, diversificación de las fuentes de energía,

inversiones, seguridad de la infraestructura, almacenamiento de reservas, balance de poder político y militar, eficiencia energética, mercados y sostenibilidad del suministro [YUSTA, 2008].

Otra definición alrededor del término "seguridad energética" considerada por organismos internacionales como la *Agencia Internacional de la Energía* (IEA), se refiere a la probabilidad de que la energía sea suministrada de forma continua a una nación [LE COQ & PALTSEVA, 2009; BRANCUCCI, BOLADO *et al.*, 2012]. La baja confiabilidad del suministro energético, conduce a precios altos y volátiles. Como resultado, hay otro tipo de concepto geopolítico ya que la disponibilidad de energía es el activo estratégico, esencial para cada economía para apalancar su crecimiento [IEA, 2002].

Algunos otros autores introducen indicadores técnicos que cuantifican el potencial exergético mineral representado en las reservas de energía de los minerales como el carbón, el gas natural y petróleo en el suelo, por lo que es posible predecir el agotamiento de las principales reservas de estos minerales en los próximos 50 años [VALERO, 2008]. En esas discusiones, la seguridad energética se refiere a la necesidad de las naciones para garantizar la aplicación de los avances tecnológicos que les permitan abandonar la gran dependencia del petróleo y otros combustibles fósiles para asegurar su independencia energética.

En general, existe acuerdo para definir que el sistema de energía de un país es interconectado y complejo. Las interrupciones en una parte de la infraestructura se pueden diseminar a través del sistema. En resumen, el concepto de **infraestructura crítica y recursos clave** incluye todos aquellos activos tan vitales para cualquier país, que su destrucción o degradación puede tener un efecto debilitador sobre las funciones esenciales de los gobiernos, la seguridad nacional, la economía o la salud pública [HULL, BELLUCK *et al.*, 2006]. La interrupción de un solo sector de la infraestructura crítica, a causa de ataques terroristas, desastres naturales o daños provocados por el hombre, puede tener efectos en cascada sobre otros sectores [LÖSCHEL, MOSLENER *et al.*, 2010].

La Figura 2.1 esquematiza, a manera de ejemplo, cuán entrelazados con las infraestructuras energéticas de una nación, se encuentran los recursos clave y los servicios de agua, electrónica y telecomunicaciones [NESS, 2006], indispensables para mantener el desarrollo y funcionamiento en todas las instancias de una sociedad. La no comprensión de estas interdependencias llevará a la realización de respuestas no efectivas, y a la falta de coordinación entre las organizaciones y los grupos

responsables de los rescates, la recuperación y la restauración en una emergencia. También puede causar la mala administración de recursos, provisiones y protección a la vida humana.

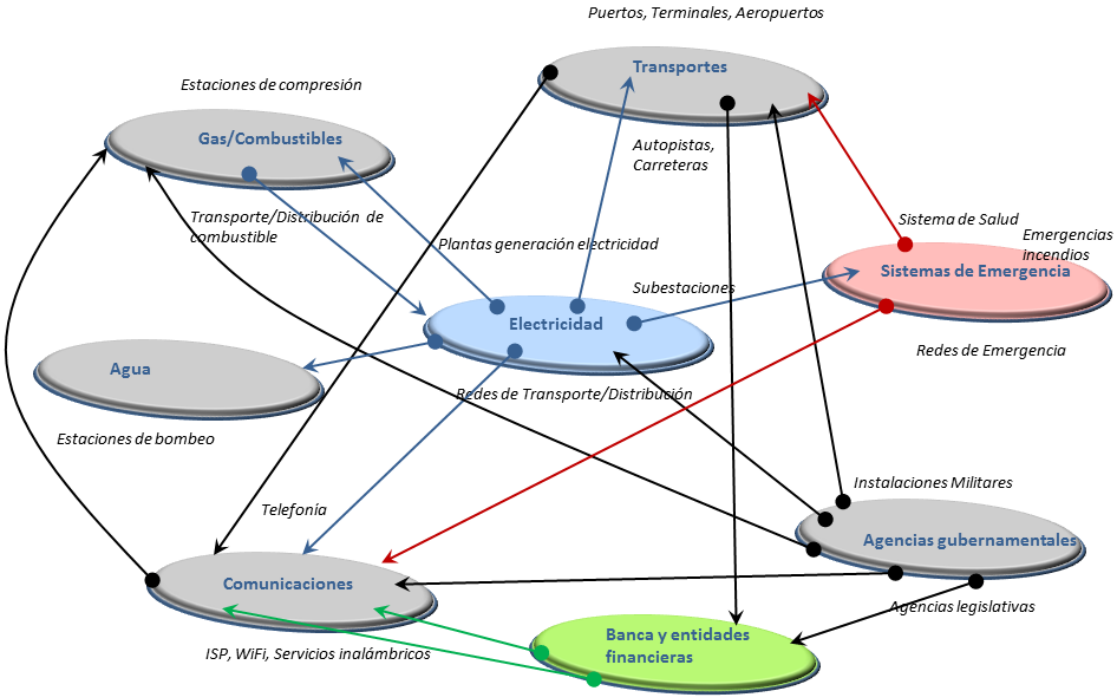


Figura 2.1: Interdependencia entre el sistema energético y otras infraestructuras críticas

En consecuencia, los gobiernos, entidades reguladoras, y expertos de la industria han enfocado su atención en el estudio de las vulnerabilidades del sistema de suministro energético de las naciones ante ataques intencionales, accidentes o desastres naturales. Actualmente, el tema de seguridad energética se contempla como uno de los asuntos de mayor importancia en las políticas nacionales. Los gobiernos representan un papel vital en la protección del sector energético, en la prevención y gestión de crisis relacionadas con el suministro energético. [BELLUCK, HULL *et al.*, 2006]

En resumen, la definición clásica de la seguridad energética, inicialmente limitada al suministro de energía suficientemente asequible, ahora es un concepto tan amplio que las estrategias deben estar sintonizadas en la protección frente a distintas amenazas.

2.2.2 CONCEPTO DE INFRAESTRUCTURAS CRÍTICAS

Son múltiples los enfoques que distintos gobiernos y organizaciones internacionales realizan al tema de la protección de la infraestructura. Los países de la

Unión Europea, Norteamérica, América Latina, y Australia/Nueva Zelanda han liderado el desarrollo de políticas para asegurar los planes de protección de infraestructura crítica. Algunas de sus definiciones son:

- **Según el USA Patriot Act de 2001**: Las infraestructuras críticas están compuestas por aquellos sistemas y sus activos, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la inhabilitación o la destrucción de estos sistemas y sus activos tienen un alto impacto en la seguridad económica nacional, en la salud pública, en la seguridad nacional, o cualquier combinación de estas cuestiones [US Dept Energy Office, 2002].
- **Según la Directiva 2008/114/CE de la UE**: Las infraestructuras críticas son todos los elementos, sistemas o parte de éstos situados en los Estados miembros, esenciales para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones [CUE, 2008].
- **De acuerdo con la ley Española 08/2011 sobre protección de infraestructuras críticas**: Están constituidas por aquellas instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios públicos esenciales, cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su interrupción o destrucción tendría un grave impacto sobre los servicios públicos esenciales, los cuales a su vez son requeridos para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y de las Administraciones Públicas [CNPIC, 2010; BOE, 2011a].

Las infraestructuras están sometidas a *riesgos corto plazo* (relacionados con la interrupción inesperada de su operación) y *riesgos* de *largo plazo* (relacionados con la suficiente disponibilidad de energía para satisfacer la demanda y la adecuación de la infraestructura para abastecer los mercados que, a su vez, dependen de los niveles de inversión y contratación, el desarrollo tecnológico y la disponibilidad de fuentes de energía primaria).

La gran mayoría de los activos relacionados con los sistemas de infraestructura crítica en los países de la OCDE son propiedad de organizaciones privadas. Cerca del 80% de estas infraestructuras las posee y las opera directamente firmas privadas [ARROYO, 2010]. Algunas excepciones las constituyen los sectores

como el agua, las instalaciones gubernamentales, y los servicios de emergencias (que son propiedad de los gobiernos o de entidades mixtas).

2.2.3 DESCRIPCIÓN DE LA CADENA DE VALOR DE LOS SISTEMAS ENERGÉTICOS

Los riesgos para la población y el medio ambiente, asociados a los sistemas eléctricos, no están localizados solamente en la etapa de producción de electricidad. Los riesgos afectan en general a todas las etapas de la cadena de valor: generación, transporte, distribución y comercialización de la electricidad. En la Figura 2.2 se presenta un esquema de los subsistemas que componen la cadena de valor de los sistemas eléctricos.

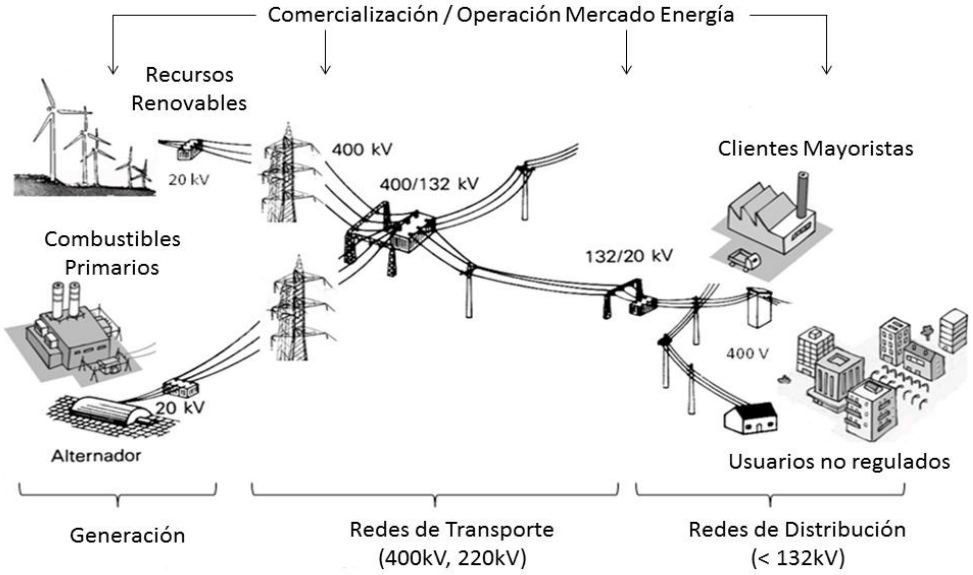


Figura 2.2: Subsistemas de la cadena de valor del sistema eléctrico

Particularmente, la red de transporte de energía eléctrica es la parte de la cadena de valor del sistema de infraestructura eléctrica constituida por los elementos necesarios para llevar hasta los puntos de consumo y a través de grandes distancias la energía eléctrica generada en el subsistema de generación.

Para ello, los niveles de energía eléctrica producidos deben ser transformados elevándose su nivel de tensión. Un ejemplo del sistema de transporte de electricidad lo constituye el sistema interconectado nacional de transporte en alta tensión cuyos esquemas se aprecian en la Figura 2.3, comparando el sistema colombiano [ISA, 2009] y el sistema español [REE, 2009]. En el capítulo 6 se realiza un análisis detallado sobre las posibles vulnerabilidades a las que se someten las

redes presentadas en la Figura 2.3, correspondientes a los sistemas de 400kV en el caso de España y 220kV, 500kV en el caso de Colombia.

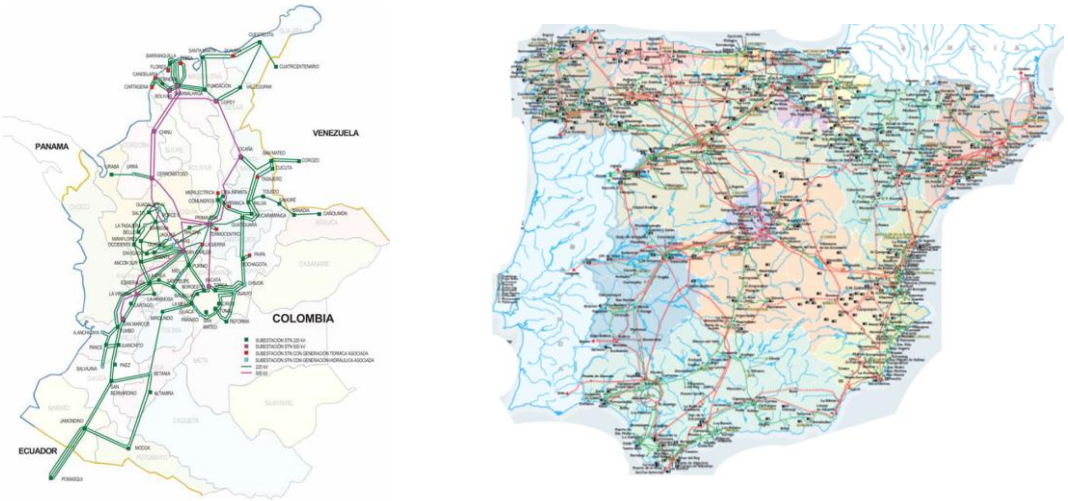


Figura 2.3: Sistema interconectado nacional de alta tensión en Colombia y España

Aunque es indudable la necesidad de proteger la red de mayor escala, es decir la red de transporte en alta tensión, también requieren atención las redes de distribución, que por medio de un extenso conjunto de instalaciones permiten el suministro eléctrico a todos los consumidores. En el caso español, por ejemplo, la red de transporte suma más de 50.000 km. de líneas eléctricas, pero las redes de distribución superan los 500.000 km. Las redes eléctricas siempre han sido vulnerables y quienes precisan el aseguramiento de sus necesidades energéticas por cuestiones estratégicas adoptan habitualmente soluciones basadas en recursos disponibles in-situ [CURTIS, 2007]. Entre otras, las instalaciones militares se dotan habitualmente de suministros eléctricos alternativos y autónomos que les garanticen respaldo al abastecimiento energético en caso de fallo de la fuente principal de suministro.

2.2.4 PLANES DE PROTECCIÓN DE INFRAESTRUCTURA

Es evidente que existe amplio consenso en la definición de las infraestructuras críticas como aquellas cuya indisponibilidad repentina pueda significar pérdida de vidas o impactos graves en los sistemas sanitarios, de seguridad o económicos de los ciudadanos.

A partir de las definiciones establecidas previamente en la sección 2.2.2, tanto en los Estados miembros de la Unión Europea, como en los Estados Unidos de América, se han conformado comités y grupos de trabajo sobre prevención,

preparación, respuesta a los ataques terroristas y los programas de solidaridad sobre las consecuencias de las amenazas a las infrastructuras. Como resultado, la Comisión Europea adoptó en 2005 un Libro Verde "*programa europeo para la protección de infraestructuras críticas*" [CE- Europa, 2005]. Posteriormente, en diciembre de 2008, el Consejo Europeo aprobó la Directiva 2008/114/CE [CUE, 2008]. En 2009 el gobierno de Estados Unidos aprobó el *Plan de Protección de Infraestructura Nacional* [NIPP, 2009] a través del Departamento de Seguridad Nacional. Ambos programas definen las áreas críticas en las que los esfuerzos deben centrarse en la prevención y la protección de la infraestructura. La Tabla 2.1 resume el listado de infraestructuras críticas definidas por cada uno de los enfoques.

Tabla 2.1: Listado de los Sectores de Infraestructura Crítica, según los enfoques del NIPP (EEUU) y de la Directiva de la Unión Europea.

IDENTIFICACIÓN MACROSECTORES EN EL NIPP (EEUU)	IDENTIFICACIÓN MACROSECTORES DIRECTIVA 2008/114/CE	
Agricultura y Alimentos	Energía	Electricidad
Banca y Finanzas		Petróleo
Comunicaciones		Gas
Instalaciones militares y de defensa	Transportes	Carreteras
Energía		Ferrocarriles
Tecnologías de la Información		Aviación
Monumentos e Íconos nacionales		Vías navegables interiores
Sistemas de Transporte		Transporte Marítimo y puertos
Agua potable y plantas tratamiento		

Estos planes ofrecen la oportunidad de definir más claramente los sistemas de alerta con el fin de proteger la infraestructura crítica, incluyendo la planificación y ejecución de las actividades para asegurar la continuidad y la fiabilidad de estas infraestructuras. Tales planes de protección de infraestructuras se concentran principalmente en los sectores de energía, transporte, tecnología de la información y las comunicaciones. Es más amplia la visión presentada por el NIPP, dado que abarca más cantidad de sectores en los que se identifican Infraestructuras Críticas. Sin embargo, aunque la aproximación inicial realizada por la Comisión Europea en el Libro Verde [CE- Europa, 2005], inicialmente apuntaba a cubrir la mayor cantidad de infraestructuras posible, finalmente la directiva expedida [CUE, 2008] se enfocó básicamente en los sectores de Energía y Transporte, incluyendo la cadena de valor básica y auxiliar.

Estas metodologías también sugieren el uso de modelos de riesgos. Dichos modelos están concebidos como una estrategia para reducir la incertidumbre que

emplea la recopilación de datos de los activos y de las interrelaciones en las infraestructuras, además del uso de enfoques prioritarios para llegar a las diferentes partes interesadas en la cadena de valor.

2.2.4.1 El programa NIPP de Estados Unidos

El *Plan Nacional de Protección de la Infraestructura Crítica y de los Recursos Clave* proporciona un marco global y unificado a través de entidades federales, estatales, territoriales, locales, tribales y el sector privado [US Dept Home Security, 2003], incluidos los sectores específicos, el Estado, y los socios del sector privado en materia de seguridad.

En el NIPP se identificaron tres áreas específicas de interés: Las interdependencias entre los sectores, la seguridad cibernética, y el carácter internacional de las amenazas sobre las infraestructuras críticas [CONSOLINI, 2009].

El marco de gestión de riesgos NIPP incluye seis pasos que implican: establecimiento de objetivos de seguridad; identificación de activos, sistemas, redes y funciones; evaluación del riesgo; priorización de acciones; ejecución de programas de protección; y medición de la eficacia. Adicionalmente, se proporciona un marco de retroalimentación y de mejora continua, en un marco flexible y adaptable al panorama de riesgo de cada sector. El esquema de este plan se presenta en la Figura 2.4.

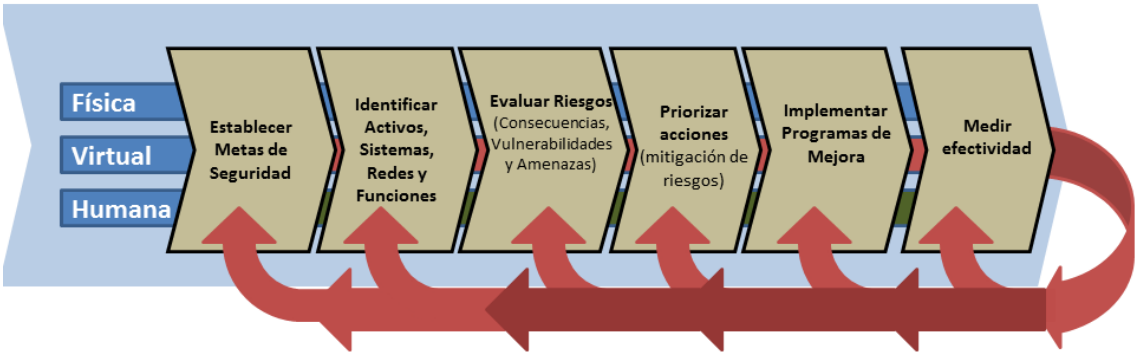


Figura 2.4: Ciclo de mejora continua para la protección de infraestructuras críticas. [NIPP, 2009]

Las metas de seguridad representan en su conjunto la posición deseada en materia de seguridad nacional. Estas metas varían entre los sectores y deben tener en cuenta los elementos físicos, humanos y cibernéticos de la protección de la infraestructura crítica y de los recursos clave.

Desde la perspectiva del sector, en el marco de la gestión de riesgos, la etapa del **establecimiento de las metas de seguridad** tiene en cuenta consideraciones

determinantes como la pérdida de vidas humanas, el impacto económico, y el impacto de la seguridad nacional para la formulación de sus objetivos.

La **identificación de recursos, sistemas, redes y funciones** consiste en la elaboración de un inventario completo que contenga información básica sobre los recursos, sistemas y redes del país. Este inventario puede utilizarse para determinar los recursos, sistemas o redes críticas en el ámbito nacional, estatal o local de acuerdo al perfil de riesgo más reciente.

En la etapa de **evaluación de riesgos** se deben emplear metodologías verosímiles de valoración de riesgos, de manera que se ofrezcan resultados razonablemente completos mediante un proceso cuantitativo, sistemático y riguroso.

Para la etapa de **priorización de acciones**, el NIPP propone trabajar con los socios en materia de seguridad y establecer prioridades a partir de las evaluaciones de riesgo. De esta manera se identifica dónde es más apremiante la reducción del riesgo y se determinan las medidas de protección. Este punto requiere una comparación de los niveles relativos de riesgo de los sectores y recursos disponibles, junto con las opciones para lograr los objetivos de seguridad establecidos. Las medidas de protección se aplican donde sea posible reducir el riesgo, resultando en una mejor relación coste-beneficio.

En la etapa de **implementación de los programas de protección**, las medidas de protección están dirigidas a reducir el riesgo a través de detección de posibles atentados, reducción del atractivo de los recursos, sistemas o redes, mitigación de la gama de posibles atentados o atención para una recuperación eficaz y eficiente.

Finalmente, la etapa de **medición de la eficacia** se establece a partir de un sistema de indicadores para aportar información sobre el logro de objetivos específicos de seguridad, definidos en [NIPP, 2009].

Los indicadores ofrecen una base para establecer la responsabilidad de los agentes participantes, documentar los procesos de análisis desarrollados, facilitar diagnósticos, promover una gestión eficaz y reexaminar metas y objetivos en el ámbito nacional y local.

2.2.4.2 PEPIC: Programa Europeo para la Protección de Infraestructura

En el PEPIC se aplica la legislación europea, sus directivas, recomendaciones, las cuales constan de los siguientes elementos: [CE, 2006]

- Un procedimiento de identificación y designación de las infraestructuras críticas europeas y un enfoque común para evaluar la necesidad de mejorar su seguridad.
- Medidas destinadas a facilitar la aplicación del PEPIC, entre las que figuran un plan de acción, una red de alerta relativa a las infraestructuras críticas (CIWIN), la creación de grupos de expertos de Protección de las Infraestructuras Críticas, procedimientos para compartir información acerca de las infraestructuras, definición y análisis de interdependencias.
- Ayuda a los Estados miembros, a petición de estos, en cuanto a la seguridad de las infraestructuras críticas nacionales, y el diseño de planes de intervención.
- Medidas financieras complementarias y, en particular, el programa específico "Prevención, preparación y gestión de las consecuencias del terrorismo y de otros riesgos en materia de seguridad" para el período 2007-2013, que facilitará nuevos medios de financiación de medidas relacionadas con la protección de infraestructuras críticas.

El sector europeo de la energía proporciona una mayor atención a la protección de su infraestructura de energía a gran escala y las instalaciones. También se ha establecido una red de operadores críticos de infraestructura energética en electricidad, gas y petróleo, a cambio de su experiencia a nivel europeo en temas relacionados con la seguridad [EC, 2011b].

2.2.4.3 Otras experiencias internacionales

En casi todos los países existen objetivos políticos de protección de sus infraestructuras esenciales. En la mayor parte se han establecido comités y grupos de trabajo, cuyo mandato incluye análisis de escenarios, evaluación de amenazas y establecimiento de sistemas de alerta temprana. Cada país cuenta con una organización acorde con su cultura. Sin embargo, la mayoría presenta una organización vertical para la protección de sus infraestructuras críticas, que es dirigida desde el más alto nivel del gobierno [YUSTA, CORREA *et al.*, 2011].

La Tabla 2.2 presenta los principales planes gubernamentales que han sido documentados a través de los respectivos organismos designados, respecto a la protección de infraestructuras críticas. En general, los programas nacionales de protección de infraestructuras constituyen el marco de referencia, que se complementa con la aplicación de modelos para la gestión de riesgos. En estos modelos se emplea tanto la recopilación de datos de los activos, las interrelaciones entre las

infraestructuras, así como el uso de enfoques prioritarios para abarcar todos los subsistemas de la cadena de valor.

Tabla 2.2: Planes actuales de infraestructuras críticas.

PAÍS	PROGRAMA	PROPÓSITO	PUBLICACIÓN	AGENCIA
Alemania	Equipo CERT-Federal (CERT-Bund)	Metodología CERT/CSIRT (Internet, Telecomunicaciones)	[BSI, 2011]	Federal Office for information security
Argentina	Ciber-seguridad	Metodología CERT/CSIRT (Internet, Telecomunicaciones)	[ONTI, 2011]	Oficina Nacional de Tecnologías de Información
Australia	National Strategy for Critical Infrastructure Protection	Capacidad del país para llevar a cabo las políticas de seguridad y defensa nacional.	[Australian & CSIRO, 2008]	National Infrastructure Information
	Estándar Australiano AS/NZS 4360:1999,	Implementación de técnicas para la gestión del riesgo en sistemas y organizaciones	[AS/NZS, 1999]	Public Services Companies
Brasil	Ciber-seguridad	Metodología CERT/CSIRT (Internet, Telecomunicaciones)	[CERT.br, 2011]	Ministry of defence
Canadá	Strategy for the Protection of National Critical Infrastructure	Componentes físicos y virtuales aplicados tanto al sector público como al privado	[ABDUR RAHMAN, 2009]	North American Electric Reliability Corporation (NERC)
	Agencias nacionales de seguridad	Integración entre organizaciones federales en aspectos como seguridad nacional, administración de emergencias, cumplimientos legales, prevención del crimen, vigilancia de fronteras, respuestas a amenazas (incluyendo terrorismo, fenómenos naturales, infecciones, ciberataques).	[Canadian, 2011]	Canadian Security Intelligence Service
China	Ciber-seguridad	Metodología CERT/CSIRT (Internet, Telecomunicaciones)	[CNCERT/CC, 2011]	Computer emergency response teams within China
Colombia	Ciber-seguridad	Metodología CERT/CSIRT (Internet, Telecomunicaciones)	[CERT-CCIT, 2011]	Ministerio del interior. Agencia Nacional de Protección
Corea del Sur	Ciber-seguridad	Metodología CERT/CSIRT (Internet, Telecomunicaciones)	[KrCERT/CC, 2011]	Korea Internet security center
Francia	Libro Blanco para la seguridad y defensa nacional	National infrastructure security challenges inside and outside France	[SGDSN, 2011]	Secrétariat general de la défense nationale
	Ciber-seguridad	Metodología CERT/CSIRT (Internet, Telecomunicaciones)		Centre opérationnel de la sécurité des systèmes d'information & PIRANET Plan
Países Bajos	Centro de crisis nacional	Apoyo en la evaluación del riesgo, recomendaciones de seguridad, mejores prácticas y contactos internacionales.	[NAVI, 2011]	Nationaal Adviescentrum Vitale Infrastructuur
España	Planes nacionales de protección de infraestructura en España	Coordinación de actividades para la protección de infraestructura crítica, tanto en el sector público como privado.	[CNPIC, 2010; BOE, 2011a]	Centro Nacional de Protección de Infraestructuras Críticas
	Ciber-seguridad	Metodología CERT/CSIRT (Internet, Telecomunicaciones)	[CCN-CERT, 2011]	Centro nacional de criptología

PAÍS	PROGRAMA	PROPÓSITO	PUBLICACIÓN	AGENCIA
Reino Unido	Iniciativa para los sectores de infraestructura crítica (Comunicaciones, servicios de emergencia, energía, finanzas, alimentos, agencias gubernamentales, sanidad, transporte, agua)	Políticas de protección en sectores , recursos y servicios indispensables para todos los aspectos de la sociedad.	[CPNI, 2011]	Centre for the Protection of National Infrastructure

La mayoría de las agencias gubernamentales son organizaciones verticales estructuradas en el ámbito de las infraestructuras críticas, que son dirigidas desde el más alto nivel en todos los gobiernos. En muchos casos, los gobiernos han confiado a la protección de infraestructuras críticas tanto a propietarios y operadores de los sistemas y redes. Esta tarea se realiza siempre a través de una estrecha relación entre las autoridades civiles y militares, con el fin de garantizar la protección de los activos y las redes que componen la infraestructura. La mayoría de los planes de protección de infraestructuras críticas se han basado en los marcos de gestión de riesgos como los concebidos en el estándar australiano [AS/NZS, 1999] o en la norma ISO 31000 [ISO, 2010].

En la Tabla 2.2 también se observa gran inquietud en el ámbito de los sistemas de seguridad en las tecnologías de la información, cuya protección sigue las recomendaciones de las organizaciones internacionales de combate contra ciber-ataques y delitos informáticos [ZIELSTRA, 2010]. La mayoría de los países ya ponen en práctica políticas para la protección en tecnologías de la información, especialmente en las áreas de Internet y telecomunicaciones, de conformidad con la metodología CERT/CSIRT, que se refiere a una parte esencial de los centros de coordinación nacionales que involucran a las juntas de gobierno y las empresas en seguridad cibernética, en el que los grupos de expertos que se encargan de los incidentes de seguridad informática [ALBERTS, DOROFEE *et al.*, 2004].

2.2.4.4 Marco legal para la protección de infraestructuras críticas en España

Con la aprobación de la Ley 8/2011 de 28 de Abril de 2011, se establecen en España medidas para la protección de las infraestructuras críticas [BOE, 2011a] y se da cumplimiento a la transposición a la legislación nacional de la Directiva 2008/114/CE [CUE, 2008]. La Ley crea el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), órgano adscrito al Ministerio del Interior a través del cual se coordinan y se supervisan las actividades de los agentes implicados en la protección de las Infraestructuras Críticas, se elaboran los planes generales de protección, así como los planes específicos de cada sector, fomentando las relaciones

entre el sector público y privado y la cooperación internacional, y facilitando el intercambio de información y conocimiento a todos los niveles.

En la Ley se incorporan las definiciones de la Directiva 114/CE, que incluyen la clasificación de activos estratégicos nacionales y transnacionales, los organismos y los sectores estratégicos. La Ley brinda un marco eminentemente organizativo, especialmente en lo concerniente a la composición, competencias y funcionamiento de los órganos e instrumentos que integran el Sistema de Protección de las Infraestructuras Críticas. Los agentes de dicho sistema se indican a continuación [BOE, 2011a]:

- La Secretaría de Estado de Seguridad del Ministerio del Interior.
- El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC).
- Los Ministerios y organismos integrados en el Sistema, incluidos en el anexo de la Ley.
- Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.
- Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.
- Las Corporaciones Locales, a través de la asociación de Entidades Locales de mayor implantación a nivel nacional.
- La Comisión Nacional para la Protección de las Infraestructuras Críticas.
- El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.
- Los operadores críticos del sector público y privado, responsables de las inversiones o del funcionamiento diario de una instalación, red, sistema, o equipo físico o de tecnología de la información.

En desarrollo y ejecución de la mencionada Ley, se aprueba el Reglamento de Protección de las Infraestructuras Críticas, a través del Real Decreto 704 del 20 de Mayo de 2011, con la finalidad de desarrollar, concretar y ampliar los aspectos mencionados anteriormente. Igualmente, se destacan los siguientes instrumentos de planificación contemplados dentro del Real Decreto 704/2011 [BOE, 2011b]:

- **Plan Nacional de Protección de las Infraestructuras Críticas:** elaborado por la Secretaría de Estado de Seguridad, está dirigido a mantener seguras las infraestructuras españolas que proporcionan los servicios esenciales a la sociedad.

- **Planes Estratégicos Sectoriales:** son los instrumentos de estudio y planificación con alcance en todo el territorio nacional que permiten conocer, cuáles son los servicios esenciales proporcionados a la sociedad, el funcionamiento general de éstos, las vulnerabilidades del sistema, las consecuencias potenciales de su inactividad y las medidas estratégicas necesarias para su mantenimiento.
- **Planes de Seguridad del Operador:** correspondientes a la documentación en la cual se definen las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión. Por ejemplo, el principal operador en transporte de electricidad es Red Eléctrica de España.
- **Planes de Protección Específicos:** correspondientes a la documentación donde se definen medidas concretas por los operadores críticos para garantizar la seguridad integral (física y lógica) de sus infraestructuras críticas.
- **Planes de Apoyo Operativo**: son aquellas medidas concretas por las Administraciones Públicas en apoyo de los operadores críticos para la mejor protección de las infraestructuras críticas.

Como complemento necesario para el desarrollo eficaz de la legislación y de la estrategia nacional para la protección de las infraestructuras críticas, el CNPIC está diseñando una serie de estándares o líneas de acción, así como guías de "buenas prácticas" para compartir con las empresas estratégicas nacionales. Entre otras, el CNPIC tiene las siguientes obligaciones [CNPIC, 2010]:

- La custodia, el mantenimiento y actualización del Plan de Seguridad de Infraestructuras Críticas y el Catálogo Nacional de Infraestructuras Estratégicas, que contiene la información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras estratégicas existentes en España.
- La recogida, análisis, integración y valoración de la información procedente de instituciones públicas, servicios policiales, sectores estratégicos, y de la cooperación internacional.
- La valoración de la amenaza y análisis de riesgos sobre las instalaciones estratégicas
- El diseño y establecimiento de mecanismos de información, comunicación y alerta.

- Soporte de Mando y Control en una Sala de Operaciones, cuya activación deberá estar prevista ante situaciones de activación del nivel que se determine del Plan de Protección de Infraestructuras Críticas.
- Supervisión de los procesos de elaboración de planes de intervención en materia de infraestructuras críticas y participar en la realización de ejercicios y simulacros.
- Supervisión y coordinación de los planes sectoriales y territoriales de prevención y protección que deban activarse en los diferentes supuestos de riesgo y niveles de seguridad que se establezcan, tanto por las Fuerzas y Cuerpos de Seguridad como por los propios responsables de las operadoras.
- La elaboración de protocolos de colaboración con personal, con organismos ajenos al Ministerio del Interior, y con empresas propietarias y gestoras de infraestructuras estratégicas.
- Supervisión de proyectos y estudios de interés en la protección de infraestructuras críticas, así como la coordinación en programas financieros y subvenciones procedentes de la Unión Europea.

El CNPIC es responsable de administrar los sistemas de gestión de la información y comunicaciones que se diseñen en el ámbito de la protección de las infraestructuras críticas, que deberá contar para ello con el apoyo y colaboración de los agentes del Sistema y de todos aquellos otros organismos o entidades afectados [BOE, 2011b]. El CNPIC ha orientado claramente sus esfuerzos a la protección de las infraestructuras críticas desde un punto de vista integrado. En el sector privado, el CNPIC mantiene contactos con los propietarios y operadores de infraestructuras críticas, para lo cual se emplea el sistema de información HERMES como herramienta para mantener comunicación permanente entre todos los actores involucrados en los planes.

2.3 CLASIFICACIÓN, EVALUACIÓN, VALORACIÓN DE AMENAZAS AL SUMINISTRO ENERGÉTICO EN LOS ESQUEMAS DE LA GESTIÓN DE RIESGOS

Las cadenas de suministro energético presentan características muy diferentes, y estas cadenas interaccionan entre sí en caso de crisis. Estos problemas tienen habitualmente carácter técnico, pero también existen amenazas no técnicas que pueden afectar a la seguridad del suministro energético del país.

2.3.1 METODOLOGÍAS EN PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

La investigación científica en materia de **protección de infraestructuras críticas (PIC)** se apoya en metodologías, modelos y aplicaciones de software, las cuales son presentadas en la Tabla 2.3. La revisión presentada en esta sección se fundamenta en 55 artículos de revistas, informes y normas legales, en el período comprendido entre 1999 y 2011. Dicha tabla contiene toda la información disponible acerca de las metodologías y modelos de simulación encontrados en esta revisión del estado del arte.

La recopilación se concibe sobre la base de cuatro características principales que describen las características de cada metodología:

- **Listado de Infraestructura Crítica**: Según el listado de sectores de infraestructuras críticas, propuestas en [NIPP, 2009] y en la Directiva 114/CE [CUE, 2008], como se ha informado previamente en la Tabla 2.1. Las metodologías existentes cubren los siguientes tipos de infraestructura: electricidad, gas natural, petróleo y oleoductos, agua potable, alcantarillado y aguas residuales, control industrial, telecomunicaciones, redes informáticas y sistemas de información, ferrocarriles, carreteras y autopistas, actividades humanas, banca y finanzas. También se ha añadido un sector de políticas y regulaciones, requeridas para la formulación de políticas y toma de decisiones.
- **Tipos de Modelos**: Las técnicas de modelización utilizadas por las diferentes metodologías se aplican en PIC a través de paradigmas de simulación y de procedimientos para la toma de decisiones: sistemas multi-agente, dinámica de sistemas, matrices de calificación, las bases de datos relacionales y la teoría de grafos. Esas técnicas de modelado también se combinan con métodos computacionales y técnicas complementarias: simulación en tiempos continuos (*Cont*), tiempos discretos (*Disc*), simulación de Monte Carlo (*MC*), árboles de decisión (*AD*), sistemas de información geográfica (*SIG*) , técnicas de gestión de riesgos (*RISK*), y monitoreo de eventos en tiempo real (*T_Real*).
- **Disponibilidad y madurez**: Las aplicaciones y plataformas pueden estar todavía bajo investigación (I) o desarrollo (D); o ya están disponibles para su uso por el público en general con fines comerciales (C) o por un grupo limitado o restringido, por lo general a los militares (L).
- **Etapa en la gestión de riesgos**: Esta revisión se centra en las etapas de gestión del riesgo según la funcionalidad en cada etapa de los planes PEPIC y NIPP

(identificación, evaluación de riesgos, la priorización de acciones, implementación de programas, y medición de la efectividad), como se presentó en la Figura 2.4.

La Tabla 2.3 también indica aquellas metodologías que se representan directamente en una aplicación de software. Una explicación más profunda de cada una de estas herramientas de software se describe en el anexo A.

La información clasificada de esta manera permite un análisis más claro de las diferentes tendencias en el área de análisis, modelado y gestión del riesgo en las infraestructuras críticas, de acuerdo con las tendencias actuales de investigación. En esta revisión, se analiza primero la combinación de las diferentes técnicas de modelización y luego se discute el caso específico en las infraestructuras eléctricas.

Tabla 2.3: Aplicaciones y modelos para análisis de vulnerabilidades de Infraestructuras Críticas.

APLICACIÓN/ METODOLOGÍA	PUBLICACIÓN	SOFTWARE	DISPONIBILIDAD	SECTOR DE INFRASTRUCTURA													TÉCNICAS DE MODELIZACIÓN						ETAPA				
				Electricidad	Gas Natural	Petróleo, Oleoductos	Agua Potable	Aguas residuales	Control Industrial	Telecomunicaciones	Redes y TIC's	Ferrocarriles	Carreteras	Actividades Humanas	Banca y finanzas	Políticas y regulaciones	Sistemas multi-agentes	Dibnámica de sistemas	Matrices de calficación	Bases datos relacional	Teoría de Grafos	TÉCNICA SUPLEMENTARIA	Identificación	Evaluación de riesgo	Priorización de acciones	Implementación	Medición efectividad
AIMS	[GHORBANI & MARSH, 2004]	●	I					●									●					Cont	●	●			
Athena	[DRABBLE, BLACK *et al.*, 2009]	●	L	●	●	●	●	●	●	●	●	●	●	●	●	●					●	AD		●			
CASCADE	[NEWMAN, NKEI *et al.*, 2005]	●	I	●															●			RISK	●	●			
CARVER2	[National Infrastructure Institute & PEIMER, 2010]	●	C																●			RISK	●		●		
CEEESA	[Argonne Labs & PEERENBOOM, 2010]	●	L	●	●										●				●	●		SIG	●	●		●	●
CERT/ CSIRT	[ALBERTS, DOROFEE *et al.*, 2004]		C											●	●					●		T_real	●		●	●	
CI[3]	[Argonne Labs, PEERENBOOM *et al.*, 2007]	●	L	●	●		●	●	●	●											●	MC			●		●
CIMS	[Idaho & DUDENHOEFFER, 2006]	●	C	●					●					●			●					MC		●	●	●	●

APLICACIÓN/ METODOLOGÍA	PUBLICACIÓN	SOFTWARE	DISPONIBILIDAD	SECTOR DE INFRASTRUCTURA													TÉCNICAS DE MODELIZACIÓN						ETAPA				
				Electricidad	Gas Natural	Petróleo, Oleoductos	Agua Potable	Aguas residuales	Control Industrial	Telecomunicaciones	Redes y TIC's	Ferrocarriles	Carreteras	Actividades Humanas	Banca y finanzas	Políticas y regulaciones	Sistemas multi-agentes	Dibnámica de sistemas	Matrices de calficación	Bases datos relacional	Teoría de Grafos	TÉCNICA SUPLEMENTARIA	Identificación	Evaluación de riesgo	Priorización de acciones	Implementación	Medición efectividad
CIP/DSS	[Argonne Labs, Sandia Labs *et al.*, 2008a]	●	L	●	●	●	●	●	●	●		●	●	●	●	●		●				Cont	●		●	●	●
CIPMA	[Australian & CSIRO, 2008]	●	L	●	●	●				●	●				●	●		●				Cont				●	●
CISIA	[PANZIERI, SETOLA *et al.*, 2005]	●	I	●				●	●								●			●		AD			●	●	
COMM-ASPEN	[Sandia Labs, BARTON *et al.*, 2004]	●	D	●						●					●		●					MC	●	●			●
DEW	[BROADWATER, 2006]	●	L	●					●											●	●	AD	●	●	●		
DUTCH NRA	[PRUYT & WIJNMALEN, 2010]		L	●		●	●						●	●		●			●			RISK	●	●	●		
EAR-PILAR	[MAÑAS, 2007]	●	C								●			●		●			●	●		AD	●	●	●	●	
ECI-GIS	[PEGGION, BERNARDINI *et al.*, 2008]	●	D											●	●	●						SIG	●	●			
EMCAS	[Argonne Labs & CONZELMANN, 2008]	●	C	●						●					●		●					Disc	●	●	●		
FAIT	[Sandia Labs & BROWN, 2005a]	●	L	●	●			●				●							●	●		SIG	●	●			
FINSIM	[Los Alamos Labs & FLAIM, 2006]	●	I							●					●		●					Cont	●	●			
FMEA/FMECA	[MILULAK, 2004]		C						●	●				●	●				●			RISK	●	●	●		
Fort Future	[USACE, ERDC *et al.*, 2010]	●	L	●	●	●	●	●	●	●	●	●	●	●	●	●	●					SIG	●	●	●		●
FTA	[ISOGRAPH Inc, 2010]		C						●	●				●	●				●			RISK	●	●	●		
GAMS-CERO-ERA	[ERA, 2010; Pragma, 2010]		C											●	●	●			●	●		AD	●	●	●	●	
GIS Inter-operatibility	[LI, ZLATANOVA *et al.*, 2007]		I									●	●									SIG			●		●
GoRAF	[DONZELLI & SETOLA, 2007]	●	I	●			●		●					●			●			●		AD		●	●	●	

APLICACIÓN/ METODOLOGÍA	PUBLICACIÓN	SOFTWARE	DISPONIBILIDAD	SECTOR DE INFRASTRUCTURA													TÉCNICAS DE MODELIZACIÓN						ETAPA				
				Electricidad	Gas Natural	Petróleo, Oleoductos	Agua Potable	Aguas residuales	Control Industrial	Telecomunicaciones	Redes y TIC's	Ferrocarriles	Carreteras	Actividades Humanas	Banca y finanzas	Políticas y regulaciones	Sistemas multi-agentes	Dibnámica de sistemas	Matrices de calficación	Bases datos relacional	Teoría de Grafos	TÉCNICA SUPLEMENTARIA	Identificación	Evaluación de riesgo	Priorización de acciones	Implementación	Medición efectividad
CERT Initiatives	[CNPIC, 2010; ZIELSTRA, 2010; CCN-CERT, 2011]		C						●		●			●		●				●		T_real	●		●	●	
HAZOP	[ISOGRAPH Inc, 2008]		C	●	●	●			●	●				●		●			●		●	RISK	●	●	●		
IEISS	[Los Alamos Labs, Sandia Labs *et al.*, 2006]	●	L	●	●		●	●								●	●					MC	●		●	●	
IIM	[QUARLES & HAIMES, 2007]	●	I	●			●			●	●		●			●			●		●	Cont	●		●	●	
Infrastructure Disruptions	[BEYELER & BROWN, 2004]	●	I											●		●		●				Cont				●	●
IRAM	[EZELL, V. *et al.*, 2000]	●	I				●	●											●			RISK		●	●	●	
IntePoint Vu	[IntePoint & ARMSTRONG, 2010]	●	C	●						●		●	●	●			●					SIG			●		
Knowledge Management & Visualization	[DODRILL, GARRETT *et al.*, 2007]	●	I	●												●			●			RISK				●	●
LUND	[JOHANSSON, 2010]		I	●								●	●							●	●	RISK	●	●			
MARGERIT V2	[CCN Criptología, 2010]		C								●			●	●	●			●			RISK	●	●		●	
MIA	[ENEA, Europa *et al.*, 2010]		I	●						●	●					●			●	●		AD	●	●			
MIN	[PENGCHENG, SRINIVAS *et al.*, 2005]	●	I										●	●			●					Cont	●				
Modular Dynamic Model	[BEYELER, BROWN *et al.*, 2002]	●	I	●														●				Cont		●		●	●
MUNICIPAL	(Lee et al., 2005)	●	I	●						●	●									●		RISK	●		●		
N-ABLE	[Sandia Labs & BROWN, 2005b]	●	L	●								●			●		●					Disc	●		●	●	●
NEMO	[SPARTA Inc, GOODWIN *et al.*, 2005]	●	L	●	●		●					●				●	●			●		Cont			●	●	●

APLICACIÓN/ METODOLOGÍA	PUBLICACIÓN	SOFTWARE	DISPONIBILIDAD	SECTOR DE INFRASTRUCTURA													TÉCNICAS DE MODELIZACIÓN						ETAPA				
				Electricidad	Gas Natural	Petróleo, Oleoductos	Agua Potable	Aguas residuales	Control Industrial	Telecomunicaciones	Redes y TIC's	Ferrocarriles	Carreteras	Actividades Humanas	Banca y finanzas	Políticas y regulaciones	Sistemas multi-agentes	Dinámica de sistemas	Matrices de calificación	Bases datos relacional	Teoría de Grafos	TÉCNICA SUPLEMENTARIA	Identificación	Evaluación de riesgo	Priorización de acciones	Implementación	Medición efectividad
NSRAM	[McMANUS, BAKER *et al.*, 2004]	●	I	●						●										●		MC			●	●	●
NGFast	[PORTANTE, CRAIG *et al.*, 2007]	●	L		●	●													●			SIG	●	●			●
OGC CIPI	[OGC, 2002]		I													●			●			SIG	●		●		●
PCI-Information	[FERIGATO & MASERA, 2007]		I													●			●			RISK				●	
MAPAS DE RIESGOS	[COSO, 2004; PMI, 2004; ERM Initiative, 2010]		I	●	●	●	●	●	●	●	●	●	●	●	●	●						RISK	●				
SAIV	[COURSAGET & (SGDSN), 2010]		I													●			●			RISK				●	
TEVA	[Argonne Labs, Sandia Labs *et al.*, 2008b]	●	I				●													●		SIG	●	●	●		
TRAGIS	[Oak Ridge, JOHNSON *et al.*, 2003]	●	L									●	●			●						SIG	●				
TRANSIMS	[Los Alamos Labs & SMITH, 1999]	●	C											●			●					Disc					●
UIS	[Los Alamos Labs & MICHELSEN, 2008]	●	L				●	●		●			●	●			●					Disc	●	●	●	●	
UML-CI	[BAGHERI & GHORBANI, 2007]		I													●				●		T_real	●				
USArmy Risk Mitigation	[LEE, 2001]	●	I				●	●						●				●				Cont		●		●	●
WISE	[Los Alamos Labs & HOLLAND, 2008]	●	D				●	●									●					Cont	●	●		●	●
VINCI	[BAIARD, SALA *et al.*, 2007]		I								●								●			T_real				●	

Aunque la lista de las metodologías y aplicaciones que se muestran en Tabla 2.3 no es exhaustiva, sí refleja la mayoría de las investigaciones que se realizan en el

área de protección de infraestructuras críticas (PIC). El anexo A recoge una breve descripción de las características principales de cada uno de estos sistemas.

En este estudio se ponen de manifiesto dos tendencias principales en las metodologías revisadas. Una primera tendencia se centra en el estudio, análisis y comprensión de la infraestructura de las primeras etapas de construcción y montaje de la infraestructura. En esta tendencia se identifican técnicas, herramientas y gráficos para describir el estado actual de la infraestructura, y utiliza los métodos de evaluación de las amenazas para obtener una visión más clara sobre el funcionamiento de la infraestructura. Para ello, se tienen en cuenta cada uno de los posibles riesgos que afectan al sistema y se determinan sus posibles consecuencias.

Otra línea de investigación se centra en la comprensión del comportamiento dinámico de los sistemas de infraestructura, y utiliza técnicas de simulación (dinámica de sistemas, simulación de Monte Carlo, sistemas multi-agente, etc) con los que se exploran los procesos de operación, para identificar las causas de inestabilidad en una infraestructura.

Cada una de las aplicaciones examinadas en la Tabla 2.3 proporciona características únicas. El análisis de dicha información busca identificar características comunes, sus ventajas e inconvenientes, así como las tendencias en el uso de las técnicas de modelización. Se estima que la investigación en esta área seguirá aumentando en los próximos años debido a las políticas emergentes y a la creciente preocupación de la sociedad, por lo que la información presentada aquí puede proporcionar una guía para mejorar ciertas deficiencias de tales áreas de estudio.

2.3.2 APLICACIONES PARA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

De las 55 aplicaciones y plataformas, el 69% corresponden a herramientas de software y el 31% conciernen a metodologías analíticas. Un primer debate se impulsa desde las siguientes perspectivas:

- Disponibilidad y la madurez de las aplicaciones.
- Combinación de modelos matemáticas y técnicas computacionales que se utilizan actualmente en la investigación sobre protección de infraestructuras críticas.
- Uso de modelos computacionales aplicados a la lista de los sectores de infraestructura crítica.
- Uso de técnicas de modelización en cada etapa del marco de gestión de riesgos.

2.3.2.1 Disponibilidad y madurez

Aproximadamente la mitad de las aplicaciones se han enfocado al desarrollo de plataformas informáticas, ya sea de tipo comercial o de uso restringido, por ejemplo, a nivel corporativo, institucional, organismos privados o militares, como se muestra en la Figura 2.5. Una cuarta parte de las aplicaciones tienen disponibilidad limitada y en su mayoría están dirigidas a los segmentos militares y gubernamentales. Esto podría explicarse por el liderazgo generado por algunos laboratorios de EE.UU., que a su vez, son patrocinados por el Departamento de Seguridad Nacional y el Departamento de Energía. Este apoyo ha surgido como resultado del cumplimiento de las directivas pertinentes en la PIC [US Dept Home Security, 2003; US Dept Home Security & Office, 2007; US Dept Home Security, 2009b; US Dept Home Security, 2009a].

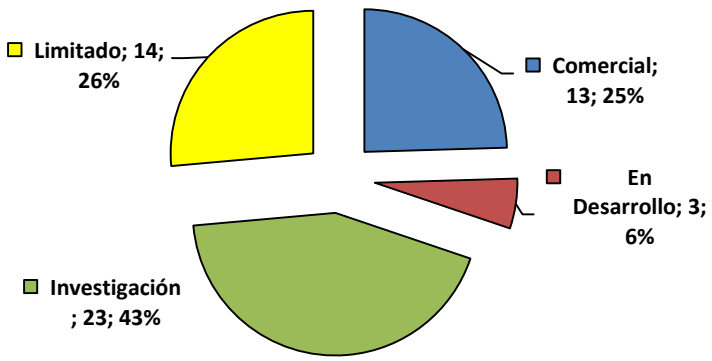


Figura 2.5: Estado de los proyectos de investigación en Infraestructura Crítica.

Otra cuarta parte de las aplicaciones tienen fines comerciales (licencias de la plataforma informática, consultoría, etc.). Dichas aplicaciones se aplican en sectores energéticos, en seguridad cibernética y en la definición de estrategias para la respuesta a emergencias.

La otra mitad de los proyectos se originan en los proyectos públicos de investigación y tesis (investigaciones terminadas o en desarrollo). Se espera que esta proporción aumente debido a la creciente atención que las organizaciones, empresas, agencias gubernamentales, centros de investigación y las universidades están prestando al tema de *PIC*.

2.3.2.2 Combinación entre modelos matemáticos y técnicas suplementarias de cómputo

Los modelos de infraestructura crítica se asocian principalmente con las técnicas de simulación y con modelos matemáticos que se combinan con técnicas

suplementarias de computación: simulación continua (*Cont*), simulación discreta (*Disc*), simulación Monte Carlo (*MC*), árboles de decisión (*AD*), sistemas de información geográfica (*SIG*), técnicas de gestión de riesgos (*RISK*), y monitorización de eventos en tiempo real (*T_real*) como soporte para la toma de decisiones, según se muestra en la clasificación de la Figura 2.6.

Existe amplia aceptación de los paradigmas de simulación, especialmente a través de modelos que utilizan **sistemas multi-agente** y **dinámica de sistemas**, que generalmente se combinan con métodos computacionales continuos (*Cont*), discretos (*Disc*) y Monte Carlo (*MC*) los cuales son adecuados para encontrar soluciones óptimas. Algunas otras aplicaciones de simulación basada en agentes, en combinación con los *SIG*, permiten predecir tanto el comportamiento humano, como el funcionamiento de la infraestructura en caso de emergencias dentro de áreas geográficas específicas.

Por su parte, las **matrices de calificación** permiten evaluar el impacto de los riesgos, a la vez que facilitan los procedimientos para la toma de decisiones. Su uso incluye el procesamiento de datos mediante mapas de riesgos y técnicas tradicionales para apoyar la toma de decisiones (Por ejemplo, datos provenientes de *SIG* o indicadores de seguimiento). Las matrices de riesgo son muy populares porque permiten combinar técnicas computacionales y facilitan el análisis de sensibilidad.

Las **bases de datos relacionales** constituyen la opción predominante en el almacenamiento de datos, registros, los cuales representan las propiedades del sistema de una manera precisa. Por esa razón, las bases de datos relacionales se utilizan ampliamente en los inventarios de activos y se pueden combinar con el monitoreo de eventos en tiempo real, la georreferenciación (*SIG*), los registros de errores, el control de acceso, los riesgos de los componentes, etc. Por lo tanto, es posible establecer relaciones entre los elementos que componen la infraestructura crítica, haciendo coincidir los datos con características comunes que se encuentran dentro de los conjuntos de datos.

La **teoría de grafos** permite identificar nodos críticos en la infraestructura, y se refieren a las propiedades del sistema de una manera más precisa. La complejidad de los modelos en la teoría de grafos aumenta exponencialmente en grandes infraestructuras, pero su aplicabilidad está ganando acogida, gracias a la capacidad computacional que permite procesar los algoritmos y medidas estadísticas de los grafos.

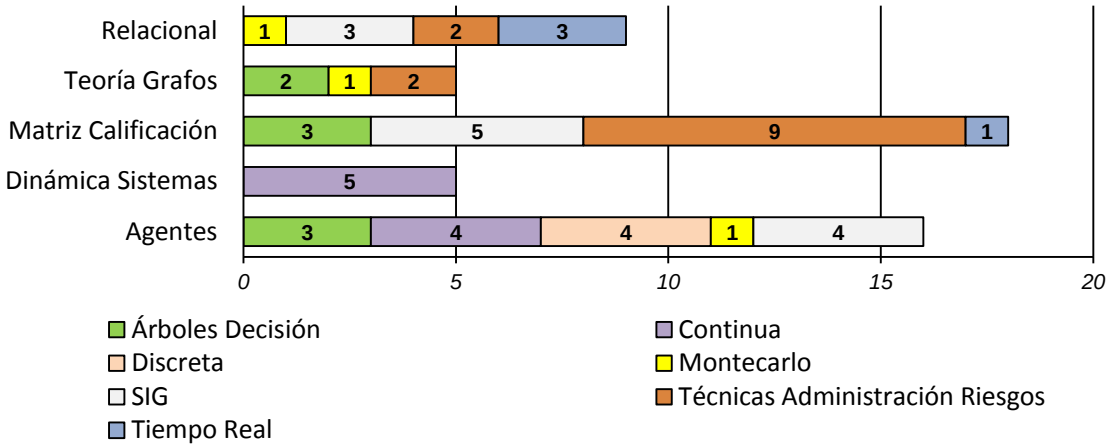


Figura 2.6: Combinaciones de técnicas de modelización en la literatura revisada

Alrededor del 39% de las publicaciones estudiadas proponen la integración de técnicas de simulación (dinámica de sistemas y simulación basada en agentes) con árboles de decisión, o con simulación Monte Carlo, simulación continua y/o discreta. 18 publicaciones (34%) realizan la evaluación de riesgos a través de la combinación de **matrices de calificación**, ya sea con los SIG, con los árboles de decisión, la supervisión en tiempo real o con técnicas de gestión de riesgos. La **teoría de grafos** y las **bases de datos relacionales** están incluidas en 18 publicaciones (26%), las cuales se combinan con simulaciones Monte Carlo (para encontrar decisiones óptimas), SIG, árboles de decisión, y con técnicas de gestión de riesgos.

Una cierta proporción de estas publicaciones (9 de 55) se basan en metodologías que combinan las **técnicas de gestión de riesgos** con **matrices de calificación**. Esto se puede explicar por el hecho que en realidad es la técnica más sencilla, ya que la evaluación se basa principalmente en juicios semi-cuantitativos.

Los modelos construidos sobre **sistemas multi-agente** se hacen cada vez más atractivos ya que el diseño de estos agentes es relativamente simple y los resultados pueden ser notables. Cerca del 30% de las solicitudes examinadas se basan en la combinación de los sistemas multi-agente, con árboles de decisión, SIG, y con técnicas de simulación continua, discreta o Monte Carlo. La mayoría de estos métodos se aplican al estudio de las interdependencias entre las infraestructuras críticas. Sus interacciones pueden explicar las acciones, comportamientos y predicción de la respuesta en situaciones de emergencia.

Por su parte, la **dinámica de sistemas** se centra más en las políticas de regulación de las actividades de las organizaciones, mediante el análisis de las interacciones entre las variables. Incluso un sistema complejo como la infraestructura

crítica puede ser fácilmente representado en estos modelos. El 9% de las plataformas dentro de la literatura revisada utilizan la herramienta mediante la definición de las interacciones entre las variables y de su causalidad circular.

2.3.2.3 Técnicas de modelización de las infraestructuras críticas

Las aplicaciones y herramientas en este estudio han sido clasificadas de acuerdo a los sectores de infraestructura crítica definidas en la Tabla 2.1.

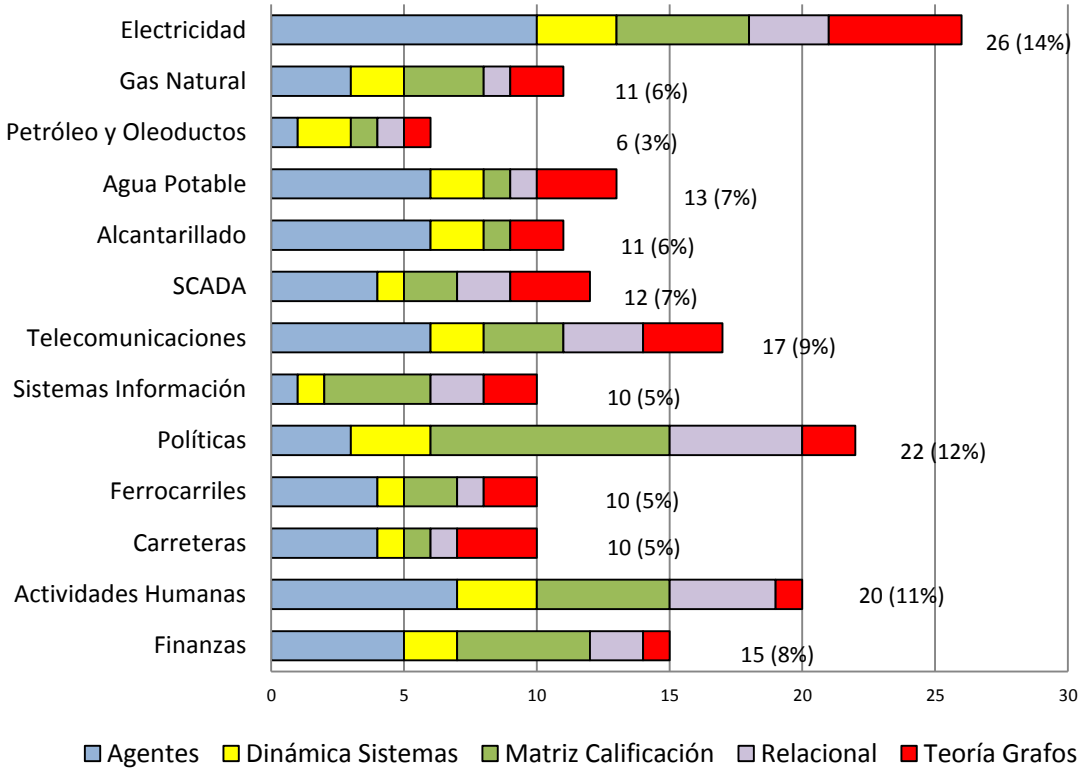


Figura 2.7: Técnicas de modelización en el estudio de cada sector de infraestructuras críticas.

Las referencias a las metodologías empleadas en cada uno de los sectores estratégicos de la infraestructura crítica se pueden apreciar en la Figura 2.7. El 23% de las publicaciones están relacionadas con los sectores de infraestructura energética (electricidad, gas natural, petróleo y oleoductos). Dichas aplicaciones se basan principalmente en las **matrices de calificación**, así como en el uso de simulación mediante **dinámica de sistemas** o **sistemas multi-agente**.

Otro énfasis de las publicaciones se relacionan con las tecnologías de la información, los sistemas de control y las telecomunicaciones (21%), agua (13%), transporte (10%), banca y finanzas (8%). Alrededor del 11% de las metodologías están relacionadas con el comportamiento de las actividades humanas y las respuestas de la infraestructura crítica, bajo condiciones de emergencias, requerimientos de seguridad

industrial y recomendaciones de políticas en la protección de los bienes y la protección de la vida humana.

La implementación de políticas y regulaciones tiene una atención especial en el 12% de las plataformas revisadas. Esto se hace a través de la evaluación del éxito en la toma de decisiones y la formulación de recomendaciones, con el fin de prevenir situaciones de emergencia, a la vez que se garantiza la continuidad del funcionamiento de los sistemas de infraestructura, incluso bajo condiciones de estrés.

2.3.2.4 Técnicas de modelización en el marco de la gestión de riesgos

Las metodologías revisadas se basan principalmente en cinco técnicas de modelización: bases de datos relacionales, teoría de grafos, matrices de calificación, dinámica de sistemas y simulaciones basadas en agentes.

Dentro de los conceptos establecidos en el marco de gestión de riesgos, es posible distinguir entre cinco etapas de análisis que faciliten la toma oportuna de decisiones para la adecuada mitigación del riesgo, según contempla el programa [NIPP, 2009], cuyas etapas se han presentado previamente en la Figura 2.4: *Identificación de riesgos*, *Evaluación de riesgos*, *Priorización de acciones*, *Implementación de programas de mejora*, *Medición de la efectividad*.

Como resultado de la revisión de literatura, los modelos que se adaptan a cada etapa se muestran en la Figura 2.8.

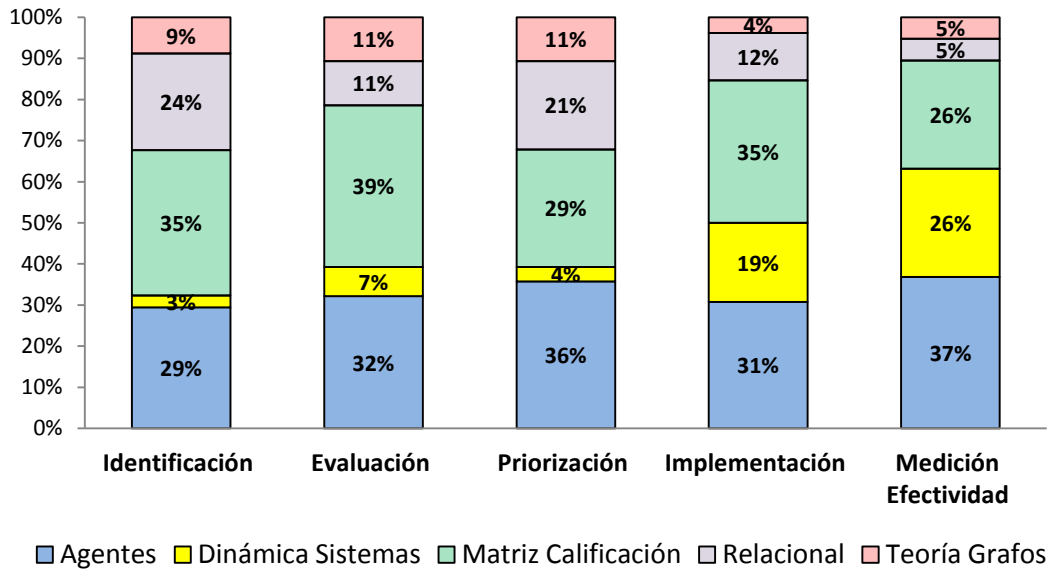


Figura 2.8: Utilización de metodologías en cada etapa de la gestión de riesgos

Los **sistemas multi-agente** y las **matrices de calificación** son las técnicas de modelización más extendidas en un marco de gestión de riesgos. La **dinámica de sistemas** es importante especialmente cuando se simulan comportamientos a largo plazo, por ejemplo, las actuaciones para estimar la eficacia de una medida que se implementa en un sistema de infraestructura.

Las **matrices de calificación** tienen amplia aceptación, especialmente en las etapas de identificación y evaluación de riesgos. También son la base para la generación de **mapas de riesgos**. Del mismo modo, las estrategias de gestión de riesgos se basan en la generación de modelos de decisión que utilizan indicadores usuales en las matrices de calificación. Por esta razón, la investigación sobre la identificación y evaluación de riesgos está tomando un impulso especial, así como la variedad de estrategias para cuantificar los riesgos.

En las etapas de la priorización de las acciones e implementación de programas, las **matrices de calificación** se generan a partir de las técnicas de toma de decisiones, las cuales son útiles para los procesos de análisis de sensibilidad.

2.3.3 CASO ESPECÍFICO ORIENTADO A INFRAESTRUCTURAS ELÉCTRICAS

Una característica inherente en la protección de la infraestructura eléctrica corresponde a la interrupción del servicio: un problema de gestión de riesgos. La mayoría de las investigaciones para cuantificar los riesgos y amenazas (técnicas y no-técnicas) en la infraestructura eléctrica, se encuentra actualmente en fase de desarrollo. En estas discusiones se afirma la amplia aceptación de las metodologías de gestión de riesgos. Esto se refleja en el hecho de que la mayoría de las organizaciones y agencias gubernamentales están trabajando actualmente con dicho marco, para generar acciones de diagnóstico y planes de protección en la infraestructura crítica de energía.

La Figura 2.9 muestra las diferentes metodologías en el marco de gestión de riesgos para la infraestructura eléctrica crítica. Como se mencionó anteriormente en la Tabla 2.3, algunas aplicaciones pueden utilizar más de una técnica de modelización, por ejemplo, simulación multi-agentes, combinada con matrices de calificación, pero en todos los casos, las técnicas de modelización se suplementan con métodos de computación (*Cont, Disc, MC, SIG, AD, RISK, T_real*). La mitad de las metodologías referidas, en el caso de PIC eléctrica, se basan en técnicas de simulación (sistemas multi-agentes 38% y dinámica de sistemas, 12%). La otra mitad corresponde a

matrices de calificación (19%), teoría de grafos (19%) y bases de datos relacionales (12%).

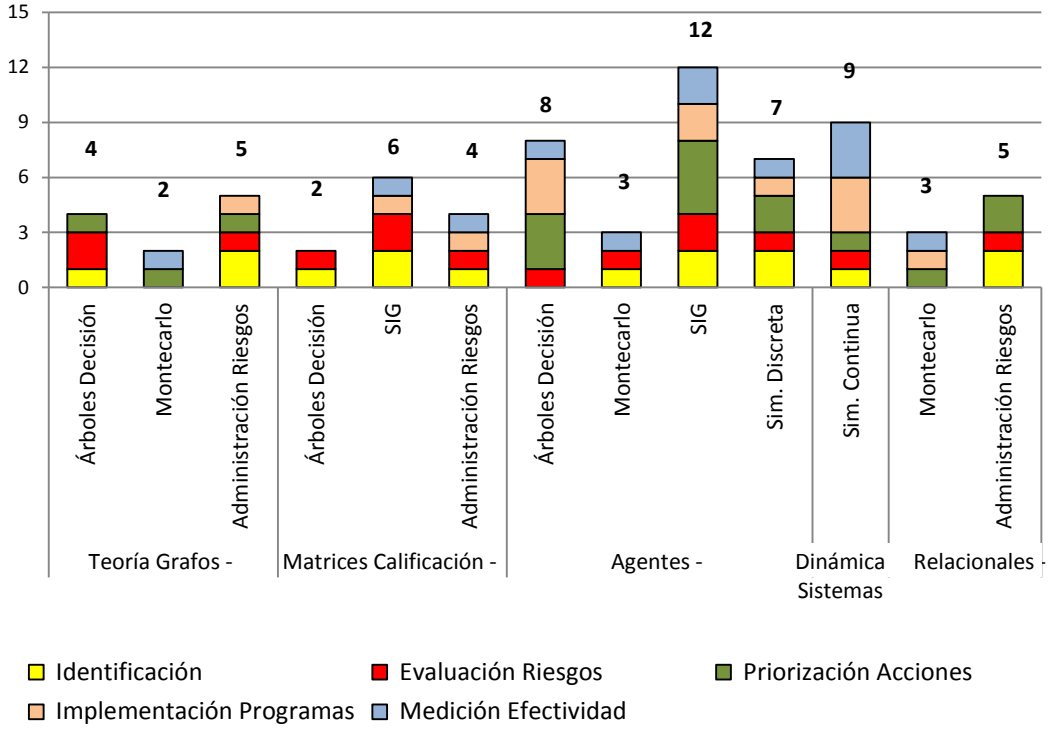


Figura 2.9: Referencias de las metodologías de modelización en el marco de gestión de riesgos (protección de la infraestructura eléctrica).

Se destaca sin embargo la aceptación de las metodologías de **simulación con dinámica de sistemas**, así como el uso de **sistemas multiagentes** (combinados con sistemas de información geográfica y con árboles de decisión), para aplicar los esquemas de gestión del riesgo, en lo referente a priorización de acciones, implementación de actividades y medición de la efectividad. Particularmente, los sistemas multiagentes permiten determinar el comportamiento de los indicadores en un sistema de infraestructura, en el corto plazo. Por su parte, la dinámica de sistemas es más útil para analizar el comportamiento del sistema de infraestructura en el mediano y largo plazo.

Aquellas publicaciones que hacen referencia a las **bases de datos relacionales** son útiles en los inventarios de activos de la red.

Las aplicaciones basadas en la **teoría de grafos** son presentadas como investigaciones académicas. En ellas se determinan las medidas de la centralidad de los nodos en redes pequeñas, y sus probabilidades de fallo, según se eliminen un porcentaje de los nodos dependiendo de su conectividad. De esta manera, se pueden obtener valoraciones sobre posibles fallos en cascada.

La Figura 2.10 muestra un resumen de los modelos clasificados en un marco simplificado de gestión de riesgos de sólo tres etapas, ya que los esfuerzos, en realidad, se concentran especialmente en la **identificación** y **evaluación** de riesgos. Es posible verificar que tanto las técnicas de matrices de riesgo, como las aplicaciones basadas en agentes, tienen amplia aceptación en todas las etapas de gestión de riesgos en los sistemas de infraestructura eléctrica.

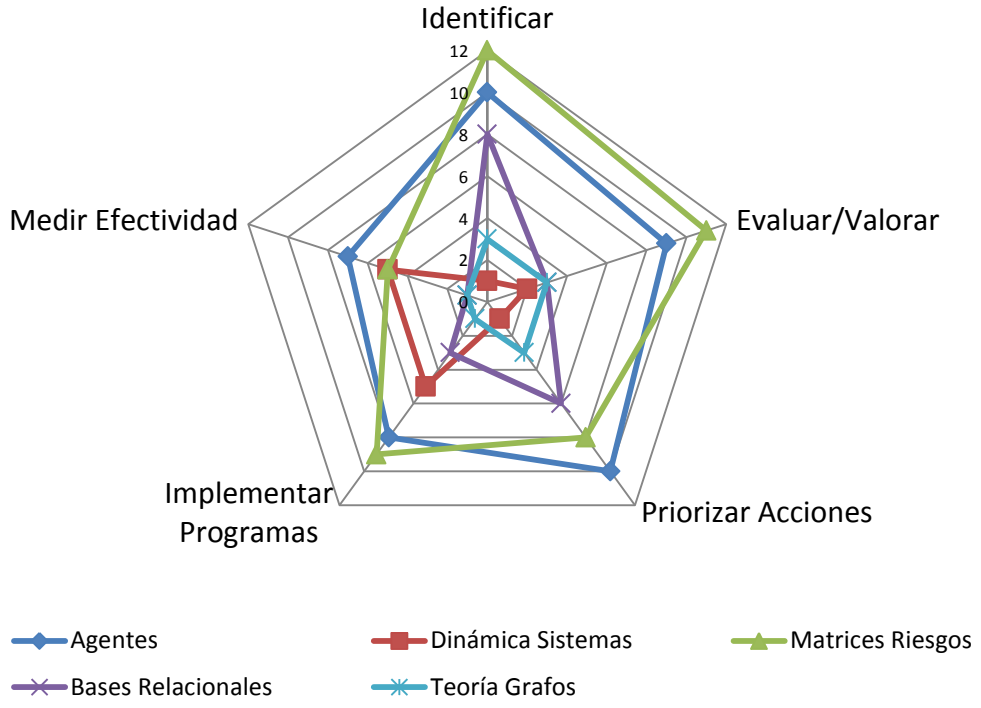


Figura 2.10: Uso de técnicas de modelización en el marco de gestión de riesgos del sector eléctrico.

Existe conciencia de que los riesgos no pueden eliminarse totalmente y que un cierto nivel de riesgo debe ser aceptado por la sociedad. Entre otras cuestiones, se reconoce ahora la necesidad de que las agencias de inteligencia nacionales deben prestar más atención a estos asuntos. Todos los países reconocen la importancia de las alianzas público-privadas y los gobiernos están promoviendo el intercambio de información con el sector privado, ya que la mayoría de la infraestructura eléctrica pertenece o es operada por empresas privadas.

2.3.3.1 Etapa de Identificación de Riesgos

Sobre la base de las metodologías presentadas en la Tabla 2.3 se pueden distinguir las siguientes plataformas computacionales específicamente para la infraestructura eléctrica crítica. Esta clasificación incluye quince aplicaciones basadas en simulación y en modelos analíticos (CASCADE, CEEESA, CIP/DSS, DEW, EMCAS, FAIT, Fort Future, IEISS, IIM, MIA, MUNICIPAL, N-ABLE), y cinco

metodologías de trabajo (HAZOP, teoría grafos, mapas de riesgos, NIPP, Directiva 114/CE).

La mayoría de las aplicaciones se concentran en la identificación de las amenazas no técnicas dentro del sistema de infraestructura eléctrica. Sin embargo, se destaca que seis herramientas de software (50% de los modelos) también permiten identificar riesgos técnicos. En los modelos revisados, nueve herramientas de software (75%) se puede utilizar para identificar los riesgos en un ámbito geográfico local o regional.

En particular, el uso de la teoría de grafos [JOHANSSON, 2010] se convierte en una metodología muy útil para investigar la vulnerabilidad de las redes de distribución eléctrica, así como las interdependencias con otros sistemas de infraestructura crítica. Su aplicación en la *etapa de identificación* debe combinarse con la evaluación de medidas sobre las topologías y de esta manera obtener el listado de activos más vulnerables de una red.

Metodologías como HAZOP requieren un tratamiento cualitativo e inductivo de grupos de expertos. A pesar de su rigor se ven limitados por la necesidad de un estudio exhaustivo de todos los nodos, los circuitos y los activos de la red eléctrica.

Las herramientas más universales de identificación se basan en las metodologías de **mapas de riesgos** [COSO, 2004; ERM Initiative, 2010] que se ajustan a los requisitos de la Directiva 114/CE [CUE, 2008] y el NIPP [NIPP, 2009]. En ese sentido, las metodologías que contienen mapas de riesgos se convierten en una alternativa importante a considerar en el proceso de identificación de las amenazas a los sistemas de infraestructura eléctrica.

2.3.3.2 Etapa de Evaluación de Riesgos

De acuerdo con el marco de gestión de riesgos, este paso consiste en medir el riesgo según su probabilidad de ocurrencia y el impacto de sus consecuencias, de acuerdo con escalas predefinidas para cada recurso. Las decisiones relativas a la evaluación de riesgos pueden resultar en la necesidad de gestionar o ignorar las amenazas.

Existen catorce metodologías de evaluación de riesgo en el sistema eléctrico: diez de ellas corresponden a aplicaciones de software (CASCADE, CEEESA, CIMS, COMM-ASPEN, DEW, EMCAS, FAIT, Fort Future, MIA, Modular Dynamic Model) y cuatro encajan como metodologías analíticas (HAZOP, Teoría Grafos, NIPP, Directiva 114/CE). Casi el 43% de estas herramientas se basan en técnicas de simulación

mediante dinámica de sistemas o mediante agentes, los cuales tienen la conveniencia de evaluar los impactos de las políticas y regulaciones en el sector. Las **matrices de riesgos** son ampliamente aceptadas (30% de los modelos) y son recomendadas en los programas de gestión de riesgos. En particular, esta metodología tiene en cuenta la probabilidad y el impacto del riesgo.

Las técnicas relacionadas con la **teoría de grafos** calculan medidas de centralidad y estadísticas topológicas para determinar la eficiencia de las redes que representan a cada sistema. Aunque su formación matemática es más rigurosa que las demás metodologías, esta técnica se está difundiendo cada vez más, gracias al desarrollo de su soporte teórico y la posibilidad de implementarla a nivel computacional.

Aquellas metodologías que involucran **matrices de calificación** se convierten en una alternativa importante dentro de la etapa de evaluación de riesgos en los sistemas de infraestructura eléctrica. La universalidad de las técnicas basadas en **matrices de calificación** hace que sean incluso adecuadas para la evaluación de políticas.

2.3.3.3 Etapas de priorización de acciones, implementación de programas y medición de efectividad

Dado que las organizaciones toman decisiones una vez que el riesgo ha sido identificado y evaluado, es posible examinar conjuntamente las etapas relacionadas con la aplicación de los procedimientos para reducir la probabilidad de que los riesgos se materialicen, así como la gravedad de sus consecuencias. El uso eficaz de técnicas de simulación mediante dinámica de sistemas y técnicas multi-agente (en combinación con los SIG o con árboles de decisión) se puede aplicar en las etapas de la priorización de acciones, ejecución de programas y medición de la efectividad.

Como se muestra en la Figura 2.10 se han encontrado veintiún herramientas de software (*CEEESA, CI3, CIMS, CIP/DSS, CIPMA, CISIA, COMM-ASPEN, DEW, EMCAS, Fort Future, GoRAF, IEISS, IIM, IntePoint Vu, Knowledge Management & Visualization, Modular Dynamic Model, MUNICIPAL, N-ABLE, NEMO, NSRAM*) y una metodología analítica (*HAZOP*). Todos estos métodos tienen en cuenta las directrices incluidas en NIPP y en la Directiva 114/CE de realizar el establecimiento de prioridades, la implementación de acciones y el seguimiento. A partir de estas herramientas de software, doce (62%) se apoyan en simulaciones (agentes, dinámica de sistemas), lo que permite predecir el comportamiento de la infraestructura crítica, al aplicar decisiones. Las otras ocho técnicas (38%) son métodos relacionales (que

permiten el análisis de las decisiones que deben tomarse en momentos diferentes) y técnicas de evaluación, para apoyar la toma de decisiones en la gestión de amenazas (técnicas multi-criterio).

En este punto, la metodología utilizada por la norma australiana [AS/NZS, 1999], predecesor de la norma ISO 31000 [ISO, 2010] es la que representa con mayor precisión lo que la mayoría de las organizaciones y agencias gubernamentales están haciendo actualmente. Sus características principales incluyen la identificación de interdependencias, la identificación de los nodos de fallo y otros puntos de alta vulnerabilidad, así como estrategias para mitigar el impacto de los riesgos. Esto se complementa con la definición de escenarios, incluidos los desastres naturales y actos de terrorismo, que pueden causar la interrupción del servicio de la infraestructura eléctrica.

2.4 COMENTARIOS AL CAPÍTULO

Se ha realizado una revisión completa de las actuales metodologías, modelos y aplicaciones de simulación en torno a las etapas consideradas en los planes de protección de infraestructuras críticas, las cuales se pueden adaptar a un marco de gestión de riesgos. De esta manera, ha sido posible dar cumplimiento a los objetivos propuestos al inicio del capítulo.

Las estrategias de modelización en infraestructuras críticas se asocian principalmente con las técnicas de simulación de: sistemas multi-agentes, dinámica de sistemas, teoría de grafos y bases de datos relacionales. En este contexto, el paradigma de simulación que involucra sistemas multi-agentes y dinámica de sistemas tiene mayor aplicabilidad en el análisis de interdependencias entre las diferentes infraestructuras críticas, la predicción de respuestas de estos sistemas en situaciones de emergencia y análisis de la aplicación de políticas y regulaciones en los respectivos sectores.

Las matrices de calificación suelen combinarse con técnicas de gestión de riesgos para aplicar evaluaciones semicuantitativas y también para realizar análisis de sensibilidad en la toma de decisiones. Así mismo, las aplicaciones que combinan los modelos de bases de datos relacionales (que contienen información sobre la identificación de activos) con la teoría de grafos constituyen otra línea de investigación, con la finalidad de identificar aquellos nodos más críticos en la infraestructura y priorizar la protección de los mismos.

Un importante esfuerzo de las investigaciones revisadas está centrado en la identificación y evaluación de riesgos para las infraestructuras eléctricas, donde se reconoce la universalidad y practicidad de los métodos asociados a los mapas de riesgos y a las matrices de calificación. Por su parte, las técnicas asociadas al paradigma de simulación se utilizan especialmente en la toma de decisiones en las etapas de priorización de acciones, implementación de programas y medición de la efectividad, con la finalidad de estimar cuán eficaces son las estrategias de mitigación de riesgos y los planes de protección de las infraestructuras eléctricas.

3 IDENTIFICACIÓN DE RIESGOS EN INFRAESTRUCTURAS CRÍTICAS

En este capítulo se realiza la propuesta original de una metodología de identificación de riesgos, aplicable a la planificación de la seguridad en las infraestructuras eléctricas, considerando las amenazas técnicas y no técnicas. Esta metodología tiene el potencial de ser aplicable tanto a la red de infraestructura, como a las organizaciones propietarias y/o gestoras del sistema de infraestructura. Para el efecto, se parte del concepto de identificación de amenazas, enmarcado dentro de las metodologías de gestión del riesgo. Así mismo, se presenta una aplicación de la propuesta metodológica de mapas interconectados de riesgos para un caso real en una región o país.

3.1 OBJETIVO DEL CAPÍTULO

En este capítulo se desarrolla una estrategia metodológica para la **identificación de amenazas** en un sistema de infraestructura crítica. De esta manera, se pretende cubrir la definición y aplicación de los siguientes aspectos:

- Asociar la identificación de amenazas a los planes de protección de infraestructuras, a partir de su definición y de su propósito dentro de un esquema de gestión de riesgos.
- Estudiar el estado del arte en cuanto a metodologías y técnicas aceptadas para la identificación de riesgos en sistemas de infraestructuras críticas. Incluye el análisis de herramientas de software y metodologías de protección de infraestructuras críticas.
- Justificar el uso de las metodologías cualitativas para generalizar el proceso de identificación de riesgos en el sistema de infraestructura.

Este proceso de identificación permite obtener un listado completo de los posibles riesgos y sus componentes. Sin embargo, aunque no es posible identificar absolutamente todos los riesgos posibles, lo que se persigue es identificar las probables contribuciones a los desequilibrios y perturbaciones en un sistema, para determinar posteriormente cuáles tienen mayor impacto en la red y cuáles tienen mayor probabilidad de ocurrencia.

Así, los resultados obtenidos mediante la identificación de riesgos constituyen el insumo para la posterior utilización de metodologías de evaluación de riesgos.

3.2 HERRAMIENTAS DE SOFTWARE Y METODOLOGÍAS PARA IDENTIFICACIÓN DE RIESGOS

La identificación de riesgos, más que una técnica, es una de las etapas del marco de la gestión de riesgos. Este marco se inicia con la etapa de establecimiento de objetivos, continúa con la identificación de riesgos y sigue con la valoración e implementación de acciones para mitigarlos, según el esquema presentado en la Figura 3.1.

En un marco de gestión de riesgos, la *etapa de identificación* se enfoca en detectar **cuáles son las fuentes principales de riesgo** [ICONTEC, 2004; ISO, 2010]. Corresponde a la etapa en la que se definen los riesgos del sistema de infraestructura crítica para su posterior evaluación [NIPP, 2009]. Para clasificar los riesgos es necesario entender que la *etapa de identificación* es un proceso iterativo porque

pueden descubrirse nuevos riesgos en la medida que discurre el ciclo de vida del sistema de infraestructura [CCN Criptología, 2010]. La frecuencia de la iteración y quién participará en cada ciclo variará de un caso a otro.

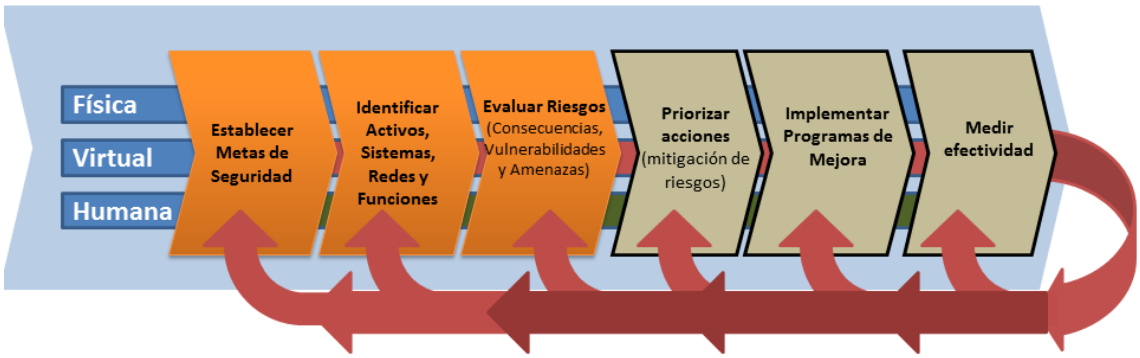


Figura 3.1: Marco de gestión de riesgos [NIPP, 2009].

El proceso de identificación suele realizarse habitualmente mediante un *análisis cualitativo de riesgos*. En algunas ocasiones, la identificación de un riesgo permite deducir sus consecuencias y esto debe registrarse para realizar otros análisis y para su implementación en el proceso de planificación de la respuesta ante las amenazas detectadas.

En resumen, el propósito al realizar el proceso de identificación de riesgos se limita a un ejercicio cualitativo, mediante el cual se obtiene la definición de los posibles riesgos en el sistema, la generación del listado de riesgos y sus componentes y la descripción de sus peculiaridades. La posterior representación de estos riesgos se podrá realizar mediante una herramienta de software (como las presentadas en los modelos de la Tabla 2.3) o con la ayuda de una metodología (por ejemplo, mediante el uso de mapas de riesgos).

Bajo el enfoque de los esquemas de gestión de riesgos, en la etapa de *identificación* se pretende precisar los posibles eventos que afecten los recursos o desvíen el logro de los objetivos de funcionamiento del sistema de infraestructura.

Una forma útil de estudio de estas amenazas es una clasificación en ***Amenazas Técnicas*** y ***No Técnicas*** [YUSTA, 2008]. Las primeras se refieren a fallos técnicos y humanos internos que afecten al funcionamiento de los sistemas de producción, transporte, distribución y comercialización de energía, actividades apoyadas en las instalaciones de infraestructura energética. Las segundas están relacionadas con aspectos financieros, fenómenos naturales o incluso ataques deliberados a la infraestructura.

En este punto también es importante anotar la clasificación que hacen tanto el Consejo Europeo, a través de la Directiva 114/CE [CUE, 2008] y el Departamento de Seguridad Nacional de EEUU a través del NIPP [NIPP, 2009] y de la Directiva 7 [US Dept Home Security, 2003] facilitando algunas pautas para clasificar la infraestructura crítica y los recursos claves, de conformidad con su impacto en la economía y en la seguridad nacional de los estados.

La revisión de herramientas y metodologías para la etapa de identificación de riesgos se centra específicamente en los sistemas de infraestructuras eléctricas. Esto se efectúa a partir de la revisión del estado del arte en metodologías para protección de infraestructuras críticas presentada previamente en la Tabla 2.3 del capítulo 2 de esta tesis.

3.2.1 ANÁLISIS DE HERRAMIENTAS Y METODOLOGÍAS

Las plataformas relacionadas en la revisión del estado del arte, dirigidas específicamente a la etapa de **identificación de riesgos** en infraestructuras eléctricas, se presentan en la Tabla 3.1.

Esta clasificación hace referencia a 12 modelos fundamentados en el paradigma de simulación (*CASCADE, CEEESA, CIP/DSS, DEW, EMCAS, FAIT, Fort Future, IEISS, IIM, MIA, MUNICIPAL, N-ABLE*). Adicionalmente existen cinco estrategias de tipo metodológico (*HAZOP, Teoría Grafos, Mapas de Riesgos, NIPP, Directiva 114/CE*. En la Tabla 3.1 se realiza un análisis de fortalezas y debilidades para cada una de las herramientas y metodologías revisadas.

Tabla 3.1: Herramientas y metodologías para la Identificación de Riesgos en Infraestructuras Eléctricas.

Herramienta / Metodología	Objetivo de Identificación	Resultado Esperado	Fortaleza	Debilidad
CASCADE	Discontinuidad del servicio eléctrico: Blackouts masivos	Localización de los Nodos Eléctricos Principales	Modelos probabilísticos, que tienen en cuenta la complejidad de la red.	Imposibilidad de identificar la topología de la red, sólo se limita a fallos técnicos.
CEEESA	Relación de los sistemas de gas con el mapa energético nacional.	Datos de los modelos energéticos nacionales (Estructura Sistema Energético, Flujo Energético, Precios de la Energía, Proyección de la demanda, Políticas y regulaciones, Proyección de emisiones)	Identificación de infraestructuras locales, ramas de aislamiento, nodos críticos, versatilidad de la infraestructura y de las compañías de gas. Se puede asociar con otras herramientas	Exigencia de disponibilidad de datos precisos y constantemente actualizados. Enfoque en sistemas de redes de gas. No se estudian emergencias.

Herramienta / Metodología	Objetivo de Identificación	Resultado Esperado	Fortaleza	Debilidad
CIP/DSS	Relaciones dinámicas entre cada uno de los componentes del sistema de infraestructura. Métricas relacionadas con datos históricos, incidentes, consecuencias, vulnerabilidades, amenazas.	Consecuencias de los ataques a la red, en términos de seguridad nacional, impacto económico, salud pública, gobernabilidad y efectos en otras infraestructuras.	Resultados a largo plazo, con datos básicos de la red. Interdependencia con otros sectores económicos y de respuesta de emergencias (Salud, regulaciones, etc).	Dificultad para identificar métricas e indicadores. Enfoque principal en pérdidas económicas. Complejidad en introducción de datos a la herramienta.
DEW	Modelos estadísticos para análisis de apagones en cascada. Depende del tiempo y la localización de los circuitos de potencia involucrados	Activos se salen de servicio debido un fallo. En presencia de restricciones, se identifican las cargas de alta prioridad y la estrategia para reconfigurar el despacho	Incorporación de toda la red de distribución de subestaciones. Aplicable a modelos multidisciplinarios con la cadena de valor. Maximización en el uso de todas las fuentes de datos disponibles	Aplicable a modelos sencillos, con baja complejidad. Requerimiento de datos precisos para garantizar funcionamiento.
EMCAS	Representaciones gráficas de nodos y enlaces, que pueden llegar a los cientos de miles de conexiones, dependiendo de la cantidad de datos disponibles	Determinación de la mejor estrategia de despacho, en caso de existir restricciones. Aplicable especialmente a la red de potencia y el mercado de energía.	Aplicable a modelos complejos. Identificación de todos los nodos y conexiones en el sistema.	Alto nivel de entrenamiento para introducir datos. Datos precisos en cada nodo.
FAIT	Definición de interdependencias a partir de conocimiento experto. La identificación de estas interdependencias se realiza gráficamente y se apoya con mapas	Asociación dinámica de los datos y creación de reglas de funcionamiento del sistema. Se identifican aquellas infraestructuras que pueden proporcionar la mayor continuidad del servicio en caso de manifestarse restricciones o amenazas.	Información se recopila a través de metadatos, y mediante integración con buscadores virtuales, lo cual facilita la identificación de riesgos en escenarios de poca información	Modelo limitado, especificado en Entradas/Salidas
Fort Future	Capacidad de las instalaciones militares, según el objetivo para el que se proyecten	Aplicaciones en la construcción y mantenimiento de bases militares, con todos sus servicios adicionales	Amplio apoyo en información virtual. Métricas se definen automáticamente según los riesgos que se vayan identificando en la red.	Modelo no disponible para aplicaciones civiles.
HAZOP	Los riesgos, los accidentes o los problemas de operatividad, se producen como consecuencia de una desviación de las variables de proceso con respecto a los parámetros normales de operación en un sistema dado y en una etapa determinada	Se delimitan las áreas a las cuales se aplica la técnica, mediante una serie de subsistemas o líneas. Se identifican una serie de nodos o puntos claramente localizadas en la red eléctrica	Amplio conocimiento en la industria. Se enfoca en el conocimiento experto para identificar riesgos. Permite actualización de la identificación. Plataformas de software disponibles.	Técnicas exhaustivas, con conocimientos muy especializados. Alta dedicación para el mantenimiento de las variables identificadas.
IEISS	Datos que permiten alimentar los modelos de simulación, como las áreas que se impactan, la duración de los apagones, componentes críticos, estrategias de restauración, opciones de mitigación	Estos análisis permiten determinar la capacidad de la red para proporcionar el servicio energético, en presencia de cortes en la red.	Capacidad de manejo en infraestructuras de energía eléctrica de la generación de energía y transporte.	Requerimiento de abundancia de información a partir de bases de datos, herramientas de análisis. Enfoque sólo en riesgos técnicos de operación.
IIM	Definición de métricas que desde el punto de vista del negocio, permitan realizar la mejor toma de decisiones, vista desde diferentes jerarquías y perspectivas	Se estiman los efectos en regiones y sectores afectadas	Formulación de indicadores integrados en infraestructuras eléctricas. Estudio vertical en varios sectores de infraestructuras.	Dificultad para determinar métricas en la identificación de riesgos. Modelo limitado, especificado en Entradas/Salidas
TEORÍA GRAFOS	Ubicación estratégica de nodos principales del sistema	Análisis de interconexiones entre nodos. Topología de la red eléctrica	Representación de la infraestructura mediante grafos. Sólo se necesita conocer la topología del sistema	Resultados aproximados, que no necesariamente coinciden con contingencias eléctricas

Herramienta / Metodología	Objetivo de Identificación	Resultado Esperado	Fortaleza	Debilidad
MAPAS DE RIESGOS	Realización de la combinación de los elementos más relevantes y aplicables a la realidad de las empresas que poseen y que operan los activos de las redes eléctricas, encontrados en las metodologías de gestión del riesgo.	Planificar, organizar, dirigir y controlar los recursos necesarios para mitigar los efectos adversos que puedan afectar el logro de los propósitos empresariales desde la perspectiva estratégica, organizacional o del entorno	Amplia difusión en organizaciones energéticas. Ideal para identificar riesgos, mediante herramientas disponibles.	Falta la formulación de métricas e indicadores en la identificación de riesgos.
MIA	Realización de mapeos, enlaces y fronteras. Particularmente se busca determinar las relaciones entre las capas físicas y lógicas de las redes	Un enfoque particular depende de las interdependencias en las redes eléctricas.	Identificación de métricas y topologías en interrelaciones funcionales entre las infraestructuras eléctricas y TIC. Metodologías analíticas para la identificación de riesgos.	Falta de intercambio de información, debido a las limitaciones de confidencialidad o las dificultades reales en su adquisición
MUNICIPAL	Base de conocimientos de expertos y de administradores del sistema. Se identifica la interdependencia entre los sectores.	Las soluciones más factibles pueden realizarse dentro de unas restricciones en un entorno urbano	Combinación bases de datos y SIG. Capacidad para identificar diferentes configuraciones, muy útil en la identificación de riesgos dentro de una cadena de valor.	La información requerida por el sistema usualmente es confidencial.
N-ABLE	Se identifican las áreas e industrias que más se afectan por la interrupción del sistema de infraestructura. Prolongación de la recuperación económica, restricciones, estabilidad, estrategias de mitigación.	Se modelan los impactos microeconómicos de las interrupciones debidas a fenómenos naturales, o como consecuencia de acciones del hombre	Arquitectura de datos que permite identificar alarmar en las políticas de empresas, los compañías y sistema de infraestructura	Aplicable al sector de infraestructura eléctrica, pero los datos para su ejecución son limitados
NIPP	Primera parte de la metodología de análisis de riesgos. Requisito previo para continuar con la evaluación de amenazas	Activos, sectores, sistemas y funciones de las infraestructuras críticas. Se registran activos críticos en el funcionamiento de la sociedad	Cualquier metodología es válida para recopilar información en la identificación de riesgos. Enfatizando en aquellos activos que afecten la economía y la seguridad nacional.	No existe un planteamiento metodológico con fundamentación matemática. La identificación de riesgos se realiza en un entorno geopolítico. Mayor enfoque en riesgos no técnicos.
PEPIC (Directiva 2008/114/CE)	Énfasis en medidas de seguridad permanentes, que identifican las inversiones y medidas técnicas, medidas organizativas, control verificación, comunicación, concienciación y formación, en función de los diferentes niveles de riesgo y de amenaza.	Número de víctimas (mortales o heridos); impacto económico y medioambiental; Impacto público (confianza de la población, sufrimiento físico y alteración de la vida cotidiana,).	Para las infraestructuras que prestan servicios esenciales, se tendrán en cuenta la disponibilidad de alternativas y la duración de la perturbación o recuperación.	No existe un planteamiento metodológico con fundamentación matemática. La identificación de riesgos se realiza en un entorno geopolítico. Mayor enfoque en riesgos no técnicos

Las herramientas y metodologías de la etapa de identificación permiten obtener información acerca de los activos y de las interdependencias, para una posterior valoración del impacto que para el sistema de infraestructura puede suponer la pérdida de los mismos. Los resultados obtenidos pueden influir en la estrategia de protección de la infraestructura (por ejemplo mediante cambios en la política de seguridad) y en la realización de mejoras concretas.

3.2.2 CLASIFICACIÓN DE HERRAMIENTAS Y METODOLOGÍAS

Con la finalidad de profundizar en el análisis más detallado de las técnicas a las que hace referencia, se puede apreciar en la Tabla 3.2 el resumen de las características empleadas por cada uno de los modelos de análisis de vulnerabilidad de infraestructuras críticas en el sector eléctrico. Los criterios de clasificación incluidos en la Tabla 3.2 proporcionan la descripción de cada herramienta, incluyendo su origen, las técnicas en las que se apoya su elaboración y el alcance de su aplicación en la etapa de identificación de riesgos, en el sector de las infraestructuras eléctricas. Los criterios de clasificación comprenden:

- **Origen**: En la Tabla 3.2 se indica cuáles de las herramientas y metodologías están fundamentadas en **propuestas metodológicas**. Éstas constituyen el fundamento para el desarrollo de otras herramientas más específicas. Las **herramientas de software** citadas en la tabla se soportan generalmente en el paradigma de simulación (dinámica de sistemas, sistemas multiagente, etc) o en formulaciones analíticas clásicas (flujos de carga, probabilidades, etc).
- **Tipo de Riesgos**: Las herramientas y metodologías citadas permiten estudiar los riesgos identificados de tipo técnico (asociados a la operación y mantenimiento de la red) o de tipo no-técnico (asociados a la administración, al entorno, políticas, etc).
- **Jurisdicción**: En general, las herramientas y metodologías se pueden aplicar a entornos globales o locales, según el caso.
- **Recolección de datos**: Para realizar el proceso de identificación de riesgos cada herramienta y metodología utiliza algunas de las técnicas de obtención de información que se detallan más adelante en la sección 3.2.3.
- **Enfoque**: El proceso de identificación se concentra en lugares específicos de las infraestructuras, en sus activos, en su interrelación con otras infraestructuras, o en su relación con el funcionamiento de otros servicios e infraestructuras.

Tabla 3.2: Clasificación de herramientas y metodologías para identificación de riesgos en infraestructuras eléctricas

CRITERIO DE CLASIFICACIÓN		CASCADE	CEESA	CIP/DSS	DEW	EMCAS	FAIT	Fort Future	HAZOP	IEISS	IIM	TEORÍA GRAFO	MIA	MUNICIPAL	N-ABLE	MAPAS RIESGO	NIPP	Directiva 114/CE
PROPUESTA METODOLÓGICA									●			●				●	●	●
HERRAMIENTA SOFTWARE	PARADIGMA DE SIMULACIÓN		●	●		●		●		●	●				●			
	MODELO ANALÍTICO	●			●		●						●	●				
RIESGOS TÉCNICOS	ESTABILIDAD RED ELÉCTRICA				●			●		●								
	FALLOS EN CASCADA	●			●					●						●		
	ESTRATEGIAS RECONFIGURACIÓN				●	●						●			●	●		
	FALLOS EQUIPOS					●				●	●		●			●		
	PERTURBACIONES	●			●					●					●	●		
	TECNOLOGÍAS DE INFORMACIÓN							●			●		●			●	●	●
	ERRORES HUMANOS							●	●			●	●		●	●	●	●
RIESGOS NO TÉCNICOS	ÁREAS GEOGRÁFICAS		●	●			●	●			●	●	●	●	●	●	●	●
	CRECIMIENTO RED		●					●	●							●		
	TERRORISMO, VANDALISMO							●				●			●	●	●	●
	FENÓMENOS NATURALES						●	●				●		●	●	●	●	●
	POLÍTICAS, REGULACIONES			●											●	●	●	●
	RED CADENA DE VALOR		●				●	●	●	●	●	●	●	●		●	●	●
	ADMINISTRACIÓN, FINANZAS, MERCADO					●					●					●	●	●
JURISDICCIÓN	REGIONAL	●	●	●	●		●	●	●	●		●	●	●		●	●	●
	NACIONAL					●					●				●	●	●	●
	INFRAESTRUCTURA VIRTUAL						●				●		●				●	●
RECOLECCIÓN DATOS	INVENTARIOS ACTIVOS					●			●		●	●	●				●	●
	GEORREFERENCIACIÓN		●			●								●				
	CONFIGURACIÓN DE LA RED	●	●		●	●		●	●	●		●	●	●	●	●	●	●
	FUENTES HUMANAS			●				●	●		●	●	●	●	●	●	●	●
	RECURSOS VIRTUALES						●	●						●		●	●	●
ENFOQUE DE LA IDENTIFICACIÓN	ACTIVOS, EDIFICIOS, EQUIPOS, SEDES					●			●			●		●		●	●	●
	PLANTAS GENERACIÓN					●		●	●	●	●	●	●			●	●	●
	TRANSPORTE/DISTRIBUCIÓN				●	●		●	●	●	●	●	●	●		●	●	●
	INTERDEPENDENCIAS	●		●		●	●		●	●	●	●	●	●	●	●	●	●
	NODOS CRÍTICOS	●	●		●	●		●	●	●		●	●	●	●	●	●	●
	MEJORAS EN REGULACIONES					●									●	●	●	●
	IMPACTO EN LA POBLACIÓN			●				●	●		●			●		●	●	●

La mayoría de las aplicaciones se enfocan en la identificación de amenazas no técnicas al sistema de infraestructura eléctrica. Sin embargo, se resalta que seis

herramientas de software (50% de las plataformas) tienen aplicación en la identificación de riesgos técnicos y no técnicos. Por su parte, las cinco metodologías analizadas tienen la posibilidad de identificar tanto **riesgos técnicos** como **no técnicos**, según puede verificarse en la Figura 3.2.

De los modelos revisados, nueve herramientas de software (75%) permiten identificar riesgos en un alcance geográfico local o regional (las demás tienen alcance geográfico nacional y/o redes virtuales). Adicionalmente, las cinco metodologías expuestas son universales y permiten identificar riesgos a nivel regional y nacional.

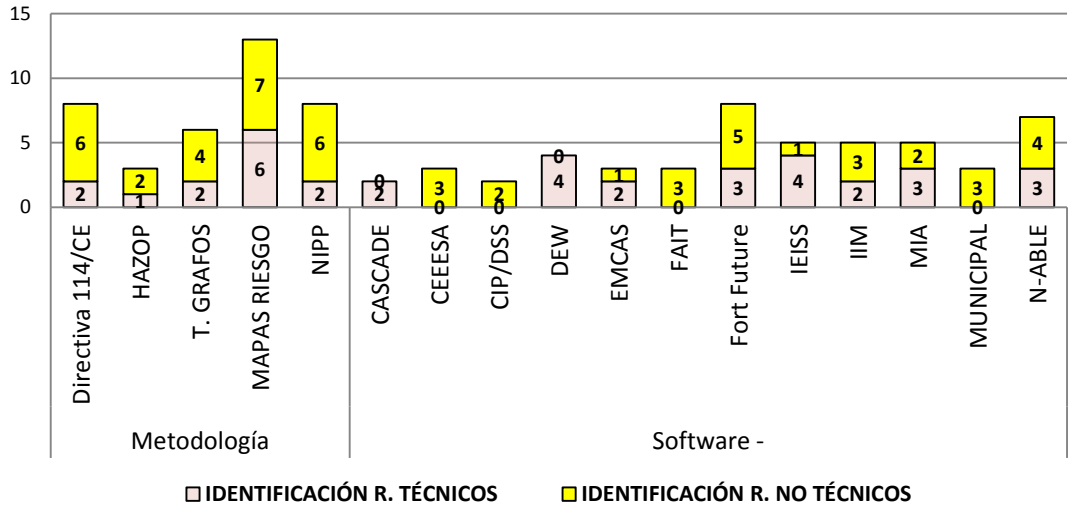


Figura 3.2: Aplicación de las herramientas y metodologías para la identificación de riesgos.

La identificación de riesgos en cada una de las herramientas y metodologías se alinea con la cadena de valor del sistema de infraestructura, con especial énfasis en la prevención de amenazas sobre los siguientes aspectos:

- Activos, edificios, equipos y sedes de las empresas propietarias/operadoras de la infraestructura eléctrica;
- Plantas de generación eléctrica;
- Redes de transporte y de distribución;
- Interdependencias con otros sectores de infraestructura crítica;
- Nodos críticos de la red eléctrica;
- Regulaciones y políticas que impactan la operación del sistema;
- Impacto sobre la población afectada.

La **propuesta metodológica** HAZOP exige un tratamiento inductivo y cualitativo con paneles de expertos, con la finalidad de realizar estudios exhaustivos sobre cada uno de los nodos que conforman el sistema de infraestructura. Se procura identificar la mayor cantidad de riesgos posible, así como las medidas de control.

Las metodologías asociadas a **teoría de grafos** [HOLMGREN, 2006; JOHANSSON, 2010] son útiles para determinar la vulnerabilidad en sistemas eléctricos, así como su interdependencia con otros sistemas de infraestructura crítica. Las medidas estadísticas obtenidas a partir del grafo, constituyen el principal indicador para la posterior calificación de los riesgos.

Por otro lado, las **herramientas de software** que se pueden aplicar para la identificación de riesgos tienen aplicaciones muy particulares. Así por ejemplo, las aplicaciones de IEISS, CASCADE, DEW, EMCAS tienen mayor validez para el estudio de los fallos en cascada; la gestión de emergencias en jurisdicciones regionales se puede abordar mediante el CEESA, CIP/DSS, MUNICIPAL, N-ABLE. Los modelos de entrada/salida como FAIT, IEISS, MIA, IIM, EMCAS permiten analizar interdependencias en regiones específicas para planificar la toma de decisiones en casos de emergencias. Aplicaciones particulares de CEESA, IIM y Fort-Future se orientan al estudio de la cadena de suministro de combustible para plantas de generación.

Sin embargo, en la Tabla 3.2 destaca la universalidad de las metodologías de **mapas de riesgos**, así como el conjunto de indicaciones establecidas en la Directiva 114/CE y en el NIPP. En ese sentido, las metodologías que involucran los mapas de riesgos se convierten en una importante alternativa a tener en cuenta en el proceso de identificación de amenazas al sistema de infraestructura eléctrico, fortaleza que se había indicado previamente en la Tabla 3.1. Cabe anotar que la identificación de estos riesgos debe realizarse con profundidad para ofrecer la mejor descripción posible de los mismos.

3.2.3 ESTRATEGIAS DE RECOLECCIÓN DE DATOS

En la Figura 3.3 se presenta un resumen práctico de herramientas y metodologías que permiten recopilar estructuradamente datos para la identificación de riesgos en la infraestructura eléctrica.

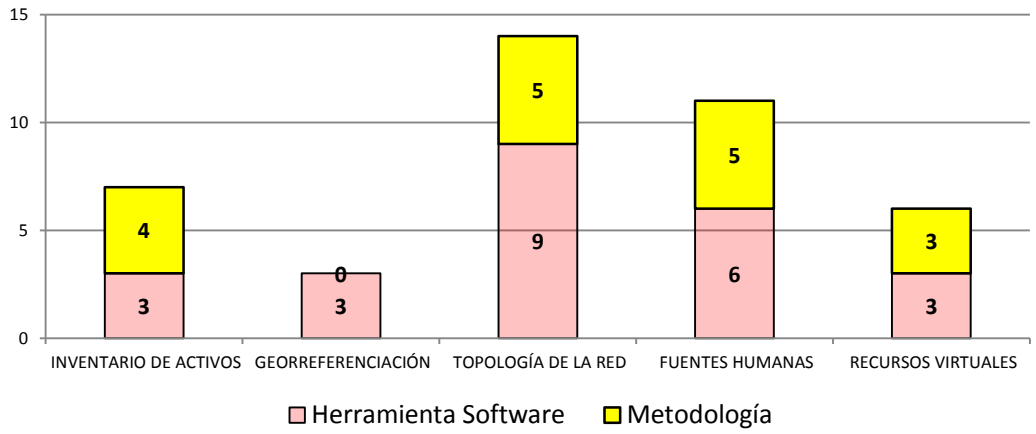


Figura 3.3: Uso de técnicas de recolección de datos para identificación de riesgos.

La información resumida en la Figura 3.3 se ha obtenido a partir del análisis de la información registrada en la Tabla 3.1 y en la Tabla 3.2. Se desglosan a continuación las cinco estrategias de recolección de datos consideradas en la revisión de herramientas y metodologías.

Fuentes Humanas

Probablemente constituya la más importante técnica de recopilación de información para identificación de riesgos. Se refiere a todas aquellas técnicas que consideran la participación de equipos de expertos, con quienes se pueden obtener una lista completa de riesgos. Estas técnicas comprenden [LÓPEZ & ARBOLEDA, 2010]:

- **Entrevistas**. Las técnicas de entrevista se usan para determinar la existencia de riesgos en áreas específicas de la infraestructura, y posteriormente cuantificar la probabilidad y el impacto de los riesgos.
- **Tormenta de ideas**: Se generan ideas acerca de los riesgos del proyecto bajo el liderazgo de un facilitador. Los riesgos son identificados y categorizados por tipo de riesgo y sus definiciones son refinadas dentro del mapa de riesgos que se explica en la sección 3.3.
- **Revisiones de Documentación**: Se puede realizar una revisión estructurada de la documentación disponible, incluidos planes y archivos de proyectos. La información publicada, incluidas las bases de datos comerciales, estudios académicos, estudios comparativos de la industria, también pueden ser útiles para la identificación de riesgos.

- **Técnicas Delphi**: Su objetivo es la consecución de un consenso basado en la discusión entre expertos. Este proceso repetitivo se basa en la elaboración de un cuestionario que ha de ser contestado por expertos. Las personas que participan en estos cuestionarios son conocedores objetivos en el tema de identificación y valoración de riesgos, para evitar la aparición de sesgos en la información obtenida.

Georreferenciación

Se refiere a los datos de coordenadas y datos determinados, utilizado frecuentemente en los sistemas de información geográfica. Los datos que alimentan las herramientas de software permiten identificar riesgos en la medida que sitúan en una región las posibles amenazas técnicas y no técnicas. Algunas características de esta información georreferenciada consiste en [PEGGION, BERNARDINI *et al.*, 2008]:

- Datos de alta resolución sobre demografía y activos económicos
- Identificación de áreas geográficas con mayor impacto de los fenómenos naturales y riesgos de desastres, los cuales incluyen peligros geológicos (Catálogo de acontecimientos históricos, superficie de ruptura de fallas geológicas, Mapas de actividad sísmica, mapas de peligro de derrumbes, mapas con fuentes potenciales de deslizamientos de tierra), peligros hidrometeorológicos: (Mapas de llanuras aluviales, cartografía de la cubierta vegetativa, mapas de ruta de los ciclones y huracanes tropicales), zonificación costera, tipología del suelo, distribución de la temperatura y del viento
- Resultados de simulaciones geográficas y físicas sobre el alcance, frecuencia e impacto de las amenazas, en especial en relación con fenómenos naturales.

Inventario de Activos

En todas las metodologías de análisis de riesgo se hace un importante énfasis en la construcción de un inventario de activos de infraestructura física constantemente actualizado, que incluya, además de los bienes materiales, también los componentes humanos y los sistemas de información. Este inventario debe proporcionar información sobre el estado de cada elemento de la infraestructura, sus programas de mantenimiento, costes, rutinas de operación, redes similares, lecciones aprendidas etc.

Topología de la red

Es una de las técnicas más ampliamente utilizada, especialmente para la identificación de riesgos técnicos en el sistema de infraestructura. La configuración de

la red eléctrica permite identificar los puntos más estratégicos de la misma, los nodos y enlaces más críticos.

La información de la topología permite aplicar técnicas numéricas, relacionadas con la operación de la red (flujos de carga, análisis de contingencias, despacho óptimo, etc) y realizar identificación puntual de posibles vulnerabilidades técnicas.

Recursos Virtuales

La información que se puede obtener se fundamenta en metabúsquedas en internet, buscadores virtuales e información contenida en medios electrónicos, con la finalidad de elaborar bases de datos con información de activos, configuraciones, referencias geográficas, etc. para la identificación de riesgos.

3.3 PROPUESTA METODOLÓGICA PARA IDENTIFICACIÓN DE RIESGOS

Una de las técnicas que sirve como punto de partida para la realización de un enfoque integral más completo en el análisis de vulnerabilidad de un sistema de infraestructura son los **mapas de riesgos** [AON, 2010; WEFORUM, 2010; YUSTA, CORREA *et al.*, 2011]. Esta técnica permite descubrir y analizar las amenazas a las que están expuestas las infraestructuras.

A partir del mapa de riesgos se construye el inventario de componentes de riesgo, asociados tanto a la red eléctrica como al entorno de la organización que la gestiona. De esta manera, los mapas de riesgos se convierten en una alternativa para el proceso de identificación de amenazas a las infraestructuras, al tiempo que se adaptan a los requisitos formulados en los programas PIC [CUE, 2008; NIPP, 2009].

En las siguientes subsecciones se proporciona una justificación sobre la elección de la metodología de mapa de riesgos y sus conceptos básicos que soportan la construcción de una propuesta original para identificación de riesgos.

3.3.1 JUSTIFICACIÓN DE LA PROPUESTA DE UTILIZACIÓN DE MAPAS DE RIESGOS

Los **mapas de riesgos** se elaboran a partir de un concepto global, aplicable tanto a las organizaciones propietarias y gestoras de las redes eléctricas, como a las infraestructuras en sí. Permiten la identificación de los incidentes que ocurren de forma interna o externa a un sistema de infraestructura crítica. Contienen información cualitativa que describe los riesgos y permiten simplificar la cantidad de categorías en

que se agrupan las componentes que caracterizan cada riesgo, por ejemplo, de tipo técnicos o no-técnicos, a la vez que facilitan una mejor representación de las interrelaciones entre los riesgos.

La revisión de las diferentes herramientas y metodologías presentadas en la Tabla 3.1 y en la Tabla 3.2 evidencian la aceptación de esta técnica, así como la universalidad de la misma en el ámbito de las infraestructuras eléctricas, por las siguientes razones:

- La técnica de mapas de riesgos permite descubrir y analizar las amenazas a los que están expuestos los activos del sistema de infraestructura. A partir del mapa de riesgos se construye un listado detallado de componentes de cada riesgo.
- La técnica es aplicable en cada uno de los sectores identificados como infraestructura crítica: redes eléctricas, de comunicaciones, instalaciones estratégicas, agua potable y plantas tratamiento, sistemas de transporte, etc.
- El mapa de riesgos permite clasificar y categorizar cada uno de los riesgos, para su posterior administración.
- Permite realizar el ejercicio de identificación de riesgos de tipo técnico y no-técnico de manera específica en cada uno de los activos del sistema, o de manera global sobre todo el sistema.
- Admite la recogida de información de fuentes humanas o mediante documentación disponible.
- La técnica permite identificar riesgos en toda la cadena de valor del sistema de infraestructura, incluyendo los subsistemas de generación, transporte y distribución. Adicionalmente, permite identificar aquellos activos más críticos de la red.
- El mapa de riesgos es un método cualitativo que admite la posterior valoración semicuantitativa de los riesgos identificados, necesaria para el proceso de evaluación de amenazas.
- Se puede combinar con otras propuestas metodológicas como HAZOP, o con las estrategias de gestión especificadas en la Directiva 114/CE y el NIPP.

Algunos aspectos que no pueden ser cubiertos mediante los mapas de riesgos incluyen las siguientes particularidades:

- Tratándose de una herramienta de descripción cualitativa, no existen modelos matemáticos para calcular métricas del estado de las diferentes condiciones del sistema a partir del mapa de riesgos.
- La metodología no se ha modelado mediante herramientas de software.
- Los mapas de riesgo sólo se pueden aplicar a la etapa de identificación. Aunque sus resultados sí pueden utilizarse en las etapas subsiguientes del ciclo de gestión de riesgos (evaluación, priorización, mejora continua).
- La técnica de mapas de riesgo es muy intuitivita y global, por cuya razón, en la medida que la etapa de identificación requiera datos precisos, la técnica será insuficiente y debe combinarse con otras metodologías que permitan procesar dicha información.
- Para la construcción de un mapa de riesgos es indispensable recoger y gestionar gran cantidad de información, dificultada la mayor parte de las veces por la inexistencia, la inaccesibilidad y la falta de fiabilidad de muchos de los datos necesarios.

3.3.2 PROCEDIMIENTO PARA LA CARACTERIZACIÓN DE RIESGOS

Existe una percepción hacia los riesgos, ya sea por su relación con las amenazas o por las oportunidades de mejorar las posibilidades de éxito en la protección del sistema. Los riesgos que son amenazas para la red de infraestructura crítica pueden ser aceptados si el riesgo está en equilibrio con el beneficio que puede ser obtenido al tomarlo.

Para cada ***riesgo*** se pueden identificar sus ***componentes***, los cuales se definen como *riesgos en sí mismos* a un mayor nivel de detalle. Dichos componentes se refieren de una manera más explícita a las causas o formas en que pueden materializarse los riesgos [AS/NZS, 1999].

Para facilitar la comprensión del procedimiento de identificación de riesgos, en esta tesis se propone relacionar riesgos, componentes y acciones sobre el sistema de infraestructura eléctrica, según se ilustra en la Figura 3.4.

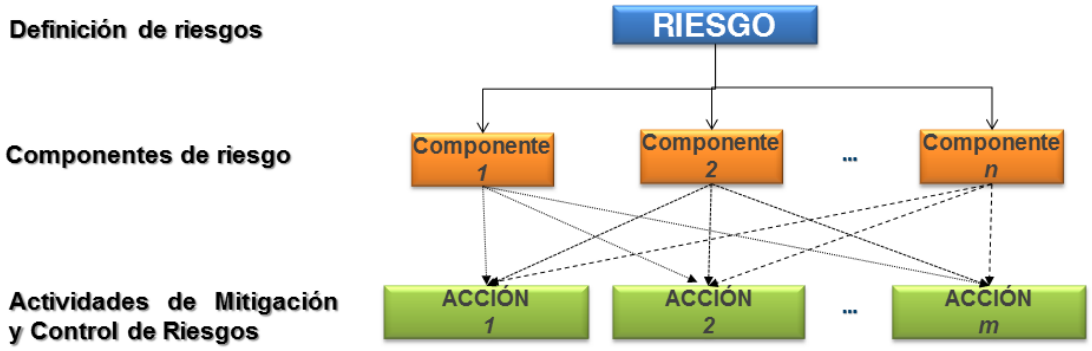


Figura 3.4: Relación entre riesgos, componentes y acciones en infraestructuras

Las ***componentes de riesgo*** proporcionan una estructura que garantiza un proceso completo de identificación sistemática de los riesgos con un nivel de detalle uniforme, y contribuye a la efectividad y calidad de la identificación de riesgos. Una estructura de desglose del riesgo, como la propuesta en la Figura 3.4, es uno de los métodos para proporcionar dicha estructura.

El esquema presentado en la Figura 3.4 caracteriza a un *riesgo* como un conjunto de **componentes de riesgo**, lo cual tiene los siguientes propósitos:

- Facilitar la identificación de medidas de gestión comunes a un mismo conjunto de riesgos.
- Facilitar las referencias para caracterizar cada componente de riesgo utilizando las fuentes de información disponibles: informes, estudios, análisis externos, etc.

3.3.3 TIPOS DE MAPAS DE RIESGOS

La revisión de herramientas y metodologías ha permitido concluir que la *técnica de mapas de riesgos* es universalmente aceptada para desarrollar la etapa de identificación dentro de planes de protección de infraestructuras críticas PIC. En desarrollo de la propuesta metodológica original que se formula en esta investigación, existe el interés de conocer previamente las particularidades de los diferentes *tipos* de mapas de riesgos, según se describen en esta sección.

Los mapas que se presentan a continuación agrupan los riesgos según su **categoría**, es decir, según el conjunto de riesgos que comparten características similares, de acuerdo a los criterios de elaboración del panel de analistas y expertos.

Mapas Auditorías COSO

El esquema de categorías, presentado en la Figura 3.5, establecido en [COSO, 2004], permite establecer una primera aproximación para la realización de los mapas de riesgos en un sistema de infraestructura eléctrica.

Figura 3.5: Propuesta de categorización de riesgos [COSO, 2004].

Esta aproximación de las categorías de riesgos facilita el control y auditoría sobre los riesgos que se identifican en las empresas propietarias y operadoras del sistema de infraestructura energética. La propuesta de [COSO, 2004; ERM Initiative, 2010] ha sido pionera en la metodología de identificación de riesgos, tomando cuatro **categorías** principales de recursos (Estratégicos, Operacionales, Informes e Indicadores), dentro de los cuales se analizan los riesgos ambientales y de procesos propios de la red.

Mapas de Radar

El proceso Identificación de Riesgos suele acompañarse de un proceso de análisis cualitativo, que se construye con información proveniente de entrevistas a los directivos administradores estratégicos de los sectores de infraestructura crítica. Dicha identificación se puede representar en un esquema tipo radar, como se muestra en la Figura 3.6.

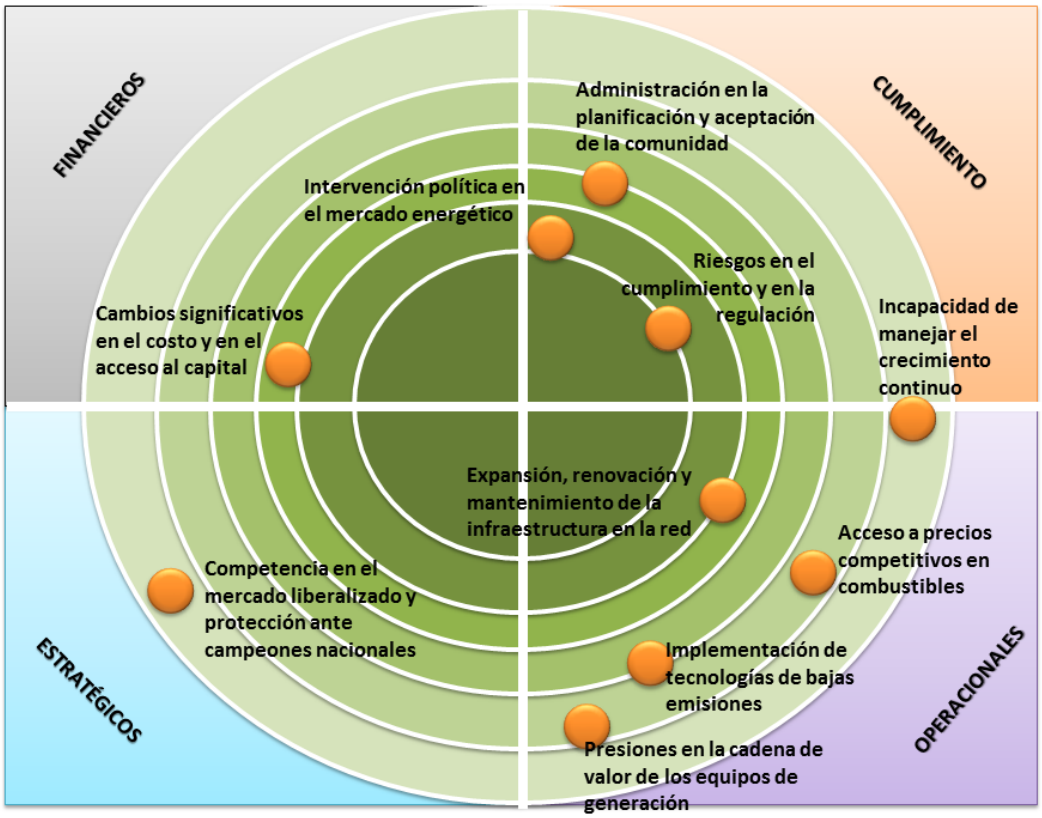


Figura 3.6: Propuesta de categorización de riesgos de empresas eléctricas, en esquema radar [ERNST & YOUNG, 2009; AON, 2010].

Los riesgos que se ubican en el centro del radar son aquellos que se identifican como los de mayor desafío a corto plazo. Esta representación es ampliamente utilizada por analistas de riesgos en sectores económicos como [ERNST & YOUNG, 2009] y [AON, 2010]. Básicamente se distinguen las siguientes categorías de riesgos:

- **Cumplimiento***:* están relacionados con las amenazas provenientes en la expedición de políticas, leyes, regulaciones o por el gobierno corporativo.
- **Financieros***:* se derivan de la volatilidad en los mercados y la economía real.
- **Estratégicos**: están relacionadas con los clientes, competidores e inversores.
- **Operacionales**: afectan a los procesos, sistemas, personas y cadena de valor global de una empresa.

Esta propuesta es de gran utilidad para el análisis de riesgos en empresas propietarias y/o operadoras del sistema de infraestructura de energía eléctrica.

Esquemas Holísticos

Probablemente una visión amplia de los riesgos y amenazas a los que se somete el sistema de infraestructura eléctrica puede centrarse en un esquema holístico, mediante el cual se exploran conexiones entre diferentes puntos de vista.

La Figura 3.7 presenta un ejemplo de estas variaciones en la representación jerárquica de las fuentes de riesgo, muy útil para proyectar la construcción y puesta en marcha de un sistema de infraestructura.

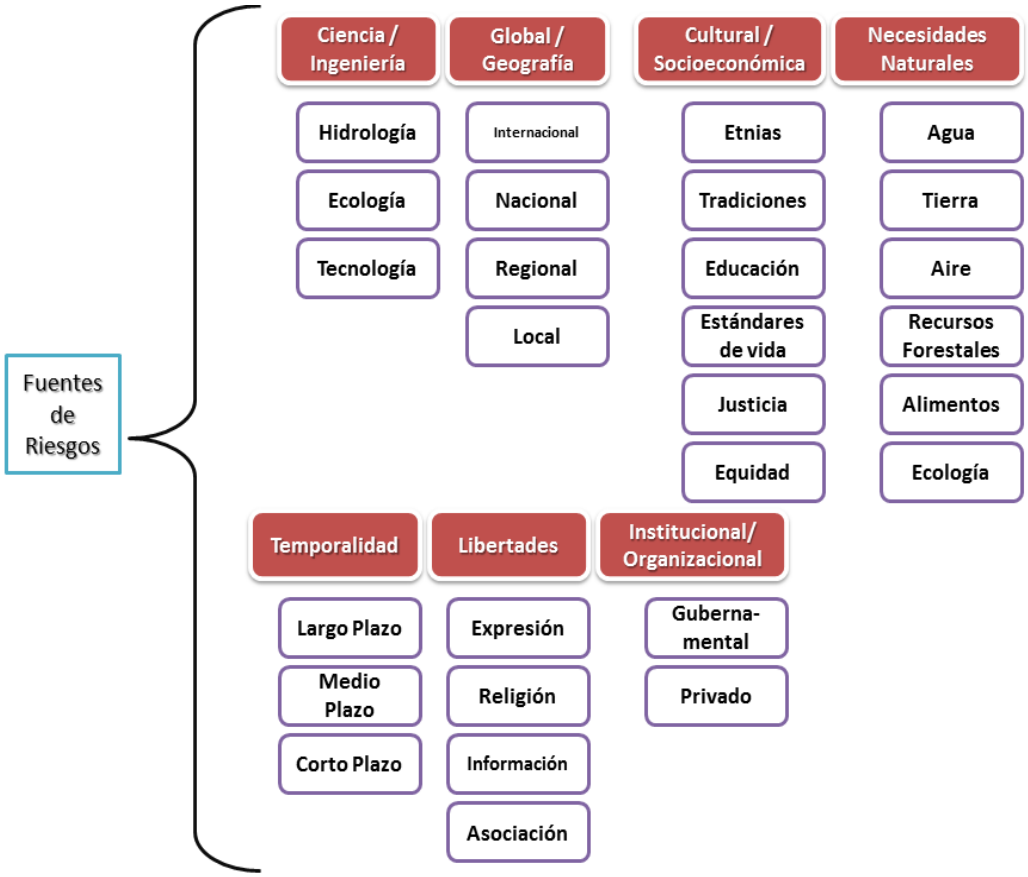


Figura 3.7: Propuesta holística de categorización de riesgos en proyectos [PMI, 2004].

Dicho esquema se adapta adecuadamente a la gestión de proyectos [PMI, 2004], sin embargo, la categorización no está debidamente resumida, y dificulta la identificación de componentes de riesgo dentro de un sistema específico como una red de infraestructura crítica.

Mapas de Riesgos Empresariales

Utilizando el esquema de clasificación de riesgos planteado en [ICONTEC, 2004] es posible clasificar los riesgos existentes en empresas que son propietarias y/o operadoras de las redes de infraestructura eléctrica en cuatro grandes **categorías**:

- **Riesgos de entorno**: Riesgos de origen externo relacionados con aspectos normativos, políticos, sociales, de clientes o proveedores, fenómenos naturales, entre otros, que afectan las operaciones y el normal funcionamiento de la empresa.
- **Riesgos estratégicos**: Aquellos cuya ocurrencia ocasiona una disminución del ritmo de crecimiento y el incumplimiento de objetivos de las empresas propietarias y operadoras del sistema de infraestructura crítica. Están directamente asociados a la estrategia y sostenibilidad del negocio de operación de la infraestructura eléctrica en el largo plazo.
- **Riesgos financieros**: Riesgos derivados del incremento de obligaciones empresariales a causa de las fluctuaciones en las tasas de interés, convertibilidad de divisas o cualquier otro parámetro financiero de referencia. También incluye el impago por parte de clientes y la imposibilidad de obtener los fondos necesarios para atender el pago de las obligaciones contraídas o para apalancar el crecimiento.
- **Riesgos operacionales**: Relacionados con la dependencia que la empresa tiene de sus procesos y personas. Evidencian fallos en la ejecución de actividades, deficiencia o ausencia de procedimientos, y fallos en la gestión del capital humano, tecnológico y organizacional.

En este punto, es posible tomar el esquema propuesto por empresas de redes de infraestructura eléctrica, como las que se referencian en [ISA, 2009; ISAGEN, 2009]. Para cada uno de los riesgos, se debe identificar el tipo de origen, el cual puede ser externo, interno o ambos.

- **Riesgos de origen externo**: aquellos que se materializan como consecuencia de factores por fuera de la empresa; tales como: fenómenos naturales, situaciones sociopolíticas, acciones de terceros, decisiones de autoridades administrativas, regulatorias, entre otras.
- **Riesgos de origen interno:** incluyen aquellos ocasionados como consecuencia de las personas, los sistemas o los procedimientos de la empresa; así mismo, por las decisiones y actuaciones de los directivos o colaboradores de la empresa.

Se puede desarrollar un caso de estudio a partir de información pública y relevante para la identificación de los riesgos, los cuales se pueden representar en un *esquema de riesgos*, como el que se presenta en la Figura 3.8. Para la construcción del mencionado mapa de riesgos, se puede retomar el trabajo previo de empresas del sector eléctrico [ISA, 2009; ISAGEN, 2009; XM, 2009].

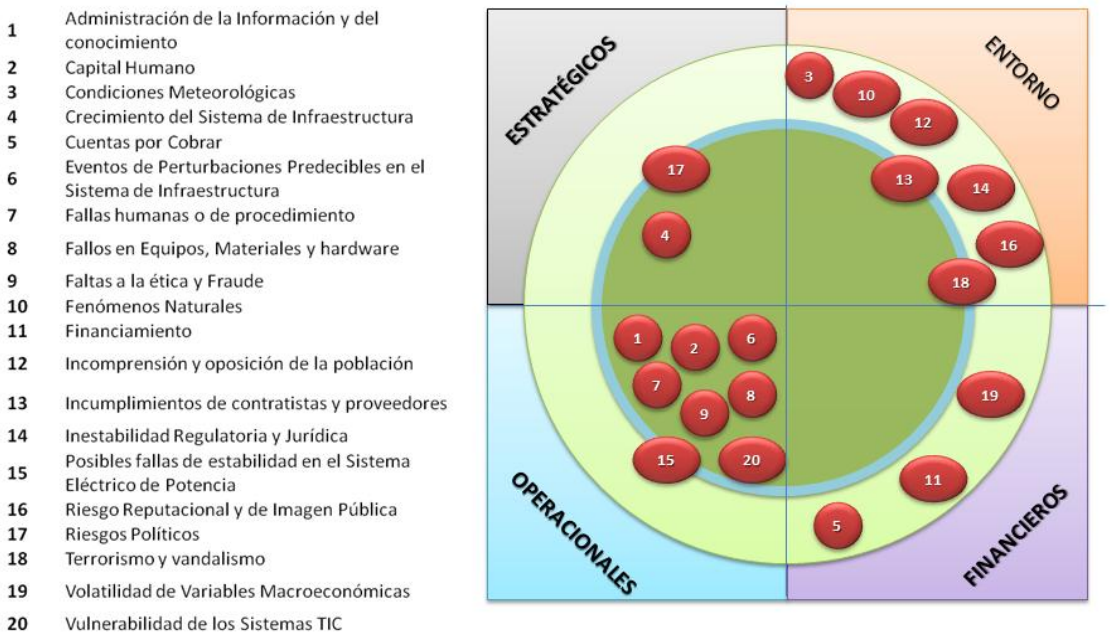


Figura 3.8: Mapa de riesgos empresariales [ISA, 2009]

Esta aproximación es muy útil en el análisis de riesgos organizacionales en las empresas energéticas. Sin embargo, es necesaria mayor profundidad en la estructuración de esta información para aplicarla a un sistema de infraestructura energética.

3.3.4 PROPUESTA DE MAPA INTERCONECTADO DE RIESGOS

A efectos prácticos en el desarrollo de esta tesis, la aplicación sistemática de una metodología para identificación de riesgos debe permitir seleccionar activos críticos, verificar interdependencias, clasificar los riesgos en categorías y determinar detalladamente las componentes de riesgo en cada definición de riesgo. De esta manera, se identificarán los riesgos que afectan de forma más grave la prestación y operación del servicio de la infraestructura crítica.

Como resultado de la revisión presentada en la sección 3.3 se ha comprobado la universalidad y la favorable aceptación de la metodología de mapas de riesgos para ejecutar la *etapa de identificación* en los planes de protección de infraestructura crítica.

Los diferentes tipos de mapas de riesgos proporcionan una información básica acerca de los riesgos que afectan al sistema de infraestructura, incluyendo a las organizaciones que se encargan de su gestión y operación. Mediante la utilización de estos esquemas se busca realizar una descripción cualitativa del sistema, que

posteriormente permite incorporar la probabilidad de ocurrencia e impacto de cada riesgo, de acuerdo con una escala descriptiva [ICONTEC, 2004; ISO, 2010].

Como contribución de la propuesta que se explica en esta sección se efectúa la adaptación de los diferentes mapas explicados en la sección 3.3 para el sistema de infraestructura del sector eléctrico. La interrelación entre los riesgos que se identifican y que se representan en un mapa de riesgos interconectado es una aportación original en esta tesis.

La realización de esta propuesta metodológica para la identificación de riesgos y de sus componentes se ha desarrollado sobre un caso de aplicación real en el sector eléctrico colombiano.

3.3.4.1 Requerimientos del mapa interconectado de riesgos

La propuesta aquí presentada consiste en la construcción de un **mapa interconectado de riesgos** que tenga en cuenta la clasificación de amenazas al sistema de infraestructura según su origen. Esto permitirá definir posteriores responsabilidades en su tratamiento, según se propone a continuación [YUSTA, 2009]:

- **Amenazas de tipo técnico**. Las cuales incluyen los riesgos financieros y los riesgos operacionales. También se incluyen aquellos ocasionados como consecuencia de las personas, los sistemas, los procedimientos, las decisiones y actuaciones que afectan al sistema de infraestructura.
- **Amenazas de tipo no-técnico**. Las cuales incluyen los riesgos de entorno, los riesgos estratégicos y los riesgos de asignación de recursos. También se incluyen aquellos que se materializan como consecuencia de factores por fuera de la red de infraestructura; tales como: fenómenos naturales, situaciones sociopolíticas, acciones de terceros, decisiones de autoridades administrativas, regulatorias, entre otras.

Adicionalmente esta propuesta de **mapa interconectado de riesgos** permite simplificar el número de elementos que agrupa las componentes de riesgo. Se distinguen las siguientes categorías de riesgos, aplicables al sistema de infraestructura crítica [LÓPEZ & ARBOLEDA, 2010].

- **Cumplimiento e Indicadores***:* están relacionados con las amenazas provenientes en la expedición de políticas, leyes, regulaciones y su impacto en el desarrollo económico y social de la región o nación en la cual se desempeña el sistema de infraestructura.

- **Activos y Finanzas***:* se derivan de la volatilidad en los mercados y la economía real, que impactan el normal funcionamiento y/o la expansión de las redes de infraestructura eléctrica. También se incluyen los riesgos relacionados con la cartera por cobrar, y la imposibilidad de obtener los fondos necesarios para atender el pago de las obligaciones contraídas o para apalancar el crecimiento del sistema de infraestructura eléctrica.
- **Entorno**: Riesgos de relacionados con aspectos normativos, políticos, sociales, fenómenos naturales, entre otros, que afectan las operaciones y el normal funcionamiento de la red de infraestructura eléctrica.
- **Operacionales**: Riesgos que afectan los procesos, sistemas, personas y cadena de valor global dentro del sistema de infraestructura eléctrica. Evidencian fallos en la ejecución de actividades, deficiencia o ausencia de procedimientos, y fallos en la gestión del capital humano, tecnológico y administrativo, que impactan el funcionamiento y el crecimiento de la red de infraestructura.

Tanto el mapa de riesgos como las componentes de riesgo forman parte del conocimiento de la organización. Existirán riesgos que afecten tanto a la cadena de valor como a cada nivel de la organización. Es decir, un riesgo puede afectar una organización, un sistema o un activo. De acuerdo al nivel de abstracción organizacional (desde un nivel estratégico y global, hasta un nivel operativo y de detalle), el mapa de riesgos puede variar para adaptarse a cada caso.

3.3.4.2 Mapa interconectado de riesgos para la cadena de valor del sector eléctrico

El **mapa interconectado de riesgos** ofrece un marco para la toma de decisiones, pues permite apreciar los riesgos de una manera integrada. Esta técnica permite descubrir y analizar las amenazas a las que están expuestas las infraestructuras. Dentro de esta propuesta metodológica se identifican aquellas vulnerabilidades de mayor desafío en el corto plazo.

En la Figura 3.9 se presenta una *propuesta original* de **mapa interconectado de riesgos** para la cadena de valor del sector eléctrico, que también es aplicable a las empresas operadoras del sistema de transporte de energía eléctrica.

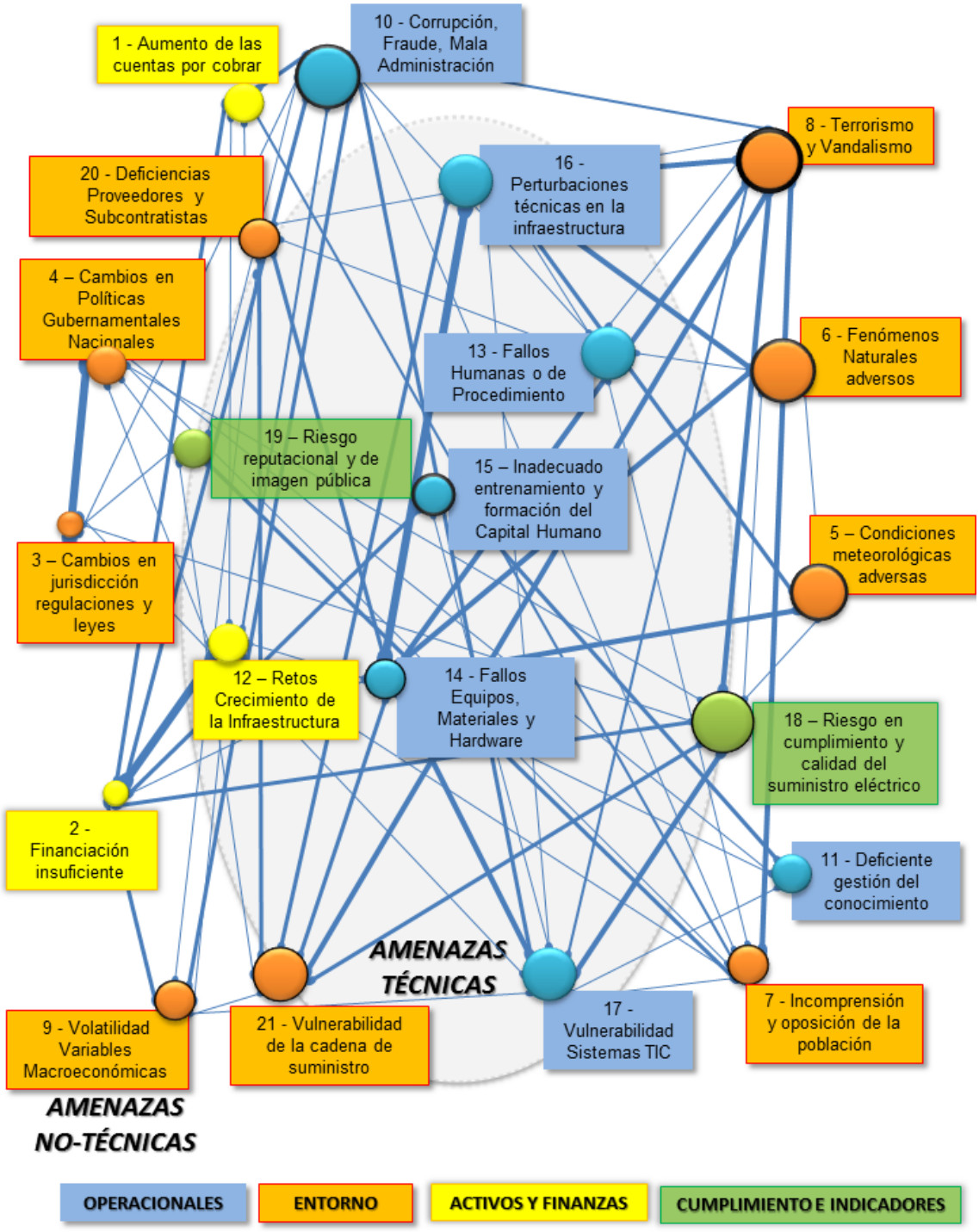


Figura 3.9: Propuesta de mapa interconectado de riesgos para infraestructuras del sector eléctrico colombiano

Este mapa de riesgos tiene en cuenta los requerimientos presentados en la sección 3.3.4.1. La recolección de información se ha realizado a partir de **fuentes humanas** (entrevistas, revisión de documentación) en empresas del sector de transporte y distribución de energía eléctrica en Colombia describiendo la identificación de amenazas de tipo técnico y no-técnico al sistema de infraestructura. Este mapa de

riesgos también incluye información extraída de publicaciones y literatura especializada,

A partir de las consideraciones previamente expuestas, se ha elaborado un listado resumido de 21 riesgos clasificados en cuatro categorías, los cuales constituyen la base para identificar el conjunto de riesgos que afectan la cadena de valor en las infraestructuras del sector eléctrico.

La información proporcionada por el **mapa interconectado de riesgos** de la Figura 3.9 aplicado a la cadena de valor de los sistemas eléctricos de infraestructura crítica, puede tener en cuenta la **probabilidad de ocurrencia** de cada riesgo, así como su **impacto** en los diferentes sectores sociales y económicos. Sus resultados se podrán representar gráficamente mediante el diámetro de cada nodo del mapa (impacto) y el grosor de la línea circular (probabilidad). Adicionalmente, en este **mapa interconectado de riesgos** el grosor de la línea puede indicar la relación más o menos estrecha entre los diferentes riesgos. A efecto del mapa de la Figura 3.9 se ha efectuado una estimación gráfica de los valores para cada riesgo, si bien su calificación y valoración se realizará con detalle en el capítulo 4 de evaluación de riesgos.

3.3.4.3 Determinación de las componentes de riesgo

Para efectuar el estudio detallado de cada uno de los riesgos del mapa es preciso realizar la identificación de sus componentes, según se ha explicado previamente en la sección 3.3.2. Aunque el propósito de esta sección se limita al establecimiento de un marco conceptual es importante anotar que, en términos prácticos, las organizaciones operadoras y/o propietarias de sistemas de infraestructura eléctrica, dentro de sus sistemas de gestión de riesgos, caracterizan cada riesgo en forma de **componentes** [AS/NZS, 1999; JP-Morgan, 1999].

Para el caso particular de los 21 riesgos identificados en la red de infraestructura eléctrica (Figura 3.9) se ha determinado un listado de 142 componentes de riesgo, que pueden consultarse en la Tabla 3.3.

La construcción de esta base de riesgos ha requerido un diseño de investigación analítico–descriptivo, que utiliza instrumentos de obtención de datos a partir de fuentes primarias en empresas propietarias y operadoras del sistema de infraestructura eléctrica. La técnica utilizada para la recolección de la información se basa en preguntas abiertas a fuentes humanas de diferentes organizaciones del sector eléctrico colombiano (sección 3.2.3).

La determinación de estas componentes de riesgo también ha tenido en cuenta la información obtenida de libros y publicaciones técnicas en estrategias de protección [KNIGHT, 2001; LEWIS, 2006; NESS, 2006; SULLIVANT & NEAVE, 2007; MACAULAY, 2008; CNA, 2009; ISA, 2009; ISAGEN, 2009; XM, 2009; LÓPEZ & ARBOLEDA, 2010; RADVANOVSKY & Mc-DOUGALL, 2010].

Tabla 3.3: Identificación de componentes de riesgo con aplicación al caso del sistema eléctrico colombiano

F = RIESGOS SOBRE ACTIVOS Y FINANZAS
I = RIESGOS SOBRE EL CUMPLIMIENTO DE INDICADORES
E = RIESGOS DEL ENTORNO
O = RIESGOS OPERACIONALES

ÍTEM	CATEGORÍA	RIESGO	COMPONENTES DEL RIESGO	OBSERVACIONES
1	F	1 - Aumento de las cuentas por cobrar (Cobranzas)	Morosidad, dudoso recaudo o no recuperación de cartera de parte de los agentes que usan la Red de Transporte	Uno de los agentes que usan la infraestructura de transporte podría no cumplir con su obligación de pago al sistema de transporte de energía. El administrador del mercado traslada el valor de la deuda no cubierto por las garantías a los agentes del mercado en la proporción correspondiente.
2	F	1 - Aumento de las cuentas por cobrar (Cobranzas)	Morosidad, dudoso recaudo o no recuperación de cartera por servicios de conexión al Sistema de Infraestructura Eléctrica (Transporte alta tensión)	Uno de los clientes (distribuidores, generadores, grandes consumidores y transportadores) puede incumplir con su obligación de pago.
3	F	1 - Aumento de las cuentas por cobrar (Cobranzas)	Morosidad, dudoso recaudo o no recuperación de cartera por servicios asociados y no operacionales	Uno de los clientes de servicios asociados o no operacionales podría incumplir con su obligación de pago. Los servicios asociados son: Estudios, desarrollo integral de proyectos de infraestructura, mantenimiento, uso de sus redes. Los servicios no operacionales son: venta y arriendo de activos (lotes, inventarios, sedes, equipos)
4	F	1 - Aumento de las cuentas por cobrar (Cobranzas)	Riesgo de Crédito: Falta de cumplimiento por parte de terceros de las obligaciones establecidas	Esta componente de riesgo impacta a empresas o entidades particularmente involucradas en la propiedad/operación/gestión, como agentes en la cadena de valor del sistema de infraestructura eléctrica.
5	F	1 - Aumento de las cuentas por cobrar (Cobranzas)	Altos precios en tarifas reguladas (transporte, distribución) o en comercialización	Esta componente de riesgo impacta a empresas o entidades particularmente involucradas en la propiedad/operación/gestión, como agentes en la cadena de valor del sistema de infraestructura eléctrica.
6	F	2 - Financiación insuficiente	Encarecimiento de las condiciones esperadas para la consecución de los recursos	Diferentes factores como la iliquidez de los mercados nacionales e internacionales, la disminución de la calidad crediticia de la empresa infraestructura, o de los países donde tiene presencia puede encarecer la consecución de recursos respecto a lo proyectado (Aumenta la prima de riesgo de la deuda)
7	F	2 - Financiación insuficiente	Imposibilidad de consecución oportuna de recursos	Variaciones desfavorables en el entorno financiero nacional o internacional
8	F	2 - Financiación insuficiente	Compromisos contractuales que limiten o dificulten la consecución de nuevo endeudamiento	Garantías, niveles de indicadores financieros pactados contractualmente con entidades financieras, firmas calificadoras de riesgos, el Estado, etc.
9	F	2 - Financiación insuficiente	Complejidad, demora y heterogeneidad en los procesos operativos, internos o externos, para la aprobación y consecución de recursos financieros.	Internos: distintas aprobaciones: Junta Directiva, Administración, etc. Externos: Organismos reguladores, Ministerios Públicos, Contraparte: Sector Financiero, Inversionistas
10	F	2 - Financiación insuficiente	Riesgo de mercado asociados a los movimientos en la bolsa de energía	Los precios pactados en la comercialización en bolsa, o en los contratos bilaterales, inciden en el flujo de caja, para asegurar el funcionamiento del sistema de infraestructura.

ÍTEM	CATEGORÍA	RIESGO	COMPONENTES DEL RIESGO	OBSERVACIONES
11	F	2 - Financiación insuficiente	Riesgos de mercado asociados a la variación de la tasa de cambio	Variaciones y devaluación del valor de la moneda local, impactan las negociaciones internacionales de repuestos, materias primas así como los costos de venta de la energía
12	F	2 - Financiación insuficiente	Riesgos de mercado asociados a la variación de la tasa de interés y renovación de la deuda	Variación de la tasa de interés, que redundan en el coste de los créditos pactados para el funcionamiento y/o la ampliación en proyectos de infraestructura
13	F	2 - Financiación insuficiente	Pago inoportuno de impuestos y contribuciones	Exposición a multas, impacto en el flujo de caja y deterioro de la imagen reputacional por no cumplir con las obligaciones fiscales
14	F	2 - Financiación insuficiente	Disminución en la participación del mercado (transacciones y contratos) en la bolsa de energía	Esta componente de riesgo impacta a empresas o entidades particularmente involucradas en la propiedad/operación/gestión, como agentes en la cadena de valor del sistema de infraestructura eléctrica
15	F	2 - Financiación insuficiente	Proyecciones inadecuadas en los presupuestos y flujos de efectivo en el corto, mediano y largo plazo	Esto impacta la estrategia de funcionamiento y de crecimiento del sistema, sus indicadores económicos y estabilidad de las empresas propietarias/operadoras de la red de infraestructura eléctrica
16	F	2 - Financiación insuficiente	Mayor competencia y estrategias de mercado entre agentes de la cadena de energía (Generación, Distribución, Comercialización)	Esta componente de riesgo impacta a empresas o entidades particularmente involucradas en la propiedad/operación/gestión, como agentes en la cadena de valor del sistema de infraestructura eléctrica
17	F	2 - Financiación insuficiente	Rentabilidad esperada menor al costo del capital empleado	Tanto la concepción de un proyecto, como la operación de un sistema, involucran componentes de rentabilidad, que en caso de incumplirse, ponen en peligro la sostenibilidad y viabilidad de la red
18	I	3 - Cambios en la regulación, políticas y jurisdicción en el sistema de Infraestructura	Cambios o vacíos en la regulación que incrementan la exigencia en los niveles de calidad, seguridad y confiabilidad en la prestación del servicio de transporte de energía	Las comisiones reguladoras pueden modificar, a través de resoluciones, los requerimientos que determinan los indicadores de disponibilidad de equipos y confiabilidad en el sistema comprometiendo la calidad y oportunidad en el servicio
19	I	3 - Cambios en la regulación, políticas y jurisdicción en el sistema de Infraestructura	Cambios en las normas y jurisprudencia (Inseguridad jurídica)	Incluye las normas nacionales e internacionales que afecten las operaciones de la empresa, las cuales pueden ser civiles, administrativas, comerciales, laborales, tributarias, ambientales, contables, cambiarias o estar relacionadas con la actividad de generación, transporte, distribución de energía
20	I	3 - Cambios en la regulación, políticas y jurisdicción en el sistema de Infraestructura	Diferencia de criterio en la interpretación de las normas entre las autoridades administrativas o judiciales o entre éstas	Diferencia de criterio en la interpretación de las normas de todo tipo , incluye las civiles, administrativas, comerciales, laborales, ambientales, tributarias, cambiarias, aduaneras, contables, entre autoridades judiciales y administrativas, etc
21	E	3 - Cambios en la regulación, políticas y jurisdicción en el sistema de Infraestructura	Cambios o vacios en la regulación que afectan los ingresos o egresos asociados al negocio de transporte de energía.	El negocio de transporte en Colombia es regulado y su esquema de remuneración, que se revisa periódicamente según la regulación vigente.
22	E	3 - Cambios en la regulación, políticas y jurisdicción en el sistema de Infraestructura	Indebida aplicación de las normas o indebida valoración de las pruebas, por las autoridades administrativas o judiciales	La indebida aplicación puede ser intencional o no
23	E	3 - Cambios en la regulación, políticas y jurisdicción en el sistema de Infraestructura	Reducción o pérdida de la remuneración del cargo por confiabilidad y de las subvenciones	La actual tendencia converge a eliminar estas remuneraciones y cargos en el mediano y largo plazo
24	E	3 - Cambios en la regulación, políticas y jurisdicción en el sistema de Infraestructura	Reglamentaciones no acordes con las realidades tecnológicas en las centrales de generación térmicas, hidroeléctricas, eólicas, nucleares y solares	La tecnología siempre está un paso delante de las regulaciones y de las políticas gubernamentales. Esta situación puede imposibilitar la actualización tecnológica en la red de infraestructura, y en consecuencia, hacerla menos eficiente

ÍTEM	CATEGORÍA	RIESGO	COMPONENTES DEL RIESGO	OBSERVACIONES
25	E	3 - Cambios en la regulación, políticas y jurisdicción en el sistema de Infraestructura	Incumplimiento parcial o total y/o mayores exigencias en la regulación ambiental	Generalmente las mayores exigencias ambientales, exigen mayores inversiones, reservas y responsabilidad hacia las comunidades. En casos extremos, se requiere dejar cesantes algunos activos dentro del sistema de infraestructura
26	E	4 - Cambios en las políticas Públicas Nacionales en torno al sistema de Infraestructura	Expropiación, confiscación o nacionalización	La orientación de políticas públicas puede llevar a un gobierno a ejecutar algunas de estas modalidades de toma de control de una empresa que sea propietaria y operadora de la infraestructura eléctrica: Expropiación: desposesión o privación de propiedad. Expropiación Forzosa: posesión o privación de propiedad privada por parte del Estado y entes públicos, por causas de utilidad pública, previa indemnización. Nacionalización: paso de medios de producción y servicios explotados por particulares a manos del gobierno de una nación. Confiscación: requisamiento o apropiación que el Estado hace de los bienes privados en determinadas circunstancias (generalmente incumplimientos). Tanto en la expropiación como en la nacionalización, se puede dar participación del Estado como socio a través de empresas mixtas, donde el Estado es el socio mayoritario. Estas modalidades no son excluyentes
27	E	4 - Cambios en las políticas Públicas Nacionales en torno al sistema de Infraestructura	Inconvertibilidad y restricción en la transferencia de divisas	Un gobierno puede implementar medidas de control de capitales, que impidan o dificulten a las empresas la transferencia o conversión de divisas provenientes de sus inversiones en el exterior.
28	E	4 - Cambios en las políticas Públicas Nacionales en torno al sistema de Infraestructura	Restricción a la inversión extranjera	Un gobierno puede definir políticas que restrinjan la inversión extranjera y dificulten el desarrollo de la estrategia de crecimiento de la infraestructura eléctrica
29	E	4 - Cambios en las políticas Públicas Nacionales en torno al sistema de Infraestructura	Incumplimiento por parte de los gobiernos de las obligaciones pactadas contractualmente con las empresas propietarias y operadoras de la infraestructura eléctrica	Existe la posibilidad de incumplimiento de los gobiernos de otros países en los contratos con las filiales. Algunos tipos de contrato son: * Contratos de estabilidad jurídica y tributaria: Tienen como propósito garantizar condiciones de estabilidad de la inversión, independiente de que los regímenes cambien. * Concesiones: Garantizan ingresos y formas de actualización de los mismos
30	E	5 - Condiciones Meteorológicas adversas	Tormentas de hielo y/o nieve	Rompimiento de conductores, uniones, colapso y derribo de torres de transporte y de distribución
31	E	5 - Condiciones Meteorológicas adversas	Ráfagas de vientos	Caída de árboles o materiales arrastrados por el viento que causan cortocircuitos entre las líneas aéreas de alto y media tensión
32	E	5 - Condiciones Meteorológicas adversas	Polución ambiental	Deterioro de los aislamientos en toda la cadena de transporte y distribución de electricidad, y aumenta la probabilidad del flameo sobre los aisladores
33	E	5 - Condiciones Meteorológicas adversas	Concentración de salinidad	Deterioro de los aislamientos en toda la cadena de transporte y distribución de electricidad, y aumenta la probabilidad del flameo sobre los aisladores
34	E	5 - Condiciones Meteorológicas adversas	Olas de Frío	Cargas mecánicas debidas a acumulación de hielo o nieve, aumenta el vano del conductor y con este, la probabilidad que se sobrepasen los límites de seguridad
35	E	5 - Condiciones Meteorológicas adversas	Olas de Calor	Al aumentar la corriente circulante y las pérdidas efecto Joule, aumenta el vano del conductor y con este, la probabilidad que se sobrepasen los límites de seguridad
36	E	5 - Condiciones Meteorológicas adversas	Radiación solar	Al aumentar la temperatura ambiental, aumenta el vano del conductor y con este, la probabilidad que se sobrepasen los límites de seguridad

ÍTEM	CATEGORÍA	RIESGO	COMPONENTES DEL RIESGO	OBSERVACIONES
37	E	5 - Condiciones Meteorológicas adversas	Vendaval	Rompimiento de conductores, uniones, colapso y derribo de torres de transporte y de distribución
38	E	5 - Condiciones Meteorológicas adversas	Descargas atmosféricas	Descarga atmosférica que afecte temporalmente las comunicaciones o que impacte en cable de guarda en cruce de varios circuitos, generando la salida de dos o más circuitos simultáneamente; se pierde capacidad de monitorización de la red desde el centro de control.
39	E	6 - Fenómenos Naturales adversos	Movimientos Telúricos	Dificultades de acceso o de disponibilidad de recursos (entre ellos, las personas) para restituir la operación o hacer las reparaciones necesarias en la infraestructura afectada. Es posible que se pueda seguir prestando el servicio pero no con niveles de confiabilidad y seguridad requeridos.
40	E	6 - Fenómenos Naturales adversos	Deslizamiento de tierra	Hundimiento del suelo que afecta las bases de las torres de transporte
41	E	6 - Fenómenos Naturales adversos	Avalancha o creciente	Hundimiento del suelo que afecta las bases de las torres de transporte y de la red de distribución
42	E	6 - Fenómenos Naturales adversos	Inundación o anegación	Dificultades de acceso o de disponibilidad de recursos (entre ellos, las personas) para restituir la operación o hacer las reparaciones necesarias en la infraestructura afectada. Es posible que se pueda seguir prestando el servicio pero no con niveles de confiabilidad y seguridad requeridos.
43	E	6 - Fenómenos Naturales adversos	Erupciones volcánicas	Dificultades de acceso o conflictos en las comunidades vecinas que pueden generarse como consecuencia de un evento asociado con este componente.
44	E	6 - Fenómenos Naturales adversos	Incendios forestales	Fenómeno de flameo entre las líneas aéreas de alta tensión y la vegetación, en todo el recorrido de la línea aérea
45	E	6 - Fenómenos Naturales adversos	Perturbaciones magnéticas solares	Afectación los sistemas de telemetría y control en los sistemas de potencia (periódicamente cada 10 años)
46	E	6 - Fenómenos Naturales adversos	Vegetación protuberante en área de servidumbre de la infraestructura	Fenómeno de flameo entre las líneas aéreas de alta tensión y la vegetación
47	E	7 - Incomprensión y oposición de la población	Manifestación pacífica, marcha o paro cívico	* Manifestación: Acción colectiva de la población civil que se traduce en una movilización social. Protesta masiva y pública, mediante una congregación en las calles, con el fin de expresar el apoyo o rechazo a decisiones o acciones. * Paro cívico: Acción colectiva expresada políticamente por individuos, gremios, asociaciones civiles, sindicatos, organizaciones sociales, quienes actúan como "gran grupo" -sociedad civil. Incluye la suspensión de actividades económicas, comerciales, etc. Una manifestación pública o paro cívico puede desencadenar en actos violentos (asonada).
48	E	7 - Incomprensión y oposición de la población	Asonadas	Manifestación en la que se presentan actos violentos
49	E	7 - Incomprensión y oposición de la población	Bloqueo o toma pacífica de instalaciones	Se puede materializar en la toma de una subestación o sede administrativa o al dificultar el acceso a zonas donde se encuentra la infraestructura eléctrica, impidiendo el normal desarrollo de las actividades que allí se realizan y puede poner en riesgo la vida de las personas que laboran en ellas.
50	E	7 - Incomprensión y oposición de la población	Hurto, daño o sabotaje a bienes o equipos	Incluye hurto calificado y hurto simple
51	E	7 - Incomprensión y oposición de la población	Invasión de servidumbres por razones socioeconómicas	Ocupación de una servidumbre o predio por parte de población civil por razones socioeconómicas diferentes al conflicto armado.
52	E	7 - Incomprensión y oposición de la población	Conflicto con propietarios en zonas de servidumbre	Pedidos desproporcionados de los propietarios de los predios y de las servidumbres que no permiten llegar a un acuerdo.

ÍTEM	CATEGORÍA	RIESGO	COMPONENTES DEL RIESGO	OBSERVACIONES
53	E	7 - Incomprensión y oposición de la población	Rechazo de la comunidad por el desarrollo normal de las actividades en la gestión de la infraestructura	Inconformidades de las comunidades al no coincidir sus expectativas sociales con las actividades desarrolladas por la Empresa.
54	E	7 - Incomprensión y oposición de la población	Desinstitucionalización del Estado local	Debilidad en la administración pública local que puede incidir en diversos aspectos como: limitar el inicio o desarrollo de los procesos de gestión socioambiental que acompañan las actividades de construcción, operación y mantenimiento, no contar con la autoridad local para controlar situaciones que pueden impedir o dificultar el desarrollo de actividades relacionadas con la construcción u operación y la desprotección de las servidumbres, aumentando el riesgo de volver a invadir éstas.
55	E	7 - Incomprensión y oposición de la población	Líneas de transporte comparten derechos de paso, con otras infraestructuras claves dentro de las comunidades.	Puentes, túneles, terrenos de servidumbre, entre otros, frecuentemente involucran derechos de paso para las líneas de transporte eléctricas.
56	E	7 - Incomprensión y oposición de la población	Oposición al desarrollo de las redes eléctricas	Por su visibilidad y notoriedad, se producen dificultades derivadas de la oposición social y de las organizaciones ecologistas hacia las nuevas infraestructuras
57	E	8 - Terrorismo y Vandalismo	Voladura de torres o de instalaciones	Ataque premeditado o aleatorio a torres de transporte y distribución de líneas de alta o de media tensión.
58	E	8 - Terrorismo y Vandalismo	Toma armada o ataque a instalaciones, incluyendo las plantas de generación	Afectaciones a los bienes y demás activos en el Sistema de Infraestructura y/o los Servicios Auxiliares, excluyendo las redes de transporte
59	E	8 - Terrorismo y Vandalismo	Ataque a la red de infraestructura de transporte de energía eléctrica, Voladura de torres o de instalaciones	Ataque a la red de transporte de energía eléctrica, en las que se incluyen torres, líneas, conductores, redes de fibra óptica, o cualquier otro tipo de infraestructura lineal desarrollada por la empresa.
60	E	8 - Terrorismo y Vandalismo	Sometimiento y secuestro	Privación ilegal de la libertad de una o varias personas
61	E	8 - Terrorismo y Vandalismo	Campo minado	Daños a los empleados o a los contratistas en el desarrollo de las actividades propias de la empresa por minas antipersona.
62	E	8 - Terrorismo y Vandalismo	Extorsión	Obligar o constreñir a una persona como resultado de una presión, bien sea contra su integridad, su familia o sus bienes, para que haga, tolere u omita una acción con el fin de obtener provecho ilícito.
63	E	8 - Terrorismo y Vandalismo	Bloqueo o paro armado	Acción y efecto de interceptar, obstruir, cerrar el paso, impedir el funcionamiento normal, dificultar y entorpecer la realización de un proceso, por medios violentos (incluye dificultad de acceso a ciertas zonas con condiciones particulares - cultivos ilícitos)
64	E	8 - Terrorismo y Vandalismo	Ataque armado en torres de transporte, subestaciones y plantas de generación	Tiene consecuencias en la destrucción de infraestructura de transporte o transporte de electricidad
65	E	8 - Terrorismo y Vandalismo	Fuego cruzado	Puede presentarse por operaciones de organismos de seguridad, por ataque a organismos de seguridad o por enfrentamiento de actores generadores de violencia.
66	E	8 - Terrorismo y Vandalismo	Invasión de servidumbres o predios por desplazamiento forzado	Ocupación de una servidumbre o predio por una emigración forzada de población civil originados por el conflicto armado
67	E	8 - Terrorismo y Vandalismo	Agresión física	Acto de acometer físicamente a alguien para matarlo, herirlo o hacerle daño. Es la acción intencional y directa contra las personas, no la consecuencia por materialización de otros riesgos. Ejemplo: Hostigamiento a personal en tareas de mantenimiento.
68	E	8 - Terrorismo y Vandalismo	Cultivos ilegales y zonas de reserva	Posicionamiento geográfico de este tipo de actividades ilegales, dificultando el acceso a dichas zonas y por tanto el normal funcionamiento de actividades.

ÍTEM	CATEGORÍA	RIESGO	COMPONENTES DEL RIESGO	OBSERVACIONES
69	E	8 - Terrorismo y Vandalismo	Actuaciones al margen de la ley o contrarias a los intereses de la empresa propietaria y operadora del sistema de infraestructura, por parte de contratistas	Coordinaciones y acuerdos con grupos armados ilegales, colaboración a esos grupos o pago de extorsiones, suministro de información que facilite la perpetración de delitos.
70	E	8 - Terrorismo y Vandalismo	Ataque armado con miras a sabotear los Centros de Control y sus respaldo (el ataque puede ser a través de artefactos explosivos lanzados a distancia)	Tiene consecuencias en la reconstrucción de los centros de control, reposición de equipos, indemnizaciones a empleados afectados o sus familias. Compensaciones si las reparaciones tardaran más de seis meses (es evento de fuerza mayor), además que puede producir la pérdida de la vida de empleados, contratistas y terceros que se encuentren en la sede en el momento del ataque
71	E	9 - Volatilidad de Variables Macroeconómicas	Variaciones desfavorables en índices de precios, que afectan los ingresos o los costos de gestión del sistema de infraestructura, tasas de cambio que afectan el estado de resultados y flujo de caja por el efecto de la exposición cambiaria neta	Índices de Inflación, Índices de crecimiento, tablas salariales, valor del dólar, el Euro y las tasas de cambio locales
72	E	9 - Volatilidad de Variables Macroeconómicas	Variaciones desfavorables en tasas de interés locales e internacionales que afectan el costo de la deuda	Tasas de intereses, deudas públicas y privadas
73	E	9 - Volatilidad de Variables Macroeconómicas	Volatilidad de los precios de los *commodities* que afecta la rentabilidad de los proyectos o los costos de operación	Precios del gas, carbón, petróleo (Combustibles energéticos) y materiales como acero, hierro, aluminio, cobre, que impactan el valor de la infraestructura
74	O	10 - Corrupción, Fraude, Mala Administración	Falsificación o manipulación de información	Crear, acceder, eliminar, modificar, alterar o divulgar información o documentos oficiales de manera inapropiada y dolosa. Incluye falsificación de firmas, cheques, autorizaciones, facturas, historiales de pago, órdenes de compra, certificaciones de experiencia, información en los sistemas, etc; declaración de riesgos insuficiente; reporte no verídico de ingresos, gastos, valoración de activos u otra información financiera. Incluye actividades anticompetitivas e ilícitas como licitaciones colusorias, fijación fraudulenta de precios, manipulación de ofertas. La motivación intencional de causar un daño u obtener un beneficio.
75	O	10 - Corrupción, Fraude, Mala Administración	Desviación de recursos	Cambio indebido de destinación de los recursos de la empresa propietaria y operadora de la infraestructura, para favorecer intereses propios o de terceros. Incluye: utilización inadecuada de los bienes de la empresa, malversación de fondos, pagos a proveedores fantasma, pagos dobles, manipulación de excedentes de tesorería, apropiación indebida de dineros de la empresa, etc.
76	O	10 - Corrupción, Fraude, Mala Administración	Corrupción administrativa	Práctica consistente en la utilización incorrecta de las funciones, medios y recursos de la organización, en provecho económico o de otra índole de sus empleados o de terceros. Puede materializarse como sobornos, dádivas, extorsión, complicidad para fines tales como acceso a información confidencial, adjudicación de contratos, manipulación de pruebas o fallos en procesos judiciales y administrativos. Incluye conflicto de intereses no manifiesto de empleados o administradores y lavado de dinero.
77	O	10 - Corrupción, Fraude, Mala Administración	Hurto o Sabotaje	Sustracción o daño de activos tangibles (equipos, efectivo, inventario, etc) o intangibles (propiedad intelectual, *know how*, mejores prácticas, información, etc.)

ÍTEM	CATEGORÍA	RIESGO	COMPONENTES DEL RIESGO	OBSERVACIONES
78	O	10 - Corrupción, Fraude, Mala Administración	Crímenes a través de los sistemas de información	Prácticas consistentes en la utilización inapropiada de herramientas computarizadas para causar pérdida, desconfiguración o destrucción de datos almacenados en los sistemas informáticos, afectando la integridad, disponibilidad y confidencialidad de la información; modificación fraudulenta de instrucciones y comunicaciones electrónicas computarizadas; virus informáticos, *hacking, phishing*, etc.
79	O	11 - Deficiente gestión del conocimiento	Inadecuada gestión de las destrezas, experiencias y conocimiento del trabajador	Ejecución de tareas por personal que no cumple con los requisitos técnicos y/o psicofísicos para ejecutarlas, lo cual puede desencadenar accidentes que afecta al menos una persona.
80	O	11 - Deficiente gestión del conocimiento	Inadecuada identificación y clasificación de la información	No aplicar o aplicar inadecuadamente la metodología definida para la identificación y clasificación de la información.
81	O	11 - Deficiente gestión del conocimiento	Deficiencias en la gestión del conocimiento a nivel organizacional	Posibles vacíos o aspectos a mejorar en el mecanismo por medio del cual se establecen responsabilidades para la definición de la estrategia de gestión del conocimiento, el proceso operativo que lo soporta, las prácticas, las herramientas, los instrumentos de seguimiento, medición y control.
82	O	11 - Deficiente gestión del conocimiento	Desconocimiento o no aplicación de los mecanismos definidos para el manejo adecuado de la información	La inexistencia o desconocimiento de los lineamientos, procedimientos, herramientas y otros elementos definidos para la seguridad de la información podría causar la pérdida de cualquiera de los criterios de valoración de la información (confidencialidad, integridad, disponibilidad). El desconocimiento se refiere a no saber de la existencia de estos elementos o, conociendo su existencia, no saber cómo utilizarlos
83	O	11 - Deficiente gestión del conocimiento	Deficiencia u obsolescencia en los componentes, servicios e infraestructura de seguridad asociados al ciclo de vida de la información	Fallos en los medios o servicios donde se procesa, almacena o trasmite la información (archivo documental, sistema telefónico y/o plataforma tecnológica informática)
84	O	11 - Deficiente gestión del conocimiento	Uso indebido de la información y del conocimiento	Individuos que se valen, directa o indirectamente, en beneficio propio o de terceros, de la información privilegiada de las empresas propietarias y operadoras del sistema de infraestructura eléctrica
85	O	11 - Deficiente gestión del conocimiento	No disponibilidad de información	Imposibilidad de consecución de la información requerida para realizar estudios y análisis con la precisión requerida (por inexistencia de metodologías y herramientas, dificultad para acceder a la fuente de información, etc), lo cual puede llevar a sub o sobrevaloraciones de especificaciones técnicas, errores de diseño, etc.
86	O	11 - Deficiente gestión del conocimiento	Altos costos administrativos por la ausencia de una gestión integral de riesgos	La estrategia de gestión de riesgos, y protección del sistema de infraestructura crítica, permite controlar las posibles vulnerabilidades en la red y su cadena de valor
87	F	12 - Retos del Crecimiento del Sistema de Infraestructura	Crecimiento sin valor o no alineado con la estrategia	Incursión en negocios o mercados, o inversión en proyectos o empresas que no generan valor a favor de los sistemas de infraestructura, que no contribuyen al cumplimiento de los objetivos propuestos o que no son la mejor alternativa de inversión, comprometiendo recursos y limitando la participación en otros de mayor interés
88	F	12 - Retos del Crecimiento del Sistema de Infraestructura	Incapacidad operativa, financiera o administrativa para afrontar o sostener el crecimiento	No contar con los recursos necesarios para incursionar en negocios o mercados o invertir en proyectos o empresas de acuerdo con lo definido en la estrategia o para cumplir con los planes de negocio. También hace referencia al cambio de objetivos que se pretenden lograr una vez se adquieren las empresas. Adicionalmente se considera dentro de este componente la incapacidad de tomar decisiones que generen mayores rendimientos, o que permitan apalancar el crecimiento del grupo en el futuro.

ÍTEM	CATEGORÍA	RIESGO	COMPONENTES DEL RIESGO	OBSERVACIONES
89	F	12 - Retos del Crecimiento del Sistema de Infraestructura	Decisiones o actuaciones de terceros (socios, banqueros u otros asesores) que dificulten el cumplimiento de la estrategia o afecten negativamente la ejecución de los planes de negocio	Las diferencias en los intereses, estrategias de crecimiento, capacidad financiera o administrativa, etc que se pueden encontrar con los socios implicarían restricciones. Adicionalmente, este riesgo considera el no tener el suficiente poder de negociación para establecer reglas claras de participación de éstos en los negocios en conjunto. Por otra parte, la participación de terceros como socios, banqueros de inversión y demás asesores permite que éstos puedan acceder a información que revele información específica en cuanto a la estructuración de proyectos, lo cual puede representar a futuro la disminución de competitividad en otros escenarios.
90	O	13 - Fallas humanas o de procedimiento	Falta o fallos en la definición de procedimientos	La falta de definición genera vacíos que dan lugar a interpretaciones subjetivas y falta de homologación en el desarrollo de los procesos. Sin embargo, aun cuando el procedimiento esté definido, éste podría estar desactualizado o no divulgado.
91	O	13 - Fallas humanas o de procedimiento	Error u omisión	Actuaciones humanas que ponen en riesgo la eficiencia de los procesos, las cuales no son intencionales para causar un daño. Incluye el no acatamiento de los requerimientos en el aseguramiento de la calidad de los procedimientos y de los procesos.
92	O	13 - Fallas humanas o de procedimiento	Mala concepción de procedimientos de operación, mantenimiento o montaje	Errores de despacho, ejecución de decisiones y errores que involucran las protecciones. Estos últimos pueden variar desde una inadecuada concepción del tipo de protección, hasta errores de cálculo en la configuración o en las pruebas de instalación.
93	O	13 - Fallas humanas o de procedimiento	Accidentes en tareas de mantenimiento o ejecución de un proyecto	Actuaciones que derivan en accidentes industriales, que afectan la integridad física y psicológica de empleados y contratistas, en el sistema de infraestructura eléctrica
94	O	13 - Fallas humanas o de procedimiento	Deficiente gestión operativa	Desviaciones en cualquiera de las fases de planeación, programación, ejecución y evaluación de la red de infraestructura eléctrica (generación, transporte y distribución)
95	O	13 - Fallas humanas o de procedimiento	Gestión inadecuada de la normatividad contable, fiscal, aduanera, cambiaria y financiera	Incumplimiento o diferencias en la interpretación y aplicación de la normatividad externa aplicable al sistema de infraestructura eléctrica, que pueden conllevar a consecuencias financieras y patrimoniales negativas
96	O	14 - Fallos en Equipos, Materiales y hardware	Daño accidental, súbito o imprevisto	Incluye daños en equipos informáticos, equipos de telecomunicaciones, equipos de la operación del sistema de infraestructura (generadores, transformadores, protecciones, etc), virus informáticos y daños en hardware y/o software.
97	O	14 - Fallos en Equipos, Materiales y hardware	Deterioro normal u obsolescencia	Pérdida de las características operativas de los equipos, sistemas o materiales que los hacen inadecuados para las circunstancias actuales (Incluyendo soluciones tecnológicas insuficientes o inadecuadas)
98	O	14 - Fallos en Equipos, Materiales y hardware	Fallos ocultos	Fallos en los materiales o en el funcionamiento de los equipos o sistemas que pueden generar averías que se evidencian con el tiempo o reducción de la vida útil.
99	O	14 - Fallos en Equipos, Materiales y hardware	Incendio	Combustión parcial o total del bien, ocasionado por una fuente de calor que supere los niveles de tolerancia de los materiales.
100	O	14 - Fallos en Equipos, Materiales y hardware	Rotura de maquinaria y obras civiles	Daño material inherente al funcionamiento o manejo (mantenimientos, reparaciones, inspecciones, entre otros) de equipos y obras civiles
101	O	14 - Fallos en Equipos, Materiales y hardware	Errores de diseño	Impactan la efectividad en la operación y gestión del sistema de Infraestructura
102	O	14 - Fallos en Equipos, Materiales y hardware	Ubicación de equipos de energía primaria y equipo de respaldo de confiabilidad y seguridad eléctrica	Tanto los sistemas de energía primaria, como los equipos de respaldo de seguridad y confiabilidad de suministro en la misma habitación para facilitar el mantenimiento

ÍTEM	CATEGORÍA	RIESGO	COMPONENTES DEL RIESGO	OBSERVACIONES
103	O	15 - Inadecuado entrenamiento, formación y capacitación del capital humano	Deficiente gestión en el desarrollo del talento humano	Incluye prácticas inadecuadas de atracción, retención, vinculación y desvinculación de empleados, cuadros de reemplazo, gestión de su funcionamiento, planeación, y formación del recurso humano
104	O	15 - Inadecuado entrenamiento, formación y capacitación del capital humano	Falta, inoportuna o inadecuada toma de decisiones asociadas al recurso humano	Ejecución de tareas por personal que no cumple con los requisitos técnicos y/o psicofísicos para ejecutarlas, lo cual puede desencadenar accidentes que afecta al menos una persona.
105	O	15 - Inadecuado entrenamiento, formación y capacitación del capital humano	Pérdida de capital humano por retiro de personal	Incluye retiro por jubilación, por mejores opciones en otro lugar (salariales, de promoción, etc.)
106	O	15 - Inadecuado entrenamiento, formación y capacitación del capital humano	Restricciones legales para los procesos de desvinculación	Incluye restricciones para la vinculación, desvinculación, procesos laborales, investigaciones administrativas y de entes de control
107	O	15 - Inadecuado entrenamiento, formación y capacitación del capital humano	Contratación incorrecta o desfavorable	Decisiones alrededor de la contratación y su administración que conlleven a pérdidas económicas, de imagen, sanciones o requerimientos de los entes de control
108	O	15 - Inadecuado entrenamiento, formación y capacitación del capital humano	Inadecuada definición y aplicación de autorizaciones para la seguridad de la información y la utilización del conocimiento organizacional	No tener definidas autorizaciones o hacerlo de manera inadecuada podría permitir el acceso a personas no autorizadas y potencialmente podría perderse alguno de los criterios de valoración de la información (confidencialidad, integridad, disponibilidad, transparencia y confiabilidad); el conocimiento podría fugarse o ser utilizado para fines distantes a los intereses organizacionales o incluso en contra de éstos.
109	O	15 - Inadecuado entrenamiento, formación y capacitación del capital humano	Desmotivación del personal frente al trabajo en equipo y compromiso en las empresas propietarias/operadoras	Lo anterior se traduce en baja productividad e ineficiencia en el mantenimiento y operación de la red de infraestructura
110	O	16 - Perturbaciones técnicas en el Sistema de Infraestructura	Deterioro en la capacidad de la Infraestructura	Las plantas de generación que están en operación, pueden exhibir síntomas, como los incrementos en las vibraciones de los ejes.
111	O	16 - Perturbaciones técnicas en el Sistema de Infraestructura	Falta suministro de los servicios auxiliares en una planta o en una instalación	Las estaciones pueden requerir varios servicios auxiliares, sin los cuales no se puede garantizar la operación de una planta o estación
112	O	16 - Perturbaciones técnicas en el Sistema de Infraestructura	Riesgos en el suministro de energía primaria (Combustible para generación)	El riesgo de suministro energía primaria (combustibles, etc.) a las plantas de generación es debido a varios factores ambientales o causados por el hombre, como son: • Medidas climatológicas severas (que impiden distribuir combustibles como carbón, petróleo o gas naturas desde los sitios de almacenamiento a las plantas térmicas); Las dificultades logísticas en el suministro y/o el racionamiento de combustibles, constituyen otro riesgo que puede limitar el funcionamiento de las plantas de generación. • Condiciones hídricas adversas, que repercuten en la disminución de los niveles de los ríos y de los reservorios para generación de energía eléctrica • El caso particular de la energía nuclear, que aunque contribuye a la seguridad de suministro y reduce las emisiones de gases de efecto invernadero, pero es una tecnología con un alto índice de riesgo, en la operativa de las centrales y en el posterior tratamiento y almacenamiento de los residuos nucleares.

ÍTEM	CATEGORÍA	RIESGO	COMPONENTES DEL RIESGO	OBSERVACIONES
113	O	16 - Perturbaciones técnicas en el Sistema de Infraestructura	Riesgos en el personal de operación	El trabajo de rutina en una dependencia es menos dependiente de la disponibilidad de personal que en la estación de trabajo, pero en condiciones críticas, la cantidad de trabajo pendiente por hacer puede ser mucho mayor que el número de equipos de trabajo disponible para atenderlos
114	O	16 - Perturbaciones técnicas en el Sistema de Infraestructura	Riesgos en el personal de control	La mayor parte de las reparaciones, el mantenimiento y nuevas construcciones se realizan en jornadas laborales diurnas, requiriendo planes de trabajo para garantizar la continuidad del servicio, aún bajo contingencias.
115	O	16 - Perturbaciones técnicas en el Sistema de Infraestructura	Inadecuada incorporación de nuevas centrales y de nuevos centros productivos	Fallos y deficiente operación en la incorporación de nuevos centros productivos, que ocasionan la no disponibilidad en el sistema de infraestructura eléctrica
116	O	16 - Perturbaciones técnicas en el Sistema de Infraestructura	Obsolescencia en la tecnología de las plantas generadoras de energía eléctrica	Dentro de los ciclos continuos de mejora y mantenimiento, es imprescindible realizar los trabajos de *overhauling*, renovación y actualización tecnológica, para garantizar la operación eficiente y económica en las plantas
117	O	17 - Vulnerabilidad de los Sistemas TIC	Ataque Informático en Centro de Control	Sistemas de supervisión control y adquisición de datos (SCADA), sistemas de control de transporte y distribución de energía (DCS), controladores lógicos programables (PLCs) que controlan la producción energética, están interconectados mediante redes, y también son accesibles de forma remota
118	O	17 - Vulnerabilidad de los Sistemas TIC	Pérdidas de datos en el sistema informático	Pérdida de información catalogada como crítica en el Sistema de Gestión de Seguridad de la Información, por borrado o daño irreparable en uno de los dispositivos tecnológicos de almacenamiento. La información de respaldo no se recupera oportunamente.
119	O	17 - Vulnerabilidad de los Sistemas TIC	Fallos en la confidencialidad e integridad de la información	El acceso no autorizado, cambios en la información, divulgación o conocimiento de la información confidencial o secreta, que ocasiona perjuicios a las empresas propietarias y gestoras de la red de infraestructura eléctrica
120	O	17 - Vulnerabilidad de los Sistemas TIC	No disponibilidad de los sistemas TIC	Interrupción de los servicios de la plataforma tecnológica en periodos no programados
121	O	17 - Vulnerabilidad de los Sistemas TIC	Deficiencia en la infraestructura de telecomunicaciones (Telemedición de fronteras, intranet, internet, SCADA, extranet, etc)	La tecnología de información constituye la red nerviosa del sistema de infraestructura. Deficiencia en el funcionamiento, impide el adecuado control y gestión
122	I	18 - Cumplimiento y calidad en el suministro eléctrico	Balance entre Generación y Demanda	Los cambios súbitos en generación o en demanda resultan en un desbalance y puede ser debido a numerosas causas: Pérdidas de transferencias desde sistemas externos o redes de baja tensión; Disparos de los circuitos de transporte (Aislando las partes del sistema con mejor funcionamiento en generación o en demanda, etc…) Como comentario general, esta forma de perturbación puede ser una de las más peligrosas para garantizar la viabilidad del sistema. Es una de las causas más frecuentes que puede resultar en desbalances de otras partes del sistema (Fenómeno en cascada), causando más desbalances en otras regiones.
123	I	18 - Cumplimiento y calidad en el suministro eléctrico	Dificultades en el control de despacho de electricidad con energías renovables	El problema principal es que los parques eólicos no garantizan el suministro continuo de energía al sistema. Además, al ser una energía que no se puede programar con antelación, es necesario mantener una alimentación de reserva (por ejemplo, térmicas, de gas o carbón) que mitiga la variabilidad del viento.

ÍTEM	CATEGORÍA	RIESGO	COMPONENTES DEL RIESGO	OBSERVACIONES
124	I	18 - Cumplimiento y calidad en el suministro eléctrico	Riesgos de fallos en las plantas de generación	. De hecho, la probabilidad de riesgo en los generadores, son una de las formas más comunes de falla en una infraestructura eléctrica. • El margen de generación se propaga entre todo el sistema • En consecuencia, la pérdida de uno o varios generadores repercute en menor o mayor medida a lo largo de toda la red. • La pérdida de un generador puede ser consecuencia de que falle una parte de alguna instalación auxiliar.
125	I	18 - Cumplimiento y calidad en el suministro eléctrico	Condiciones de operación o de fallos dentro de las plantas	Las condiciones que puedan llevar a generar fallos dentro de un sistema (grande o pequeño) pueden incluir: • Sobrecargas. • Tensiones fuera de los límites. • Frecuencias fuera de los límites. • Inestabilidad (Transitorios, Dinámicos, Tensiones). • Desconexión de subestaciones o estaciones de generación. • División del sistema.
126	I	18 - Cumplimiento y calidad en el suministro eléctrico	Incidentes operacionales del sistema de potencia, que ocasionan modos de fallo en la Regulación Primaria, Regulación Secundaria, Regulación Terciaria y Control de Tensión en la Red	Algunos de los incidentes que pueden llevar a estas condiciones son: • Fallos en equipos primarios. • Mala operación de los equipos de protección. • Mala operación en las comunicaciones. • Mala configuración de los parámetros de los equipos de protección. • Tensiones por fuera de límites. • Mala configuración de los rangos para funcionamiento tanto en estado permanente, como en estado transitorio. • Oscilaciones dinámicas. • Huecos de Tensión.
127	I	19 - Riesgo Reputacional y de Imagen Pública	Actuaciones indebidas u omisiones por parte de personal interno o agentes externos	Podrían entenderse como actuaciones indebidas el déficit de transparencia, las actuaciones públicas de agentes externos o personal interno para desprestigiar las empresas de infraestructura eléctrica, las actuaciones empresariales e individuales no coherentes con el código de ética o en general con el marco de referencia corporativo o cualquier otro evento que dé lugar a una valoración desfavorable de las empresas
128	I	19 - Riesgo Reputacional y de Imagen Pública	Liderazgo de las empresas propietarias y operadoras del sistema de infraestructura	Carencias en la definición y actualización de lineamientos y directrices que fortalezcan la gestión de liderazgo, prevengan de una actuación empresarial por fuera de lo establecido en los modelos de negocio, operativo y de gobierno y faciliten el logro de la unidad de propósito y dirección del grupo empresarial.
129	I	19 - Riesgo Reputacional y de Imagen Pública	Actuación de empresas por fuera del modelo de gobierno corporativo	No implementación de las directrices, lineamientos y prácticas definidas en sus Modelos de Negocio, Operativo y de Gobierno.
130	E	20 - Deficiencias de proveedores y subcontratistas del sistema	Deficiencia en el proceso de contratación	Hace referencia al proceso interno que se surte para realizar una contratación y comprende desde la definición de la necesidad hasta la finalización del plazo contractual. De este proceso hace parte la normatividad, la documentación oficial, los procedimientos para seguimiento y monitoreo de las actividades contractuales y la evaluación del proveedor. Dentro de las deficiencias se incluyen los vacíos en los requerimientos de información, inexactitud en la definición del alcance del contrato, demoras en el proceso interno de contratación, falta de claridad de las causales de terminación del contrato, falta o deficiencia en el seguimiento del funcionamiento del proveedor
131	E	20 - Deficiencias de proveedores y subcontratistas del sistema	Pago inoportuno de obligaciones contractuales con proveedores y subcontratistas	Actividades tan importantes como el mantenimiento de la red, adquisición de equipos, realización de proyectos, obras, servicios y demás tareas, se pueden suspender, afectando la operación de la red.

ÍTEM	CATEGORÍA	RIESGO	COMPONENTES DEL RIESGO	OBSERVACIONES
132	E	20 - Deficiencias de proveedores y subcontratistas del sistema	Incumplimiento de las condiciones pactadas	Hace referencia a los riesgos asociados a los proveedores (componente externo): incapacidad técnica, financiera o administrativa de un proveedor, que dificulte o impacta el funcionamiento del sistema de infraestructura. Estos riesgos se derivan de las relaciones de interdependencia, la falta o deficiente aplicación de criterios de diversificación y seguimiento de proveedores.
133	E	21 - Vulnerabilidad de la cadena de suministro	Deficiencias en el suministro de gas natural para operar las plantas de generación.	Esto puede originarse por factores como: 1. Alta dependencia de regiones o países productores y falta de diversificación, que impactan la confiabilidad del suministro. 2. Imposibilidad de explotar el recurso a nivel regional o nacional. 3. Falta de mallado de la red de transporte y distribución de gas, o indisponibilidad de plantas compresoras. 4. Mercado limitado, especulación y volatilidad de precios del combustible, que lo hacen inaccesible 5. Indisponibilidad de la infraestructura de suministro de gas natural
134	E	21 - Vulnerabilidad de la cadena de suministro	Deficiencias en el suministro de carbón para operar las plantas de generación.	Esto puede originarse por factores como: 1. Alta dependencia de regiones o países productores y falta de diversificación, que impactan la confiabilidad del suministro. 2. Imposibilidad de explotar el recurso a nivel regional o nacional. 3. Fallo en la logística de transporte del mineral 4. Mercado limitado, especulación y volatilidad de precios del combustible que lo hacen inaccesible
135	E	21 - Vulnerabilidad de la cadena de suministro	Deficiencias en el suministro de petróleo y sus derivados (Diesel, Fuel Oil, Gasolina) para operar plantas de generación.	Esto puede originarse por factores como: 1. Alta dependencia de regiones o países productores y falta de diversificación, que impactan la confiabilidad del suministro. 2. Imposibilidad de explotar el recurso a nivel regional o nacional. 3. Falta de mallado de la red de transporte y distribución de gas, o indisponibilidad de refinerías 4. Mercado limitado, especulación y volatilidad de precios del combustible que lo hacen inaccesible 5. Prioridad para atender otros sectores económicos, como transporte o industria 6. Indisponibilidad de oleoductos, o de tanques de almacenamiento
136	E	21 - Vulnerabilidad de la cadena de suministro	Deficiencias en el tratamiento y en los procesos requeridos dentro de las plantas nucleares	Esto puede originarse por factores como: 1. No disponibilidad de sitios para almacenamiento de residuos 2. Cumplimiento de la vida útil de la planta de generación 3. No disponibilidad operativa de los reactores
137	E	21 - Vulnerabilidad de la cadena de suministro	Tendencias divergentes en el precio de derivados del petróleo (Fuel Oil, Diesel)	Altos precios del petróleo afectan la capacidad de generación y de atención de la demanda, dado que otros sectores de la economía tienen prelación en el despacho del combustible
138	E	21 - Vulnerabilidad de la cadena de suministro	Tendencias divergentes en el precio del gas natural	Altos precios del gas natural afectan la capacidad de generación y de atención de la demanda, dado que otros sectores de la economía tienen prelación en el despacho del combustible
139	E	21 - Vulnerabilidad de la cadena de suministro	Falta de infraestructura dual de consumo de combustible en las plantas de generación	La existencia de equipos de back-up en las calderas y/o turbinas, permiten amortiguar el efecto de los daños en caso que falle el equipo principal
140	E	21 - Vulnerabilidad de la cadena de suministro	Disminución de la capacidad de generación, por fallos en el suministro de combustibles	Por efectos de la no disponibilidad de combustibles primarios, debido a la interrupción del transporte

ÍTEM	CATEGORÍA	RIESGO	COMPONENTES DEL RIESGO	OBSERVACIONES
141	E	21 - Vulnerabilidad de la cadena de suministro	Disminución de la capacidad de generación, por imposibilidad de operar plantas hidroeléctricas	Niveles bajos en embalses, requieren la suspensión de la operación de una o varias turbinas en las plantas hidroeléctricas, suspendiendo la generación eléctrica
142	E	21 - Vulnerabilidad de la cadena de suministro	Disminución de la capacidad de generación, por condiciones adversas en el recurso renovable	La no disponibilidad de recurso eólico, o de radiación solar, imposibilitan la inyección de energía a la red eléctrica.

Esta propuesta metodológica de **mapas de riesgos** tiene aplicabilidad integral en el caso de organizaciones integradas verticalmente (es decir, que la misma empresa desarrolla los negocios de generación, transporte, distribución y comercialización de energía). Si no hay integración vertical, es preferible identificar los riesgos por separado, según afecten cada elemento de la cadena de valor.

Es evidente que los riesgos no pueden ser eliminados totalmente y que algún nivel de riesgo debe ser aceptado por la sociedad, existiendo siempre un balance entre costes y niveles de seguridad.

3.3.4.4 Aplicación de las componentes de riesgo a la cadena de valor

La etapa de identificación desarrollada en el marco de la gestión de riesgos que se ha presentado en la Tabla 3.3 está constituida por 4 categorías, 21 riesgos y 142 componentes de riesgo.

En la Figura 3.10 se indica el número de componentes de riesgo asociadas a cada uno de los 21 riesgos identificados. En dicha figura también se presenta un resumen de la clasificación de las componentes de riesgo del sistema de infraestructura eléctrica se presenta.

Se observa la existencia de riesgos cuyo origen es de tipo técnico y no-técnico, aunque existen algunos casos en que tienen ambos orígenes (por ejemplo, la vulnerabilidad de la cadena de suministro para las plantas de generación, o los riesgos de incumplimiento en indicadores de calidad).

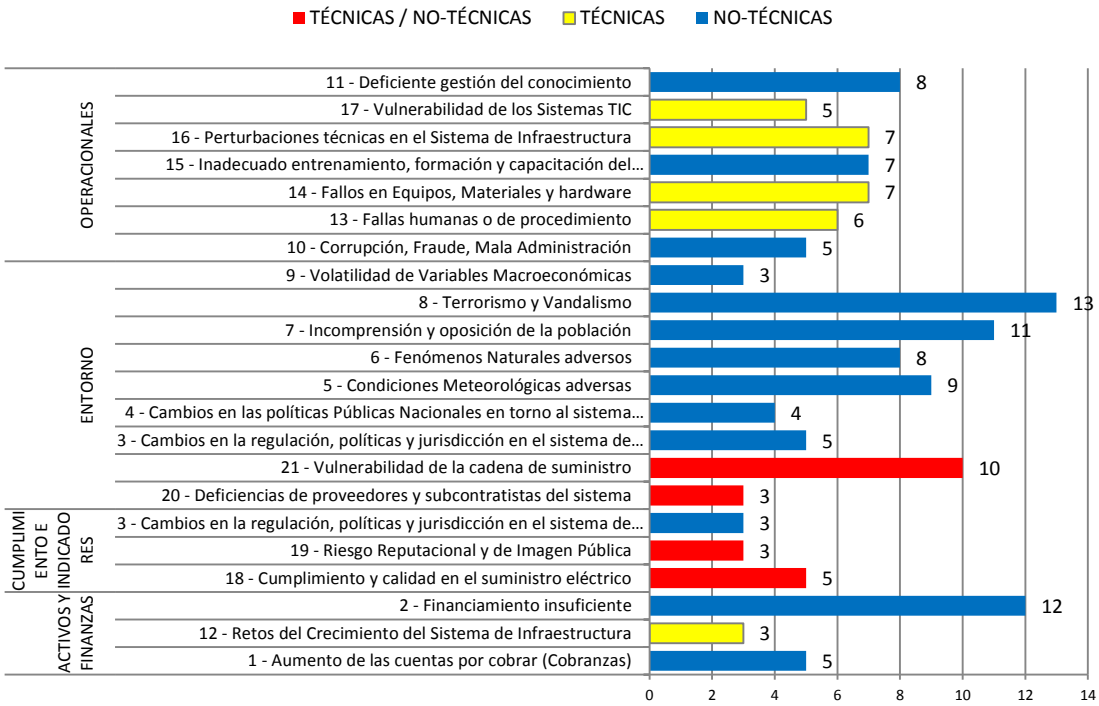


Figura 3.10: Componentes de riesgo en el sistema de infraestructura eléctrico

Una forma de validar la adecuada selección de estas componentes de riesgo es estudiar cómo afectan a cada una de las actividades de la cadena de valor del suministro eléctrico: generación, transporte, distribución, comercialización y servicio al cliente final, como se muestra en la Figura 3.11. Esta figura contiene la clasificación de las componentes de riesgo, teniendo en cuenta si una componente afecta uno o más elementos de la cadena de valor

Se puede observar que una componente de riesgo puede afectar a todas y cada una de las etapas de la cadena de valor (por ejemplo, las perturbaciones técnicas al sistema). Sin embargo, como se presenta en la Figura 3.11, la mayor cantidad de componentes de riesgo que afectan la cadena de valor pertenecen a la categoría de riesgos de entorno y operacionales, que a su vez son amenazas de tipo no-técnico.

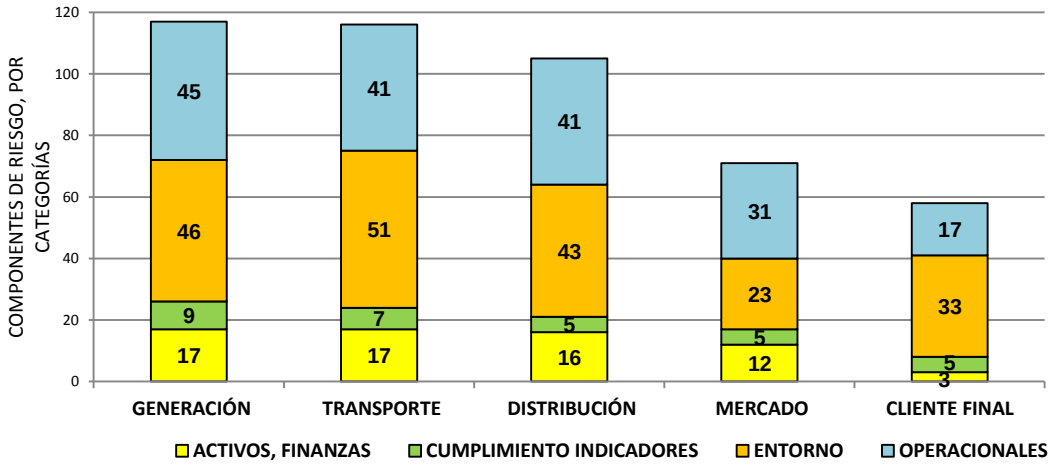


Figura 3.11: Componentes de riesgo que afectan la cadena de valor en el sistema de infraestructura eléctrica

Los subsistemas de generación, transporte y distribución tienen mayor exposición a las componentes de riesgo, dado que son los sistemas que reúnen mayor cantidad de activos, además que tienen mayor cobertura geográfica y mayores interrelaciones con otros sistemas económicos y sociales.

3.4 COMENTARIOS AL CAPÍTULO

Se ha propuesto desarrollar la etapa de identificación en los planes de protección de infraestructura mediante la utilización de mapas de riesgos. Un mayor nivel de detalle en esta actividad ha requerido la determinación de las respectivas componentes de riesgo y su categorización. A tal efecto, se ha presentado una aplicación de la metodología al sistema eléctrico colombiano que contiene 21 riesgos, clasificados en cuatro categorías (riesgos operacionales, de entorno, financieros e indicadores de calidad y cumplimiento) e interdependientes entre sí. También se han determinado 142 componentes de riesgo, clasificados tanto por su naturaleza como por la afectación en la cadena de valor del sistema de infraestructura eléctrica.

La generalización de la estrategia metodológica aquí presentada permite cumplir con los requerimientos legales establecidos en la Directiva 114/CE, en el NIPP y en legislaciones nacionales, las cuales exigen la identificación y designación de infraestructuras, sistemas y activos, para mejorar la prevención, preparación y respuesta frente a riesgos y amenazas.

La propuesta de trabajar con mapas de riesgos se apoya en el análisis del estado del arte, confirmando la universalidad de la técnica y la aceptación de la misma. Este enfoque metodológico, tal y como se propone, es novedoso y más completo que otras estrategias de identificación de riesgos.

Los resultados de esta metodología tienen aplicabilidad para empresas propietarias y operadoras de los sistemas de infraestructura crítica. También puede resultar de utilidad en la orientación de políticas y regulaciones gubernamentales en torno al tema de protección de infraestructura crítica.

4 EVALUACIÓN DE RIESGOS EN INFRAESTRUCTURAS CRÍTICAS

Una vez realizada la labor de identificación de los riesgos en el sistema de infraestructura crítica, es necesario realizar su valoración. Según el marco de gestión de riesgos, esta etapa consiste en la medición del riesgo frente a su probabilidad de ocurrencia y el impacto de sus consecuencias, de acuerdo con las escalas preestablecidas para cada recurso. Lo anterior permite disponer un esquema de toma de decisiones, que incluye aceptarlos, eliminarlos o gestionarlos.

En este capítulo se realiza una propuesta de metodología de evaluación basada en matrices y cartas de riesgos, fundamentada en la revisión de la literatura especializada. También se propone una aplicación práctica de la propuesta metodológica de evaluación a un caso real.

4.1 OBJETIVO DEL CAPÍTULO

Las actividades que dan continuidad a la identificación de riesgos, como la evaluación y la priorización de acciones, permiten completar el proceso de gestión de riesgos de las infraestructuras, desplegando en última instancia los elementos de defensa para que las amenazas no causen daños.

En este capítulo se realiza la propuesta de una aproximación metodológica para la evaluación de riesgos, en el marco de los requerimientos del NIPP y de la Directiva 114/CE. Básicamente, pretende aplicar una metodología de evaluación que tenga en cuenta los siguientes aspectos:

- Estudiar el estado del arte en cuanto a metodologías y técnicas aceptadas para la valoración de riesgos en sistemas de infraestructuras críticas, complementado con el análisis de herramientas de software y metodologías de protección de infraestructura crítica.
- Presentar una aproximación metodológica aplicable a la valoración de riesgos en infraestructuras críticas del sector eléctrico, a partir de la información contenida en los mapas de riesgos.
- Generar evaluaciones mediante *matrices de riesgos* y *cartas de riesgos*, que comprenden la aplicación de técnicas semicuantitativas, aplicadas al sistema de infraestructura crítica.
- Aplicar la aproximación metodológica en el diagnóstico y planificación de acciones para la protección de infraestructuras energéticas críticas.

Este capítulo también presenta una aplicación del desarrollo metodológico de valoración a partir de un caso de estudio en Colombia, haciendo posible la generación de *matrices y cartas* para evaluación de riesgos*.* Como punto de partida se toman los resultados de la aplicación al mismo caso real de la metodología de identificación de riesgos realizada en el capítulo 3.

4.2 HERRAMIENTAS DE SOFTWARE Y METODOLOGÍAS PARA EVALUACIÓN DE RIESGOS

Dentro del marco de gestión del riesgo en los sistemas de infraestructura, la etapa de evaluación de amenazas es una de las más críticas. A partir de los resultados concluyentes de esta fase, que sigue a la identificación de riesgos, es posible definir e implementar acciones para mitigarlos.

Sobre la base de herramientas y metodologías descritas en el estudio del estado del arte, específicamente en la Tabla 2.3 del capítulo 2 (Aplicaciones y modelos para análisis de vulnerabilidades de Infraestructuras Críticas) se pueden distinguir algunas plataformas para realizar la evaluación de riesgos en el ámbito de las infraestructuras eléctricas, las cuales se presentan en la Tabla 4.1. Esta clasificación hace referencia a 16 plataformas constituidas por herramientas de software (incluyendo sistemas de información geográfica) y metodologías analíticas fundamentadas en funciones de probabilidad, matrices de calificación, teoría de grafos, árboles de decisión. Los criterios de clasificación comprenden:

- **Origen**: En la Tabla 4.1 se indica cuáles de las herramientas y metodologías están fundamentadas en **propuestas metodológicas** enfocadas en técnicas de gestión de riesgos o en el cálculo de indicadores de la red eléctrica. Las **herramientas de software** citadas en la tabla generalmente se apoyan en el paradigma de simulación (dinámica de sistemas, sistemas multiagente, etc) o en formulaciones analíticas clásicas (flujos de carga, probabilidades, análisis estadísticos, etc).
- **Objeto de la evaluación**: Las herramientas y metodologías citadas permiten evaluar los riesgos sobre el sistema eléctrico teniendo en cuenta las consecuencias y severidad de los riesgos, la probabilidad de fallos, los indicadores de desempeño de la red, las posibles emergencias, etc.
- **Presentación de resultados**: Para realizar el proceso de evaluación de riesgos, cada herramienta y metodología utiliza técnicas semicuantitativas que reflejan la calificación de los riesgos, o técnicas cuantitativas que valoran indicadores de desempeño del sistema a nivel técnico, económico y social.

Tabla 4.1: Clasificación de herramientas y metodologías para evaluación de riesgos en infraestructuras eléctricas

CRITERIO DE CLASIFICACIÓN		Athena	CASCADE	CEESA	CIMS	COMM-ASPEN	DEW	EMCAS	FAIT	Fort Future	GoRAF	HAZOP	Teoría Grafos	MIA	Modular Model	Matriz Calificación	NIPP	Directiva 114/CE
PROPUESTA METODOLÓGICA	GESTIÓN DE RIESGOS																●	●
	INDICADORES DE LA RED											●	●			●		
HERRAMIENTA SOFTWARE	MULTIAGENTES				●	●		●		●	●							
	DINÁMICA SISTEMAS														●			
	TEORÍA DE GRAFOS	●											●	●				
	SISTEMA INFORMACIÓN GEOGRÁFICA			●	●				●	●								
	ANÁLISIS ESTADÍSTICO		●				●	●										
	BASES DATOS RELACIONAL	●									●	●		●				

CRITERIO DE CLASIFICACIÓN		Athena	CASCADE	CEEESA	CIMS	COMM-ASPEN	DEW	EMCAS	FAIT	Fort Future	GoRAF	HAZOP	Teoría Grafos	MIA	Modular Model	Matriz Calificación	NIPP	Directiva 114/CE
OBJETO EVALUACIÓN	INTERDEPENDENCIAS	●		●						●	●		●	●	●	●	●	
	ESTABILIDAD TÉCNICA DE LA RED		●				●											
	RESPUESTA EN EMERGENCIAS	●			●	●									●		●	
	POLÍTICAS, REGULACIONES							●					●		●		●	●
	CADENA DE SUMINISTRO (GENERACIÓN)			●				●		●					●			
	PROBABILIDAD DE FALLOS		●				●		●	●								
	IMPACTO EN EL SISTEMA				●	●			●	●				●		●		
	INDICADORES DESEMPEÑO									●			●		●	●	●	●
PRESENTACIÓN RESULTADOS	RESPUESTA DINÁMICA DE COMPONENTES		●				●											
	ECONOMÍA DE MERCADO			●				●	●		●				●			
	GRAFOS INTERRELACIONADOS	●										●	●	●	●			
	UBICACIÓN GEOGRÁFICA NODOS			●	●					●		●						
	MATRIZ DE RIESGOS	●		●					●	●		●				●	●	●

Algunas de herramientas se apoyan en el paradigma de simulación con sistemas multiagentes o con dinámica de sistemas, lo cual tiene la conveniencia de evaluar los impactos de políticas y regulaciones en el sector en el medio plazo.

En la Tabla 4.1 se resume el estudio individual de:

12 herramientas de software: *Athena [DRABBLE, BLACK et al., 2009], CASCADE [NEWMAN, NKEI et al., 2005], CEEESA [Argonne Labs & PEERENBOOM, 2010], CIMS [Idaho & DUDENHOEFFER, 2006], COMM-ASPEN [Sandia Labs, BARTON et al., 2004], DEW [BROADWATER, 2006], EMCAS [Argonne Labs & CONZELMANN, 2008], Fort Future [USACE, ERDC et al., 2010], FAIT [Sandia Labs & BROWN, 2005a], GoRAF [JEBARAJ & INIYAN, 2006], MIA [ENEA, Europa et al., 2010], Modular Dynamic Model [BEYELER, BROWN et al., 2002]*)

5 metodologías: *HAZOP [ISOGRAPH Inc, 2008], TEORÍA GRAFOS [HOLMGREN, 2006; JOHANSSON, 2010], Matrices de Calificación, NIPP [NIPP, 2009], Directiva 114//CE [CUE, 2008]*

Con la finalidad de profundizar en el análisis más detallado de las técnicas a las que hace referencia, puede apreciarse en la Tabla 4.2 el resumen de las características empleadas por cada uno de los modelos de evaluación de

vulnerabilidades en infraestructuras críticas en el sector eléctrico. Dicha información se construye a partir de las fichas técnicas presentadas de cada herramienta y metodología.

Tabla 4.2: Herramientas y metodologías para la Evaluación de Riesgos en Infraestructuras Eléctricas.

Herramienta / Metodología	Resultado de Evaluación	Modelización Principal	Fortaleza	Debilidad
Athena	Valoración de dependencias entre la infraestructura eléctrica y sus usuarios, determinación de los nodos críticos, efectos en cascada sobre el sistema y calificación de los nodos más vulnerables durante emergencias	Herramienta de software. Fundamentos en Teoría Grafos y Árboles de Decisión	Relaciones de dependencia y realimentación en los riesgos, de un nodo de riesgo sobre otro. Realización de un modelo ontológico que admite cierta abstracción	Se requiere amplio conocimiento de la red, sus interdependencias, nodos y personas involucradas en su operación, para alimentar los datos del sistema
CASCADE	Fallos en cascada como un proceso iterativo, evaluando la probable fallo en un nodo cuando se le transfiere cargas de circuitos en fallo hasta que cada red llega a su límite	Herramienta de software. Fundamentada en matrices de calificación y cuantificación de probabilidades de fallos	Calificación de la Probabilidad de fallos de uno o varios nodos. Metodología iterativa que permite predecir la vulnerabilidad de la red y sus componentes	Limitación a fallos técnicos. No se evalúa el impacto de la falla
CEEESA	Funcionamiento del sistema, incluyendo variables técnicas de operación en el sistema de gas, que suministra combustible a las plantas de generación	Herramienta de software, que combina Matrices de Calificación, control de variables operativas y SIG	Calificación de la vulnerabilidad en la cadena de suministros (Infraestructura de gas). Evaluación de vulnerabilidad en las plantas de generación de gas	Exigencia de disponibilidad de datos precisos y constantemente actualizados.
CIMS	Valoración del comportamiento entre componentes e interdependencias en la red, así como el cálculo de la respuesta y recuperación del sistema	Herramienta de software, que combina simulación multiagente con SIG	Modelización interactiva en 3D de entidades en movimiento (vehículos, equipos, personas) Construcción de modelos de infraestructura utilizando imágenes de mapas, fotos satelitales, y otras imágenes electrónicas	Mayor enfoque en riesgos no técnicos y sólo para casos de emergencia.
COMM-ASPEN	Valoración de la interdependencia entre las comunicaciones, los sistemas financieros y el sistema eléctrico. Indicadores de los tiempos de recuperación del sistema ante una vulnerabilidad	Herramienta de software de simulación multiagentes combinada con simulación Montecarlo	Predicción del comportamiento de los nodos críticos, las interacciones entre componentes y posibilidad de evaluar políticas	Enfoque únicamente en interdependencia Comunicaciones - Electricidad. Se requiere alto nivel de experticia y programación en lenguajes de agentes
DEW	Valoración de las contingencias, parámetros operativos (corrientes de falla, impedancias de cortocircuito, sobrevoltajes, etc.), estrategias de reconfiguración y comportamiento de protecciones, ante probables eventos de fallos en cascada	Herramienta de software de simulación dinámica, teoría de circuitos de potencia, y configuración de redes	Incorporación de toda la red de distribución de subestaciones. Aplicable a modelos multidisciplinarios con la cadena de valor. Maximización en el uso de todas las fuentes de datos disponibles	Aplicable a modelos sencillos, con baja complejidad. Requerimiento de datos precisos para garantizar respuestas útiles. No se pueden evaluar políticas
EMCAS	Evaluación del mercado, tendencias económicas, nodos y enlaces críticos (que pueden llegar a los cientos de miles de conexiones)	Herramienta de software de simulación discreta multiagentes	Aplicable a modelos complejos. Determinación de tendencias en precios, volúmenes, transacciones en el mercado, nodos y conexiones físicas en el sistema.	Alta experticia para introducir datos. Bajo margen de maniobra para considerar incertidumbre en los modelos

Herramienta / Metodología	Resultado de Evaluación	Modelización Principal	Fortaleza	Debilidad
FAIT	Valoración de las interdependencias, usando datos como Proximidad, fronteras, propiedad, localización. También permite estimar el impacto económico de una vulnerabilidad en la red	Herramienta de software, que combina Matrices de Calificación, con SIG	Información se recopila a través de metadatos, y mediante integración con buscadores virtuales, lo cual facilita la identificación de riesgos en escenarios de poca información	Modelo limitado, especificado únicamente en Entradas/Salidas
Fort Future	Capacidad de las instalaciones militares, según el objetivo para el que se proyecten	Herramienta de software, que combina simulación multiagente con SIG	Amplio apoyo en información virtual. Métricas se definen automáticamente según los riesgos que se vayan identificando en la red.	Modelo no disponible para aplicaciones civiles.
GoRAF	Indicadores sobre el grado en que una organización depende de los servicios y recursos proporcionados por la infraestructura tecnológica	Herramienta de software. Combinación de agentes con árboles de Decisión	Simulación de las dependencias de la red con los sectores de una empresa	Herramienta no comercial. Modelos limitados sólo a organizaciones y empresas. No disponible para aplicaciones civiles
HAZOP	Ordenamiento y priorización de los riesgos identificados, según la calificación de los expertos involucrados en la recolección de información	Metodología que combina el paradigma relacional, con Técnicas de Gestión de Riesgos	Amplio conocimiento en la industria. El conocimiento experto se usa para calificar los riesgos.	Técnicas exhaustivas, con conocimientos muy especializados. Alta dedicación para el mantenimiento de las variables identificadas y su calificación
TEORÍA GRAFOS	Medidas de centralidad, similitud y distribución que afectan cada uno de los nodos del sistema de infraestructura	Modelos de redes complejas	Representación de la infraestructura mediante grafos, identificando su grado de conectividad, o sus distancias geodésicas	Resultados aproximados
MIA	Se obtienen métricas de densidad, tiempo de respuesta y dependencia entre los componentes de la infraestructura. Se miden las relaciones entre las capas físicas y lógicas de las redes	Herramienta de software, que combina Árboles de Decisión, Teoría de Grafos y Matrices de Calificación	Determinación de métricas y topologías en interrelaciones funcionales entre las infraestructuras eléctricas y TIC.	Falta de intercambio de información, debido a las limitaciones de confidencialidad o las dificultades reales en su adquisición
Modular Dynamic Model	Propagación en el tiempo de perturbaciones a través de una cadena de interdependencias	Modelo de simulación con Dinámica de Sistemas	Óptima comprensión del sistema de riesgos e infraestructura. Posibilidad de evaluar políticas y regulaciones. Predicción del comportamiento de la red. Inclusión de riesgos técnicos y no técnicos	Altísima complejidad en la determinación de las interrelaciones de riesgos para la construcción de los modelos de simulación
MATRIZ CALIFICACIÓN	Valoración cuantitativa o semicuantitativa de variables identificadas en cada riesgo de la cadena de valor	Matrices de riesgo con evaluación semicuantitativa	Amplia difusión en organizaciones energéticas. Ideal para valorar riesgos mediante datos de personas expertas	Evaluación aproximada y global. Se emplean variables no cuantitativas, sino escalas.
NIPP	Segunda parte de la metodología de análisis de riesgos. Requisito previo para continuar con la priorización de acciones en el control de amenazas	Metodología de aplicación de las Técnicas Administración Riesgos Sugerencia de uso de matrices de riesgo	Cualquier metodología es válida para recopilar información en la evaluación de riesgos. Enfatizando en aquellos activos que afecten la economía y la seguridad nacional.	No existe un planteamiento metodológico con fundamentación matemática.

Herramienta / Metodología	Resultado de Evaluación	Modelización Principal	Fortaleza	Debilidad
PEPIC (Directiva 2008/114/CE)	Énfasis en medidas de seguridad permanentes, que incluyen medidas técnicas, medidas organizativas, control verificación, comunicación, concienciación y formación, en función de los diferentes niveles de riesgo de la red energética	Metodología de aplicación de las Técnicas Administración Riesgos. Sugerencia de uso de matrices de riesgo	Para las infraestructuras que prestan servicios esenciales, se tendrán en cuenta la disponibilidad de alternativas y la duración de la perturbación o recuperación.	No existe un planteamiento metodológico con fundamentación matemática. Mayor enfoque en riesgos no técnicos. La cuantificación de riesgos se realiza en un entorno geopolítico.

En resumen, el área de aplicación de las herramientas y metodologías presentadas en la Tabla 4.1 consiste en:

- Evaluación de interdependencias entre activos de las infraestructuras, por ejemplo, interdependencias entre el sistema bancario y el sistema eléctrico (21%).
- Respuestas ante emergencias (13%).
- Impacto de las políticas y regulaciones en el funcionamiento de la infraestructura (13%).
- Cumplimiento de indicadores de funcionamiento en las infraestructuras (13%).
- Estimación de las probabilidades de fallo de los activos que componen la infraestructura (11%).
- Impacto del suministro de combustible en la generación eléctrica (11%).
- Estabilidad del sistema de potencia (5%).

En las metodologías y herramientas se admite el uso de las siguientes estrategias para evaluar los riesgos en la infraestructura:

- Matrices de riesgo (30%).
- Grafos y medidas asociadas (22%).
- Indicadores econométricos (22%).
- Georreferenciación de los activos y nodos más vulnerables (17%).
- Probabilidades y respuestas dinámicas de los componentes (9%).

Las metodologías basadas en **matrices de riesgos** son las más utilizadas y se convierten en una alternativa a tener en cuenta en el proceso de calificación de amenazas al sistema de infraestructuras eléctricas. Esta metodología se fundamenta en la utilización de matrices de calificación a las que se asocia la información de evaluación semicuantitativa de cada riesgo.

La revisión de las diferentes herramientas y metodologías presentadas en la Tabla 4.1 y en la Tabla 4.2 evidencian la aceptación de esta técnica, así como la universalidad de la misma en la etapa de evaluación, por las siguientes razones:

- Las matrices de riesgos contienen información de análisis sobre cada una de las amenazas que afectan al sistema de infraestructura y pueden ser aplicadas al listado de componentes de cada riesgo. Es decir, permiten efectuar la evaluación semicuantitativa de los mapas de riesgos.
- La técnica es universal y también se puede aplicar a otros sectores de infraestructuras críticas, incluyendo los elementos de la cadena de valor que los conforman. Admiten el procesamiento de información obtenida de fuentes humanas o mediante documentación disponible. Adicionalmente, dada su sencillez, consume menos tiempo y tiene pocos requerimientos información.
- Se puede combinar con otras propuestas metodológicas como HAZOP, o con las estrategias de gestión especificadas en la Directiva 114/CE y el NIPP y es suficiente para valorar la mayoría de los riesgos.

Algunos aspectos que no pueden ser cubiertos mediante las matrices de riesgos incluyen las siguientes particularidades:

- Tratándose de una herramienta de evaluación semicuantitativa sólo se admite el uso de expresiones matemáticas simples para calcular indicadores del estado de las diferentes condiciones del sistema.
- La técnica de matrices de riesgo es muy intuitivita y global, por cuya razón, en la medida que la etapa de identificación requiera datos precisos, la técnica será insuficiente para el procesamiento de variables cuantitativas o para efectuar una evaluación rigurosa de diferentes opciones en el tratamiento de riesgos.

El uso de otras herramientas y metodologías para evaluación de riesgos, diferentes de las matrices de riesgo, tienen campos de aplicación muy específicos, con mayor dificultad para abarcar la evaluación del conjunto de riesgos que se ha identificado en una etapa anterior. Además están limitadas a grupos específicos de datos disponibles y pueden requerir de mucha experiencia para obtener resultados razonables.

4.3 PROPUESTA METODOLÓGICA PARA VALORACIÓN DE RIESGOS

Evaluar un riesgo significa medirlo frente a su probabilidad de ocurrencia y el impacto de sus consecuencias de acuerdo con unas escalas predefinidas [AS/NZS, 1999]. Desde el punto de vista clásico, la evaluación y valoración de riesgos se realiza a partir de los resultados obtenidos al estimar la probabilidad e impacto de cada una de las componentes de riesgo [COSO, 2004]. De esta manera, se establece el grado de exposición de la infraestructura a las amenazas identificadas para posteriormente fijar las acciones requeridas para su tratamiento.

Las estrategias para realizar la valoración de los riesgos en el sistema de infraestructura se pueden considerar:

- ***Estrategia de evaluación cualitativa y semicuantitativa***: En esta etapa se evalúa la prioridad de los riesgos identificados. En este caso se utilizan **Variables Cualitativas** usando la probabilidad de ocurrencia y el impacto correspondiente mediante etiquetas lingüísticas. Es decir, a variables que por algún motivo no se pueden medir de forma numérica se les asigna una característica como valor (por ejemplo, probabilidad *alta, media o baja*).
- ***Estrategia de evaluación cuantitativa***: En esta etapa se evalúa la prioridad de los riesgos identificados utilizando **Variables Cuantitativas**, es decir que se pueden expresar numéricamente. La naturaleza numérica de las variables cuantitativas permite un tratamiento estadístico más elaborado. Por ello facilitan una descripción más precisa y detallada de la variable. Las variables cuantitativas, propiamente dichas, son de intervalo y de razón (o de cociente).

En caso de realizar una *evaluación cuantitativa*, algunos riesgos pueden resultar difíciles de valorar matemáticamente (por ejemplo, los términos “terrorismo” o “corrupción”), por cuya razón la *evaluación semicuantitativa* ofrece la ventaja de ser mucho más sencilla e intuitiva. Dicha valoración está asociada al conocimiento experto, que será útil en la preparación de planes de protección de infraestructuras críticas.

En esta sección se propone una metodología de evaluación semicuantitativa de riesgos, la cual permite su implementación mediante **matrices de riesgo**. La formulación de dicha propuesta tiene en cuenta los siguientes aspectos:

- La valoración de riesgos puede ser de tipo pura o residual, según se explica en la sección 4.3.1.1.

- La evaluación semicuantitativa pura se puede aplicar a cada componente de riesgo en cada uno de los recursos existentes en cada empresa y organización (sección 4.3.1.2).
- La valoración de cada componente de riesgo se efectúa mediante el producto de la calificación asignada a su probabilidad y la calificación asignada a su impacto, como se explica en la sección 4.3.1.3. Como resultado, los riesgos pueden ser clasificados en los siguientes rangos: *aceptables*, *tolerables*, *importantes* y *críticos*.

La aplicación de la propuesta metodológica a un caso real de estudio en el sistema eléctrico colombiano permitirá generar una *carta de riesgos*, que representará gráficamente la evaluación semicuantitativa de cada riesgo, como se presenta en la sección 4.3.2,

4.3.1 ESTRATEGIA DE EVALUACIÓN SEMICUANTITATIVA

En general, las recomendaciones de evaluación sugeridas por los planes de protección NIPP y por la Directiva 114/CE, proporcionan una base objetiva para la gestión del riesgo y las posteriores decisiones de seguridad. Como se ha presentado en la revisión bibliográfica, existen varias técnicas para realizar este proceso de valoración. La técnica más aceptada son las *matrices de calificación de riesgos*, las cuales resumen la evaluación semicuantitativa de la posible afectación que genera cada uno de los riesgos sobre la infraestructura eléctrica, en términos de la probabilidad y el impacto de sus consecuencias [LÓPEZ & ARBOLEDA, 2010; PRUYT & WIJNMALEN, 2010; EC, 2011a]. En general, el riesgo se mide en función de su probabilidad e impacto en el sistema.

$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto} \qquad [4.1]$$

- ***Probabilidad***: Representa la frecuencia con la que se puede manifestar un riesgo en un determinado periodo de tiempo. Esta calificación se puede asociar con el análisis de expertos que incluya previsión de los métodos de ataque y daños al sistema de infraestructura. Para realizar la medición semicuantitativa de la probabilidad se utilizan escalas de calificación, como las que se presentan más adelante en la sección 4.3.1.3.
- ***Impacto:*** Representa las consecuencias que se asocian a la manifestación de un riesgo. En algunos casos puede suponer pérdidas financieras de menor importancia, pero en otros puede dar lugar a daño a la reputación de la organización, un corte del suministro de larga duración o incluso la pérdida de

vidas humanas. El impacto se mide de forma semicuantitativa mediante escalas de calificación, como las que se indican más adelante en la sección 4.3.1.3.

La valoración del riesgo quedará entonces definida por el producto de los valores asignados a la probabilidad y al impacto según la expresión [4.1].

4.3.1.1 Tipos de valoraciones

Las metodologías de gestión de riesgos sugieren la realización de valoraciones de riesgo: *Pura* y *Residual* [ERM Initiative, 2010]. En ambos casos se califica la **probabilidad** de ocurrencia y el **impacto** de un riesgo. De esta manera se puede estimar la exposición del sistema a las amenazas identificadas previamente.

- **Valoración pura**: se realiza inmediatamente después de la identificación de los riesgos, para hacer una estimación inicial de las exposiciones y determinar prioridades para la gestión de los riesgos.
- **Valoración residual**: se tienen en cuenta las medidas de gestión de riesgos. Se espera que si las medidas son efectivas, la valoración del riesgo residual sea menor que la del riesgo puro. La valoración residual se realiza una vez se hayan definido y aplicado las medidas de mitigación de riesgos.

Dependiendo del procedimiento adoptado en las políticas de la organización para cada uno de los recursos, es posible adoptar la creación de una matriz de riegos para la **valoración pura** y otra para la **valoración residual**. Esta última resultaría de utilidad en caso que se pretendiera valorar a-priori la efectividad de las medidas de control de riesgos.

4.3.1.2 Recursos de la organización para evaluación semicuantitativa

La definición del **conjunto de recursos** que conforman una organización constituye un paso previo a las etapas de identificación y evaluación de riesgos [COSO, 2004; ERM Initiative, 2010]. La definición de estos recursos tiene en cuenta los talentos y los activos fundamentales con que cuentan las empresas, los cuales se conjugan armónicamente para garantizar el adecuado funcionamiento de la organización.

Teniendo en cuenta la información y experiencia proporcionadas por algunas empresas en Colombia, se ha puesto de manifiesto que los recursos de una organización se pueden clasificar en cuatro clases: **materiales, humanos, técnicos** y **económicos** [ICONTEC, 2004; ISA, 2009; ISAGEN, 2009; XM, 2009; Pragma, 2010].

Constituyen una aproximación adecuada como punto de partida en la estructuración de un procedimiento de valoración de riesgos.

- ***Recursos Materiales***: Correspondiente a los bienes tangibles con que cuenta las empresas propietarias y operadoras de la red de infraestructura para poder ofrecer sus servicios. Estos recursos incluyen ***Instalaciones*** (edificios, maquinaria, equipo, oficinas, terrenos, instrumentos, herramientas, líneas de transporte, líneas de distribución, centros de control, centros de despacho, plantas de generación, y demás activos) y ***Materias primas*** (aquellos vectores energéticos cuya transformación permite la producción de energía eléctrica: combustibles primarios -carbón, gas, fueloil, nuclear- recursos hídricos, recursos eólicos y solar, generación distribuida, etc.) [HAMILTON, 1999].
- ***Recursos Técnicos:*** Todas aquellas herramientas e instrumentos auxiliares que permiten coordinar el montaje, operación, gestión y mantenimiento de la red de infraestructura. Los recursos técnicos incluyen los sistemas de información, los planes de diseño, gestión de proyectos, comercialización de servicios, fórmulas, patentes, marcas, recursos administrativos, etc. [PMI, 2004]
- ***Recursos Humanos:*** Estos recursos son indispensables para cualquier grupo social ya que de ellos depende el manejo y funcionamiento de los demás recursos. En ellos se incluyen toda la fuerza laboral de empleados, trabajadores, contratistas y terceros que intervienen en el montaje, operación y mantenimiento de la red de infraestructura eléctrica. El recurso o talento humano realiza funciones específicas y se organiza en niveles jerárquicos. El **talento humano** posee características como sentimientos, ideas, imaginación, creatividad, habilidades, posibilidad de desarrollo, experiencias, conocimientos, etc. [BOMPARD, CIWEI *et al.*, 2009]
- ***Recursos Económicos:*** Son los recursos monetarios propios y ajenos con los que cuenta la empresa, indispensables para su buen funcionamiento y desarrollo. Pueden ser **propios** (dinero en efectivo, aportaciones de los socios, acciones, etc.) o **ajenos** (préstamos de acreedores y proveedores, créditos bancarios o privados, emisiones de bonos).

4.3.1.3 Escalas de valoración de riesgos

La estrategia de evaluación semicuantitativa que aquí se propone se basa en el uso de **matrices de riesgo**s, las cuales se obtienen de acuerdo al producto de la **probabilidad** y el **impacto** asignados a cada riesgo [4.1]. La clasificación ordenada de las amenazas al suministro energético se realizará finalmente a partir de los valores

numéricos obtenidos como valoración de cada uno de los riesgos y de sus componentes.

La Tabla 4.3 y la Tabla 4.4 muestran las escalas propuestas a los juicios de probabilidad e impacto de los riesgos para evaluación semicuantitativa. A cada uno de estos juicios se le asigna un número en una escala de cinco niveles que varía de 1 a 9, como se sugiere en [SAATY, 2008].

Las **escalas de calificación** que se proponen en la Tabla 4.3 (evaluación de probabilidad) y en la Tabla 4.4 (evaluación del impacto) son el resultado de entrevistas con grupos de analistas en empresas del sector eléctrico [ISA, 2009; XM, 2009]. Estas escalas estarán sujetas a cambios según las circunstancias de la infraestructura, la situación del país, las políticas, el conocimiento de las fuentes humanas, las estrategias empresariales de la organización, entre otros criterios.

La calificación de la **probabilidad** del riesgo tiene en cuenta la frecuencia con la que éste se manifiesta en un periodo de tiempo, en una o varias oportunidades [EC, 2011a].

Tabla 4.3: Escala de calificación para la probabilidad de ocurrencia de riesgos

PROBABILIDAD	Remota	Improbable	Moderada	Probable	Casi cierta
ESCALA	1	3	5	7	9
FRECUENCIA	Una vez cada diez o más años	Una vez entre siete y diez años	Una vez entre tres y siete años	Una vez entre uno y tres años	Una o más veces por año

Por su parte, las escalas para valoración del **impacto** son específicas para cada recurso bajo evaluación (sección 4.3.1.2). Estas escalas tienen en cuenta el tipo de sistema, el tamaño de la red de infraestructura crítica, las estrategias organizacionales, el conocimiento de las fuentes humanas, el estado financiero de las empresas propietarias y operadoras, la sensibilidad de la infraestructura a impactos específicos, etc. [EC, 2011a]

Tabla 4.4: Escalas de calificación para la magnitud del impacto en cada recurso de la red de infraestructura eléctrica

IMPACTO	Bajo	Moderado	Intermedio	Alto	Crítico
ESCALA	**1**	**3**	**5**	**7**	**9**
RECURSO ECONÓMICO	Pérdidas menores a 1 M€	Pérdidas entre 1 M€ y 3 M€	Pérdidas entre 3 M€ y 10 M€	Pérdidas entre 10 M€ y 20 M€	Pérdidas mayores a 20 M€
RECURSO TÉCNICO	No se afectan los servicios técnicos, ni los servicios auxiliares, ni la información de las empresas propietarias y operadoras de la red de infraestructura eléctrica	No se afectan los servicios técnicos, ni los servicios auxiliares, ni la información de las empresas propietarias y operadoras de la red de infraestructura eléctrica. Sin embargo, la información involucrada o su calidad se puede recuperar o consolidada	No se afectan los servicios técnicos, ni los servicios auxiliares, ni la información de las empresas propietarias y operadoras de la red de infraestructura eléctrica. Sin embargo, la información involucrada o su calidad no puede ser recuperada o consolidada	Se afectan parte de los servicios técnicos, o de los servicios auxiliares, o de la información confidencial/estratégica de las empresas propietarias y operadoras de la red de infraestructura eléctrica.	Se afectan los servicios técnicos, o los servicios auxiliares, o la información confidencial/estratégica de las empresas propietarias y operadoras de la red de infraestructura eléctrica (sin que pueda ser recuperada)
RECURSO HUMANO	No se causan efectos sobre la integridad física mental o social de la persona	Se afecta temporalmente la integridad física mental o social de la persona, sin necesidad de intervención reparadora	Se afecta temporalmente la integridad física mental o social de la persona. Se requiere intervención reparadora, pero no quedan secuelas, ni consecuencias permanentes	Se afecta permanentemente la integridad física, mental o social de la persona. Se requiere intervención reparadora y quedan secuelas o consecuencias permanentes	Pérdida de la vida
RECURSO MATERIAL	El impacto no afecta de manera significativa y puede ser asumido por el giro normal de las operaciones del sistema energético nacional, ya que no afecta la prestación del servicio, la viabilidad empresarial o la relación con los consumidores de energía.	El impacto afecta de manera significativa pero puede ser asumido por el giro normal de las operaciones del sistema energético nacional, ya que no afecta la prestación del servicio, viabilidad empresarial o la relación con los consumidores de energía.	Se puede ver afectada la eficiencia del sistema energético nacional, lo cual disminuye la calidad del servicio, y esto genera insatisfacción en los consumidores de energía e impactos en las economías locales	El impacto afecta de manera importante y se generan pérdidas económicas y deterioro social importantes	Se afectan los estándares de los indicadores, se genera incumplimiento regulatorio, y se pone en riesgo la normal prestación del servicio en el sistema energético nacional. Se impacta la economía regional y se afecta la relación con los consumidores de energía

El nivel de precisión de un ejercicio de evaluación semicuantitativa de riesgos podrá requerir la valoración en cada uno de los cuatro recursos. Sin embargo, el procedimiento se puede simplificar mediante la limitación a sólo uno de los recursos que conforman la organización. A efectos prácticos, la mayoría de las veces se limita la realización de las matrices de riesgo a la **valoración del recurso económico**. La formulación del mapa interconectado de riesgos, descrito previamente en la sección

3.3.4 (Figura 3.9), ha tenido en cuenta dicha simplificación. Sin embargo, en la medida que se tengan en cuenta los demás recursos de la red de infraestructura, se obtienen resultados más completos dentro del ciclo de mejora continua requerido en el marco de gestión de riesgos.

La expresión [4.1] se utiliza para el cálculo de la evaluación semicuantitativa del riesgo y permite determinar los **rangos de calificación de amenazas**. La información recopilada en el desarrollo de esta tesis, basada tanto en la experiencia de empresas operadoras y propietarias del sistema de transporte eléctrico en Colombia [ISA, 2009; ISAGEN, 2009; XM, 2009] como en recomendaciones de la Comisión Europea [EC, 2011a], permite distinguir cuatro escalas para esta calificación de amenazas: *aceptables*, *tolerables*, *importantes* y *críticos*. La matriz de riesgos que se presenta en la Figura 4.1 contiene un procedimiento de evaluación semicuantitativa.

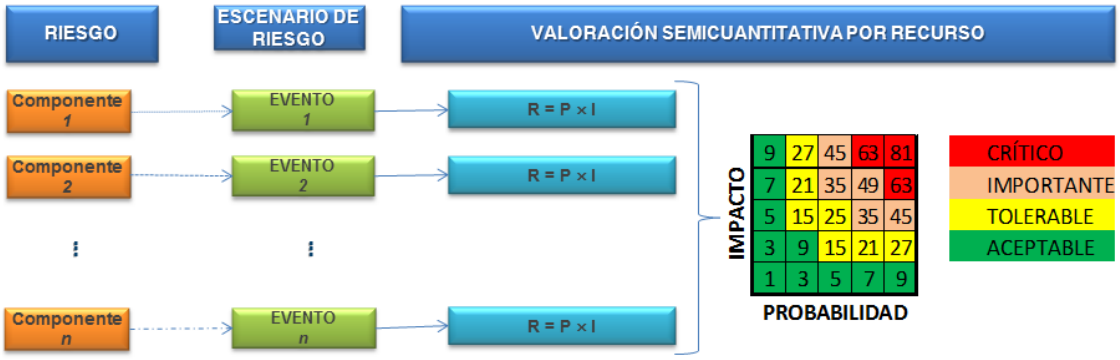


Figura 4.1: Rangos de clasificación de riesgos.

Se entiende que los riesgos clasificados en el grupo de "*críticos*" e "*importantes*" son los que requieren atención urgente, y acciones de control que permitan mitigar su frecuencia de aparición y las consecuencias de su impacto.

- ***Riesgos Críticos***: Bajo ninguna circunstancia se deberá mantener un riesgo con esa capacidad potencial de afectar el logro de los objetivos del proyecto. Estos riesgos requieren una atención de alta prioridad para buscar disminuir en forma inmediata su calificación (Rango de Valoración: 50-81).
- ***Riesgos Importantes***: Se requiere desarrollar acciones prioritarias a corto plazo para su gestión debido al alto impacto que tendrían sobre el logro de los objetivos del proyecto (Rango de Valoración: 28-49).

- ***Riesgos Tolerables***: Aunque deben desarrollarse actividades para la gestión sobre el riesgo, tienen una prioridad de segundo nivel, pudiendo ejecutarse a mediano plazo (Rango de Valoración: 10-27).
- ***Riesgos Aceptables***: El riesgo no tiene una gravedad significativa, por lo que no amerita la inversión de recursos y no requiere acciones adicionales a las ya aplicadas. Se deben conservar las acciones implementadas para mantener el nivel (Rango de Valoración: 1-9).

4.3.2 APLICACIÓN DE LA ESTRATEGIA DE EVALUACIÓN SEMICUANTITATIVA SOBRE UN SISTEMA DE INFRAESTRUCTURA ELÉCTRICA

En el capítulo 3 se aplica la propuesta de metodología de identificación de riesgos en un caso real del sistema eléctrico de un país. En dicho caso de estudio se identifican 142 componentes de riesgo agrupadas en 21 riesgos diferentes, según se estableció en la estrategia de identificación de riesgos. La estrategia de evaluación semicuantitativa definida en este capítulo 4 se aplica directamente sobre las componentes de riesgo identificadas en el capítulo 3.3.4.3 (Tabla 3.3) de acuerdo a las *escalas de calificación* establecidas en la sección 4.3.1.3 (Tabla 4.3, Tabla 4.4), con lo que se obtiene el respectivo *rango de clasificación* de cada componente.

4.3.2.1 Evaluación semicuantitativa de componentes de riesgo

La aplicación de la metodología se ha efectuado en **todos los recursos** del sistema de infraestructura crítica: *económico*, *técnico*, *humano* y *material*. En la Tabla 4.5 se presenta la **evaluación pura** del caso en estudio, es decir, sin tener en cuenta a priori las acciones de mitigación de riesgos.

Por ejemplo, en las cinco primeras líneas de la Tabla 4.5, se observa que el riesgo Nº 1 (*Aumento de las cuentas por cobrar,* Tabla 3.3) está caracterizado por cinco componentes. Para cada uno de los recursos (económico, humano, técnico, material) se ha evaluado la probabilidad y el impacto de cada una de las cuatro componentes de riesgo según las escalas de calificación predefinidas (Tabla 4.3, Tabla 4.4), y finalmente se ha aplicado el rango de valoración de cada componente de riesgo en cada uno de los recursos.

En particular, para el recurso económico en la primera componente de riesgo (*Morosidad de los agentes que usan la red de transporte*, Tabla 3.3) se han asignado unas calificaciones de *probabilidad moderada* (5) e *impacto alto* (7). El resultado del producto de ambas calificaciones arroja un valor de 35, correspondiente a un rango de

valoración "*importante*", según la escala de valoración de riesgos presentada en la sección 4.3.1.3. Idénticamente se ha realizado la valoración de la primera componente de riesgo sobre los recursos técnico, humano y material.

Tabla 4.5: Evaluación semicuantitativa de componentes de riesgo en la red de infraestructura.

RIESGO	N° COMP	RECURSO ECONÓMICO			RECURSO TÉCNICO			RECURSO HUMANO			RECURSO MATERIAL		
		PROB	IMPAC	EVAL. PURA	PROB	IMPACTO	EVAL. PURA	PROB	IMPACTO	EVAL. PURA	PROB	IMPACTO	EVAL. PURA
1	1	5	7	IMPORTANTE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
1	2	5	7	IMPORTANTE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
1	3	5	7	IMPORTANTE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
1	4	3	3	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	3	ACEPTABLE
1	5	3	3	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	3	ACEPTABLE
2	6	5	7	IMPORTANTE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
2	7	3	7	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
2	8	3	7	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
2	9	3	7	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
2	9	3	3	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
2	11	3	3	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
2	12	3	3	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
2	13	3	3	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
2	14	3	3	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
2	15	1	3	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
2	16	3	5	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
2	17	3	5	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
3	18	3	5	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
3	19	3	5	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
3	20	3	5	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
3	21	3	5	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
3	22	3	5	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
3	23	3	3	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
3	24	3	3	ACEPTABLE	3	3	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
3	25	3	3	ACEPTABLE	1	1	ACEPTABLE	3	5	TOLERABLE	1	5	ACEPTABLE
4	26	5	9	IMPORTANTE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
4	27	5	9	IMPORTANTE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
4	28	5	9	IMPORTANTE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
4	29	3	9	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
5	30	3	1	ACEPTABLE	3	3	ACEPTABLE	3	1	ACEPTABLE	3	3	ACEPTABLE
5	31	7	5	IMPORTANTE	5	3	TOLERABLE	5	3	TOLERABLE	7	5	IMPORTANTE
5	32	3	1	ACEPTABLE	3	1	ACEPTABLE	5	7	IMPORTANTE	3	1	ACEPTABLE
5	33	3	1	ACEPTABLE	3	1	ACEPTABLE	5	5	TOLERABLE	5	3	TOLERABLE
5	34	1	1	ACEPTABLE	3	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
5	35	9	1	ACEPTABLE	9	3	TOLERABLE	5	1	ACEPTABLE	9	3	TOLERABLE
5	36	9	1	ACEPTABLE	9	3	TOLERABLE	5	1	ACEPTABLE	9	3	TOLERABLE
5	37	5	7	IMPORTANTE	5	7	IMPORTANTE	5	7	IMPORTANTE	5	7	IMPORTANTE
5	38	7	3	TOLERABLE	9	7	CRÍTICO	5	3	TOLERABLE	9	7	CRÍTICO
6	39	5	7	IMPORTANTE	5	9	IMPORTANTE	5	5	TOLERABLE	5	3	TOLERABLE
6	40	7	3	TOLERABLE	7	9	CRÍTICO	7	5	IMPORTANTE	7	9	CRÍTICO
6	41	7	9	CRÍTICO	7	9	CRÍTICO	7	7	IMPORTANTE	7	9	CRÍTICO
6	42	7	9	CRÍTICO	7	9	CRÍTICO	7	7	IMPORTANTE	7	9	CRÍTICO
6	43	3	3	ACEPTABLE	3	9	TOLERABLE	3	3	ACEPTABLE	3	3	ACEPTABLE
6	44	5	3	TOLERABLE	7	7	IMPORTANTE	5	7	IMPORTANTE	7	7	IMPORTANTE
6	45	1	1	ACEPTABLE	1	5	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
6	46	5	5	TOLERABLE	7	5	IMPORTANTE	9	3	TOLERABLE	9	1	ACEPTABLE
7	47	3	1	ACEPTABLE	3	3	ACEPTABLE	3	3	ACEPTABLE	3	3	ACEPTABLE
7	48	5	3	TOLERABLE	5	7	IMPORTANTE	3	5	TOLERABLE	5	7	IMPORTANTE
7	49	5	5	TOLERABLE	5	5	TOLERABLE	5	9	IMPORTANTE	5	5	TOLERABLE
7	50	9	3	TOLERABLE	9	3	TOLERABLE	5	5	TOLERABLE	5	5	TOLERABLE
7	51	9	3	TOLERABLE	9	3	TOLERABLE	5	5	TOLERABLE	5	5	TOLERABLE
7	52	1	1	ACEPTABLE	5	3	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
7	53	5	3	TOLERABLE	5	3	TOLERABLE	5	5	TOLERABLE	5	3	TOLERABLE
7	54	5	3	TOLERABLE	7	3	TOLERABLE	3	3	ACEPTABLE	5	3	TOLERABLE
7	55	5	5	TOLERABLE	5	5	TOLERABLE	5	7	IMPORTANTE	5	5	TOLERABLE
7	56	3	3	ACEPTABLE	1	5	ACEPTABLE	3	3	ACEPTABLE	3	5	TOLERABLE
8	57	9	7	CRÍTICO	9	7	CRÍTICO	7	9	CRÍTICO	9	3	TOLERABLE
8	58	9	7	CRÍTICO	9	7	CRÍTICO	7	9	CRÍTICO	9	3	TOLERABLE
8	59	9	5	IMPORTANTE	9	5	IMPORTANTE	9	9	CRÍTICO	9	5	IMPORTANTE
8	60	9	5	IMPORTANTE	9	5	IMPORTANTE	7	9	CRÍTICO	9	5	IMPORTANTE
8	61	9	5	IMPORTANTE	9	5	IMPORTANTE	9	9	CRÍTICO	9	5	IMPORTANTE
8	62	9	5	IMPORTANTE	9	5	IMPORTANTE	7	9	CRÍTICO	9	5	IMPORTANTE
8	63	9	5	IMPORTANTE	3	3	ACEPTABLE	7	9	CRÍTICO	3	3	ACEPTABLE
8	65	9	5	IMPORTANTE	9	5	IMPORTANTE	7	9	CRÍTICO	9	5	IMPORTANTE
8	66	9	5	IMPORTANTE	5	3	TOLERABLE	1	1	ACEPTABLE	9	5	IMPORTANTE
8	67	9	5	IMPORTANTE	9	5	IMPORTANTE	9	9	CRÍTICO	9	5	IMPORTANTE
8	68	5	3	TOLERABLE	5	3	TOLERABLE	5	5	TOLERABLE	5	3	TOLERABLE
8	69	9	3	TOLERABLE	9	5	IMPORTANTE	3	9	TOLERABLE	9	5	IMPORTANTE

RIESGO	N° COMP	RECURSO ECONÓMICO			RECURSO TÉCNICO			RECURSO HUMANO			RECURSO MATERIAL		
		PROB	IMPAC	EVAL. PURA	PROB	IMPACTO	EVAL. PURA	PROB	IMPACTO	EVAL. PURA	PROB	IMPACTO	EVAL. PURA
8	70	5	7	IMPORTANTE	5	9	IMPORTANTE	5	9	IMPORTANTE	5	5	TOLERABLE
9	71	7	9	CRÍTICO	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
9	72	7	9	CRÍTICO	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
9	73	7	9	CRÍTICO	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
10	74	5	9	IMPORTANTE	5	9	IMPORTANTE	1	1	ACEPTABLE	5	9	IMPORTANTE
10	75	5	9	IMPORTANTE	9	5	IMPORTANTE	1	1	ACEPTABLE	9	3	TOLERABLE
10	76	7	5	IMPORTANTE	5	5	TOLERABLE	7	5	IMPORTANTE	7	5	IMPORTANTE
10	77	5	9	IMPORTANTE	5	9	IMPORTANTE	5	1	ACEPTABLE	5	9	IMPORTANTE
10	78	3	5	TOLERABLE	3	5	TOLERABLE	3	5	TOLERABLE	3	5	TOLERABLE
11	79	9	1	ACEPTABLE	9	3	TOLERABLE	9	9	CRÍTICO	9	1	ACEPTABLE
11	80	3	3	ACEPTABLE	3	5	TOLERABLE	1	1	ACEPTABLE	5	7	IMPORTANTE
11	81	5	5	TOLERABLE	7	7	IMPORTANTE	1	1	ACEPTABLE	7	7	IMPORTANTE
11	82	3	3	ACEPTABLE	3	5	TOLERABLE	1	1	ACEPTABLE	7	7	IMPORTANTE
11	83	3	3	ACEPTABLE	3	5	TOLERABLE	1	1	ACEPTABLE	3	5	TOLERABLE
11	84	3	3	ACEPTABLE	7	7	IMPORTANTE	1	9	ACEPTABLE	7	7	IMPORTANTE
11	85	5	1	ACEPTABLE	7	7	IMPORTANTE	1	1	ACEPTABLE	7	7	IMPORTANTE
11	86	5	9	IMPORTANTE	3	9	TOLERABLE	5	9	IMPORTANTE	5	7	IMPORTANTE
12	87	3	7	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
12	88	3	7	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
12	89	3	7	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
13	90	9	5	IMPORTANTE	9	7	CRÍTICO	5	9	IMPORTANTE	9	5	IMPORTANTE
13	91	9	1	ACEPTABLE	9	3	TOLERABLE	9	9	CRÍTICO	9	1	ACEPTABLE
13	92	9	7	CRÍTICO	5	9	IMPORTANTE	1	1	ACEPTABLE	5	9	IMPORTANTE
13	93	3	5	TOLERABLE	3	3	ACEPTABLE	3	9	TOLERABLE	3	3	ACEPTABLE
13	94	5	7	IMPORTANTE	9	5	IMPORTANTE	5	7	IMPORTANTE	7	5	IMPORTANTE
13	95	9	9	CRÍTICO	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
14	96	5	3	TOLERABLE	5	5	TOLERABLE	3	3	ACEPTABLE	5	5	TOLERABLE
14	97	3	1	ACEPTABLE	3	3	ACEPTABLE	3	1	ACEPTABLE	3	3	ACEPTABLE
14	98	5	3	TOLERABLE	7	3	TOLERABLE	3	5	TOLERABLE	5	5	TOLERABLE
14	99	5	3	TOLERABLE	7	7	IMPORTANTE	5	7	IMPORTANTE	7	7	IMPORTANTE
14	100	5	7	IMPORTANTE	5	9	IMPORTANTE	5	7	IMPORTANTE	5	9	IMPORTANTE
14	101	3	3	ACEPTABLE	3	3	ACEPTABLE	3	3	ACEPTABLE	3	3	ACEPTABLE
14	102	3	3	ACEPTABLE	3	3	ACEPTABLE	3	3	ACEPTABLE	3	3	ACEPTABLE
15	103	5	5	TOLERABLE	7	7	IMPORTANTE	5	1	ACEPTABLE	7	7	IMPORTANTE
15	104	9	1	ACEPTABLE	9	3	TOLERABLE	9	9	CRÍTICO	9	1	ACEPTABLE
15	105	5	3	TOLERABLE	7	7	IMPORTANTE	7	1	ACEPTABLE	7	7	IMPORTANTE
15	106	1	1	ACEPTABLE	1	1	ACEPTABLE	1	4	ACEPTABLE	1	1	ACEPTABLE
15	107	5	9	IMPORTANTE	7	9	CRÍTICO	3	3	ACEPTABLE	7	9	CRÍTICO
15	108	3	3	ACEPTABLE	7	5	IMPORTANTE	1	1	ACEPTABLE	7	7	IMPORTANTE
15	109	1	1	ACEPTABLE	3	7	TOLERABLE	5	9	IMPORTANTE	5	5	TOLERABLE
16	110	5	7	IMPORTANTE	5	7	IMPORTANTE	1	5	ACEPTABLE	3	5	TOLERABLE
16	111	9	5	IMPORTANTE	9	9	CRÍTICO	1	1	ACEPTABLE	9	9	CRÍTICO
16	112	9	9	CRÍTICO	9	5	IMPORTANTE	1	1	ACEPTABLE	9	9	CRÍTICO
16	113	3	1	ACEPTABLE	7	7	IMPORTANTE	3	3	ACEPTABLE	5	7	IMPORTANTE
16	114	3	1	ACEPTABLE	7	7	IMPORTANTE	3	3	ACEPTABLE	5	7	IMPORTANTE
16	115	3	7	TOLERABLE	5	5	TOLERABLE	1	1	ACEPTABLE	5	5	TOLERABLE
16	116	3	3	ACEPTABLE	5	7	IMPORTANTE	5	7	IMPORTANTE	5	7	IMPORTANTE
17	117	5	9	IMPORTANTE	5	9	IMPORTANTE	5	1	ACEPTABLE	5	9	IMPORTANTE
17	118	5	9	IMPORTANTE	5	9	IMPORTANTE	5	1	ACEPTABLE	5	9	IMPORTANTE
17	119	5	9	IMPORTANTE	5	9	IMPORTANTE	5	1	ACEPTABLE	5	9	IMPORTANTE
17	120	5	1	ACEPTABLE	7	7	IMPORTANTE	3	1	ACEPTABLE	7	7	IMPORTANTE
17	121	5	1	ACEPTABLE	7	7	IMPORTANTE	3	1	ACEPTABLE	7	7	IMPORTANTE
18	122	1	9	ACEPTABLE	1	9	ACEPTABLE	1	9	ACEPTABLE	9	9	CRÍTICO
18	123	7	5	IMPORTANTE	3	7	TOLERABLE	1	1	ACEPTABLE	5	5	TOLERABLE
18	124	5	5	TOLERABLE	1	9	ACEPTABLE	1	1	ACEPTABLE	9	9	CRÍTICO
18	125	5	5	TOLERABLE	5	7	IMPORTANTE	1	1	ACEPTABLE	9	9	CRÍTICO
18	126	5	5	TOLERABLE	5	7	IMPORTANTE	1	1	ACEPTABLE	9	9	CRÍTICO
19	127	3	9	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
19	128	3	9	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
19	129	3	9	TOLERABLE	1	1	ACEPTABLE	1	1	ACEPTABLE	1	1	ACEPTABLE
20	130	7	9	CRÍTICO	5	5	TOLERABLE	5	9	IMPORTANTE	5	5	TOLERABLE
20	131	5	7	IMPORTANTE	5	9	IMPORTANTE	3	5	TOLERABLE	3	9	TOLERABLE
20	132	7	9	CRÍTICO	7	7	IMPORTANTE	7	9	CRÍTICO	7	7	IMPORTANTE
21	133	5	5	TOLERABLE	5	9	IMPORTANTE	1	1	ACEPTABLE	5	9	IMPORTANTE
21	134	5	5	TOLERABLE	5	9	IMPORTANTE	1	1	ACEPTABLE	5	9	IMPORTANTE
21	135	5	5	TOLERABLE	5	9	IMPORTANTE	1	1	ACEPTABLE	5	9	IMPORTANTE
21	136	5	5	TOLERABLE	1	9	ACEPTABLE	1	9	ACEPTABLE	1	3	ACEPTABLE
21	137	7	9	CRÍTICO	3	3	ACEPTABLE	1	1	ACEPTABLE	3	3	ACEPTABLE
21	138	7	9	CRÍTICO	3	3	ACEPTABLE	1	1	ACEPTABLE	3	3	ACEPTABLE
21	139	7	9	CRÍTICO	7	9	CRÍTICO	1	1	ACEPTABLE	7	9	CRÍTICO
21	140	7	9	CRÍTICO	5	7	IMPORTANTE	1	1	ACEPTABLE	5	7	IMPORTANTE
21	141	7	9	CRÍTICO	5	7	IMPORTANTE	1	1	ACEPTABLE	5	7	IMPORTANTE
21	142	7	9	CRÍTICO	5	7	IMPORTANTE	1	1	ACEPTABLE	5	7	IMPORTANTE

La evaluación semicuantitativa de la Tabla 4.5 se ha aplicado a cada una de las componentes de riesgo según el recurso bajo evaluación. Con la información

obtenida es posible generar una matriz de riesgo para cada recurso y una matriz de riesgo para todo el sistema, según se explica en las siguientes subsecciones.

4.3.2.2 Matriz de riesgo por recurso

La valoración semicuantitativa de las componentes de riesgo permite obtener la valoración de cada riesgo, calculado como el promedio de sus componentes. Es decir, para cada uno de los cuatro recursos (*económico, humano, técnico, material*), un riesgo (*i*) conformado por una cantidad de componentes (*n*) tendrá la siguiente valoración:

$$(Riesgo)_i = \left(\frac{1}{n}\sum_{n\in i}(Probabilidad \times Impacto)_n\right)_i \qquad [4.2]$$

Para cada recurso se construye entonces una matriz de riesgo. En estas matrices se ubican los riesgos de acuerdo con la probabilidad e impacto asignados a cada uno. Los ejes en las matrices representan las variables de análisis de valoración. En el eje horizontal se ubica la probabilidad y en el eje vertical, el impacto. Las unidades de cada eje corresponden a los niveles de las escalas definidas en la Tabla 4.3 y en la Tabla 4.4. De esta manera se obtiene la matriz de riesgo por recurso que incluyen las valoraciones de los riesgos que les afectan.

Por ejemplo, en las cinco primeras líneas de la Tabla 4.5, se observa que el riesgo Nº 1 (*Aumento de las cuentas por cobrar*, Tabla 3.3) está caracterizado por cinco componentes, cuya evaluación semicuantitativa origina los resultados que se presentan en la Tabla 4.6. Los riesgos asociados a los recursos materiales, humanos y técnicos han obtenido una puntuación de 1.8, 1 y 1 respectivamente, con lo que quedan clasificados como *riesgos aceptables*, tomando los rangos de valoración definidos en la sección 4.3.1.3. Sin embargo, el riesgo vinculado al recurso económico arroja una puntuación de 24.6, por lo que se clasifica como *riesgo tolerable.* De manera análoga se realiza la misma operación con los demás riesgos identificados previamente en el mapa de riesgos del capítulo 3 (Figura 3.9, Tabla 3.3) y su respectiva evaluación de la Tabla 4.5.

Tabla 4.6: Evaluación semicuantitativa de componentes del riesgo N° 1

COMPONENTES DEL RIESGO	RIESGO MATERIAL	RIESGO HUMANO	RIESGO TÉCNICO	RIESGO ECONÓMICO
Morosidad, dudoso recaudo o no recuperación de cartera de parte de los agentes que usan la Red de Transporte	1	1	1	35
Morosidad, dudoso recaudo o no recuperación de cartera por servicios de conexión al Sistema de Infraestructura Eléctrica (Transporte)	1	1	1	35
Morosidad, dudoso recaudo o no recuperación de cartera por servicios asociados y no operacionales	1	1	1	35
Riesgo de Crédito: Falta de cumplimiento por parte de terceros de las obligaciones establecidas	3	1	1	9
Altos precios en tarifas reguladas (transporte, distribución) o en comercialización	3	1	1	9
Promedio componentes riesgo N°1	**1.8**	**1**	**1**	**24.6**
(Aumento de las cuentas por cobrar)	**ACEPTABLE**	**ACEPTABLE**	**ACEPTABLE**	**TOLERABLE**

En la Figura 4.2 se muestra el rango de clasificación de cada uno de los riesgos que se identificaron en el capítulo 3, según la evaluación realizada en cada recurso y que están relacionados en el mapa de riesgos de la Figura 3.9. Cada una de las matrices se divide en cuatro zonas para la clasificación de los riesgos (aceptables, tolerables, importantes y críticos), según la ubicación de su valoración de probabilidad y severidad. Por ejemplo, para el caso del riesgo N° 1 (*Aumento de las cuentas por cobrar*) se puede apreciar que su ubicación en la matriz de cada recurso se puede localizar en las celdas de color *verde* para los recursos material, humano, técnico (riesgo aceptable) y *amarillo* (riesgo tolerable) en el caso del recurso económico.

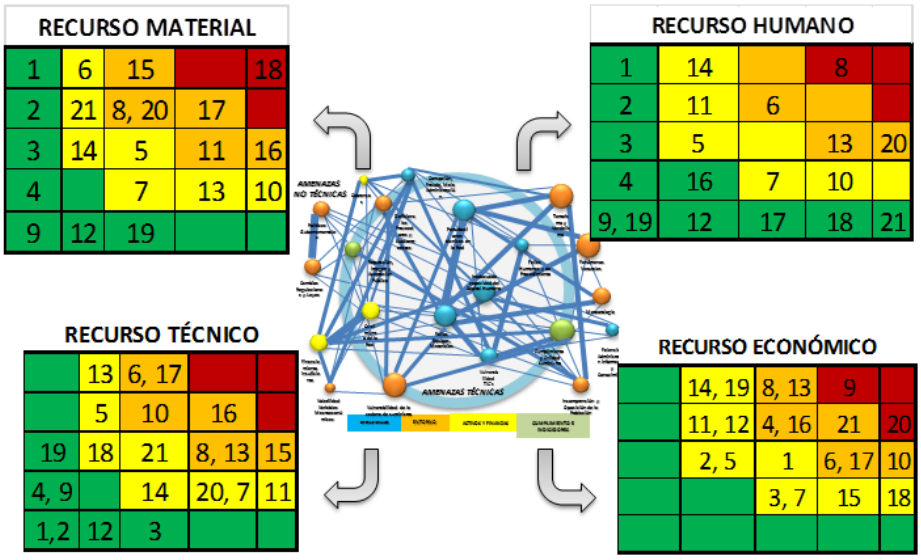


Figura 4.2: Evaluación semicuantitativa de riesgos por cada recurso.

En la Figura 4.2 se puede observar un primer diagnóstico donde claramente se indica qué riesgos y en qué tipo de recurso se demanda la priorización de acciones y de medidas en el corto plazo. Se distingue en la matriz de riesgos las celdas de color naranja (riesgos importantes) y rojo (riesgos críticos) correspondientes a los riesgos que requieren priorización de acciones de control.

En particular se destaca el riesgo N° 8 (terrorismo y vandalismo) que evaluado como *importante* en los recursos material, técnico, económico y *crítico* en el recurso humano.

El riesgo N° 16 (perturbaciones técnicas en la red) clasifica en el rango de *importante* en los recursos material, técnico, económico, pero es *aceptable* en el recurso humano.

El riesgo N° 6 (fenómenos naturales adversos) clasifica en el rango de *importante* en los recursos humano, técnico, económico, pero es *tolerable* en el recurso material.

El riesgo N° 20 (deficiencias proveedores y subcontratistas) se representa en el rango de *crítico* en el recurso económico, *importante* en recursos humano, material y *tolerable* en el recurso técnico.

Sin embargo, se destacan otros riesgos que están clasificados como *aceptables* y *tolerables* en todos los recursos, por ejemplo, los riesgos N° 1 (Aumento de las cuentas por cobrar), N° 2 (financiación insuficiente), N° 3 (cambios en regulaciones y leyes), N° 7 (incomprensión y oposición de la población), N° 19 (baja reputación imagen y aceptación pública), entre otros.

4.3.2.3 Matriz de riesgo para todo el sistema

La valoración semicuantitativa de cada riesgo se calcula como el promedio de la valoración en cada recurso. Es decir, con la información previa de cada uno de los cuatro recursos (*económico, humano, técnico, material*), un riesgo (*i*) obtendrá la siguiente valoración:

$$(Riesgo)_i = \left(\frac{1}{4}\sum_{Recurso}(Riesgo)_i\right)_{Recurso} \qquad [4.3]$$

Al tener en cuenta los cuatro recursos de la red de infraestructura, la valoración de cada de riesgo corresponde a la ponderación de todas las calificaciones asignadas de probabilidad e impacto en cada recurso, a cada uno de los riesgos. Los

resultados numéricos de la valoración final ponderada de cada riesgo pueden visualizarse gráficamente en la Figura 4.3

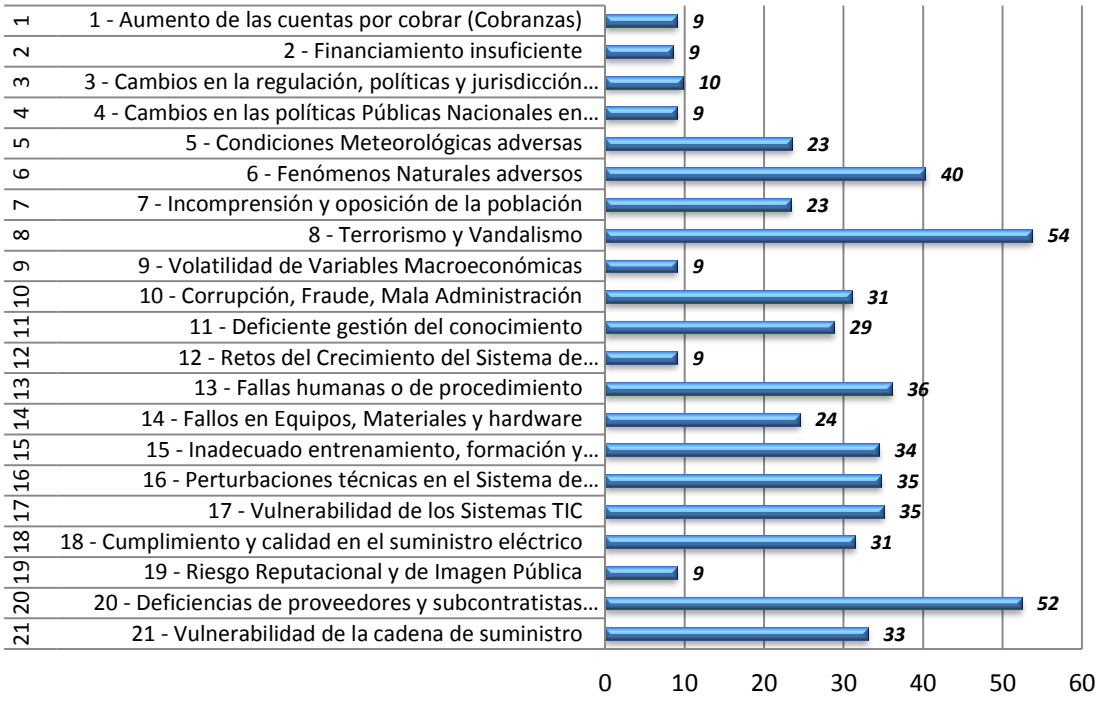


Figura 4.3: Resultados de la evaluación semicuantitativa de riesgos.

El análisis de los resultados obtenidos mediante esta técnica se realizará a partir de la calificación en riesgos críticos, importantes, tolerables y aceptables. En esta valoración semicuantitativa de la Figura 4.3, el riesgo N° 8 "*Terrorismo y Vandalismo*" ha obtenido una valoración final "*riesgo crítico*". La misma valoración la obtiene el riesgo N° 20 "*Deficiencias de Proveedores y Subcontratistas*

A partir de estos resultados, se puede concluir que dos riesgos deben ser considerados como *críticos*, es decir, requieren atención prioritaria y urgente, y ocho riesgos resultan ser *importantes* y necesitan implementación de programas en el corto plazo.

Riesgos Críticos: Terrorismo y Vandalismo (valoración = 54); Deficiencias de Proveedores y Subcontratistas (valoración = 52).

Riesgos Importantes: Fenómenos naturales adversos; Perturbaciones técnicas; Vulnerabilidad de los sistemas TIC; Corrupción & fraude; Deficiente gestión del conocimiento; Fallos humanos o de procedimiento; Inadecuado entrenamiento y capacitación del talento humano; Indicadores de cumplimiento y calidad del suministro energético; Vulnerabilidad de la cadena de suministro.

Los demás riesgos (diez en total), reciben una calificación de *tolerables* o *aceptables* y por tanto no requieren un tratamiento prioritario.

Una información complementaria a esta sección, que contiene medidas y salvaguardias para contener los riesgos identificados, se puede consultar en el Anexo B. Estas medidas se sugieren a partir del conocimiento de fuentes humanas, así como literatura especializada en protección de infraestructura [SCHNEIDER, 2005; LEWIS, 2006; NESS, 2006; SULLIVANT & NEAVE, 2007; MACAULAY, 2008; RADVANOVSKY & Mc-DOUGALL, 2010].

4.3.2.4 Generación de la carta de riesgos

Con el objetivo de ofrecer una mejor visualización que facilite la comprensión de la evaluación de riesgos y su clasificación, es necesario introducir una representación que fusione las matrices de riesgos y su respectiva calificación semicuantitativa. Por tal razón, se aplica una primera propuesta para representar la evaluación semicuantitativa de riesgos mediante **cartas de riesgos**. Una aproximación inicial de esta representación se muestra en [CCN Criptología, 2010], pero en esta tesis se propone emplear un esquema que ofrezca una visión integral y resumida acerca de la situación del conjunto de riesgos.

La Figura 4.4 proporciona una visualización integral de los rangos de clasificación de cada uno de los riesgos evaluados. Se distingue el matiz de colores que varía desde verde (riesgos aceptables) hasta rojo (riesgos críticos).

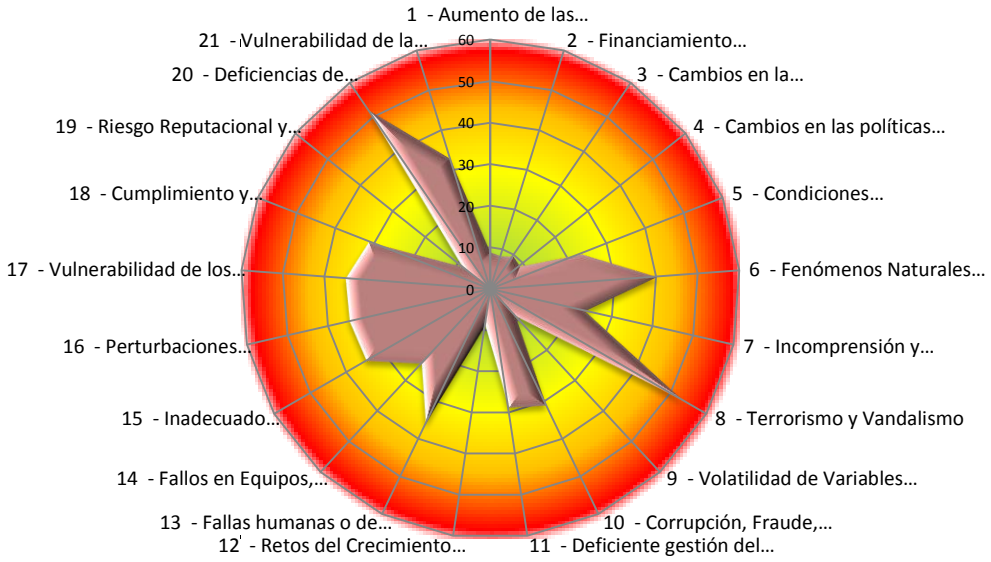


Figura 4.4: Carta de riesgos para el sistema de infraestructura eléctrica

Obsérvese que en la Figura 4.4 es fácil deducir que el **riesgo más crítico** corresponde al riesgo N° 8, *Terrorismo y Vandalismo*. Conceptualmente, esto quiere decir que, en este caso de estudio, las redes eléctricas se han convertido en objetivos de ataques que comprometen la seguridad del suministro energético, con importantes efectos en la seguridad nacional, la economía y la vida de los ciudadanos.

También se clasifica como **crítico** el riesgo Nº 20, *deficiencias de proveedores y subcontratistas*, quienes se encargan de proporcionar puntualmente los materiales y repuestos para garantizar la operación permanente de la red eléctrica. Igualmente, se incluyen los riesgos que recaen sobre los subcontratistas que con su trabajo deben responder por los cronogramas de mantenimiento y el correcto desempeño de los nuevos proyectos relacionados con el crecimiento, expansión, operación y mantenimiento de la red.

Entre los **riesgos importantes** se evidencia que el riesgo N° 6, *fenómenos naturales adversos*, requiere la preparación de medidas de emergencia y reposición del servicio ante posible destrucción de la infraestructura como consecuencia de inundaciones, terremotos, avalanchas.

Atención especial debe considerarse para el riesgo N° 13, *Errores humanos o de procedimiento*, que actualmente representa una de las mayores preocupaciones en las organizaciones propietarias y operadoras de los sistemas de infraestructura eléctrica. Dicho riesgo se relaciona con el N° 15, *Inadecuado entrenamiento, formación y capacitación del talento humano*, según se observa en el mapa de riesgos de la Figura 3.9. Ambas amenazas se explican dado que los sistemas son operados por personas, quienes pueden ocasionar errores no intencionados.

También recibe particular atención recibe el riesgo N° 21, *Vulnerabilidad de la cadena de suministro*, el cual básicamente se refiere al suministro energético para las plantas de generación (i.e. gas natural, combustible, carbón, así como operaciones industriales en plantas nucleares). Lo anterior, coincide con los esfuerzos mancomunados entre entidades oficiales y el sector privado para garantizar el suministro energético como una de las políticas de seguridad nacional más importantes.

El riesgo N° 17, *Vulnerabilidad de las tecnologías TIC*, incluye todas aquellas tecnologías de supervisión y control (SCADA), control de operación, transporte y distribución, PLC’s, etc, dado que están interconectadas a través de redes que también pueden accederse remotamente y pueden significar alguna vulnerabilidad ante ataques y virus informáticos.

Dada la cantidad de recursos organizacionales involucrados en la planificación, ejecución y mantenimiento de todos los activos y componentes de la red de infraestructura, aquellos riesgos técnicos, como las *perturbaciones técnicas de la red* (riesgo N° 16) o los *fallos en equipos, materiales y hardware* (riesgo N° 14) se califican como importantes, pues pueden desencadenar en cortes inesperados del servicio. Precisamente el riesgo N° 18, *no-cumplir los indicadores de calidad del servicio eléctrico*, tiene tanta trascendencia en una región o país que incluso tiene consecuencias políticas y sociales.

La *corrupción y mala administración* (Riesgo N° 10) se plantea como un riesgo importante, especialmente por el impacto económico y financiero que genera al interior de las organizaciones propietarias y operadoras de las infraestructuras eléctricas. Lo anterior, debido a la desviación de recursos necesarios para las infraestructuras, con el respectivo impacto en su funcionamiento.

Los **riesgos tolerables** y **aceptables** habitualmente tienen menos trascendencia. Por ejemplo, aquellos relacionados con *políticas públicas nacionales y regulaciones* (riesgos N° 3, 4), *retos en el crecimiento de la infraestructura* (riesgo N° 12), la *reputación* (riesgo N° 19). La *oposición de la población* (riesgo N° 11) puede generar dificultades en la ejecución de proyectos en la infraestructura. Sin embargo, un adecuado sistema de gestión de riesgos permitirá controlar y manejar dichas amenazas.

4.3.2.5 Generación de la carta para las componentes de riesgo

La detección de vulnerabilidades tanto en las organizaciones como en el sistema físico se lleva a cabo mediante una revisión más detallada a través de las componentes de riesgo, cuya calificación semicuantitativa se ha presentado en la Tabla 4.5. La Figura 4.5 muestra el resultado de la evaluación pura de dichas componentes. Aquellas componentes clasificadas como *críticas* e *importantes* se ubican en los matices de colores naranja y rojo, en tanto que las componentes riesgo con rango *aceptable y tolerable* se pueden distinguir en los matices de colores verde y amarillo.

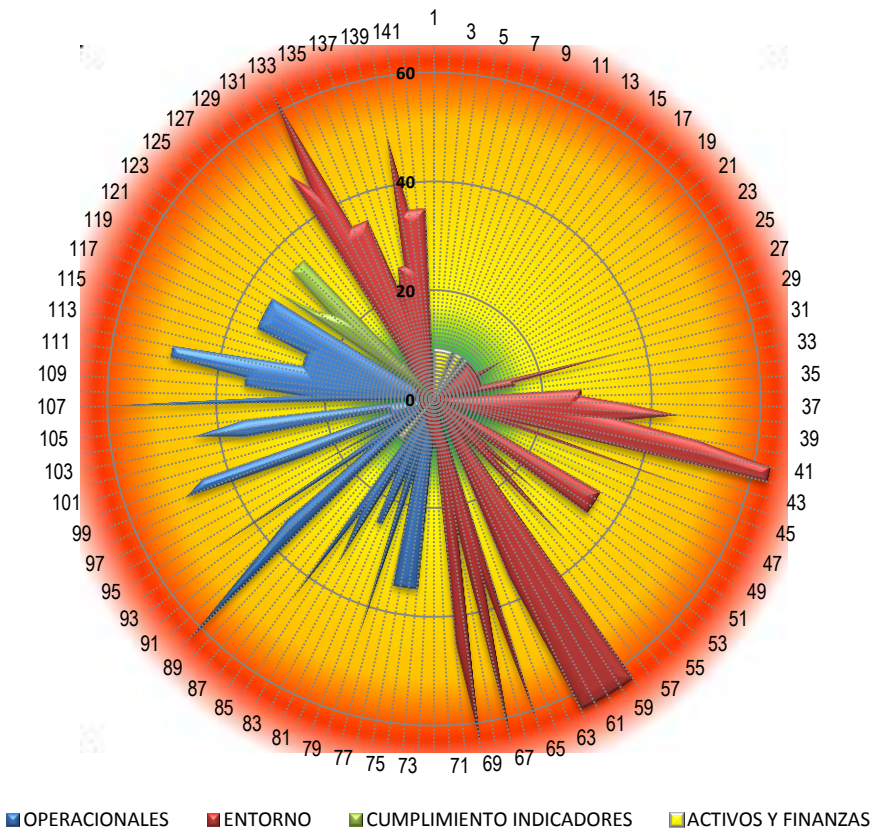


Figura 4.5: Carta de las componentes de riesgo, en el sistema de infraestructura.

También es posible observar la respectiva categorización de cada componente. Precisamente los **riesgos de entorno** y los **riesgos operacionales** (calificados como *críticos* e *importantes*) son los que tienen mayores efectos en el funcionamiento de toda la red de infraestructura, en tanto que los **riesgos de activos y finanzas** tienen menores efectos en el funcionamiento del sistema (calificados como *aceptables*). En general, se cuentan 13 componentes calificadas como *críticas*, 49 componentes son *importantes*, 30 componentes son *tolerables* y las otras 50 son componentes de riesgo *aceptable*.

La carta permite un estudio más profundo de la naturaleza de cada componente. Es interesante anotar que esta valoración se ha realizado teniendo en cuenta la experiencia de organizaciones que han soportado ataques a su infraestructura, como en el caso de Colombia. Precisamente las componentes relacionadas con *terrorismo y vandalismo* (componentes N° 58, 59, 60, 61, 62, 64, 68) concentran las valoraciones más críticas. Los fenómenos naturales también demuestran repercusiones importantes, dada la destrucción y no disponibilidad de activos importantes (componentes N° 40, 41, 42).

Los riesgos **operacionales** se asocian a los procedimientos (por ejemplo, los servicios de ajuste del operador del sistema eléctrico), mantenimiento, y administración de activos en la red eléctrica. Previsiblemente éstos se consideran componentes de riesgo *importantes* (componentes N° 94, 100, 111, 112).

Merece la pena destacar el impacto de aquellos riesgos administrativos, tales como la corrupción y la interferencia de terceros en el ejercicio organizacional (componentes N° 78, 86, 129). Esta clase de riesgos tienen una percepción alta para el sector estratégico, especialmente por los efectos que estos riesgos pueden representar en la realización de proyectos, por la vulnerabilidad en el ejercicio financiero o por la inadecuada operación y mantenimiento de la infraestructura.

Como conclusión, la metodología de identificación y evaluación de riesgos aquí presentada permite no sólo la incorporación de información en mapas de riesgos, sino también la estimación de medidas de valoración de los riesgos y sus componentes mediante *cartas de riesgos*.

El ejercicio de valoración de riesgos permite detectar vulnerabilidades tanto en organizaciones como en sistemas. Además facilita la deducción de acciones para mitigar el riesgo. Por esta razón, esta propuesta puede ser también adoptada en otras situaciones diferentes de las infraestructuras críticas.

4.3.3 CASO ESPECÍFICO PARA LA INFRAESTRUCTURA DE TRANSPORTE DE ENERGÍA ELÉCTRICA

Un riesgo puede afectar una organización, un sistema o un activo. De acuerdo al nivel de abstracción organizacional (desde un nivel estratégico y global, hasta un nivel operativo y de detalle), el mapa de riesgos puede variar para adaptarse a cada caso.

En el marco de gestión de riesgos, la propuesta metodológica de identificación con mapas de riesgos y su posterior evaluación con matrices y **cartas de riesgos**, tiene aplicabilidad integral en el caso de organizaciones integradas verticalmente, es decir, que la misma empresa integra negocios de generación, transporte, distribución y comercialización de energía. Si no hay integración vertical, es preferible identificar los riesgos por separado, según afecten cada aspecto de la cadena de valor.

En particular, para el caso específico de identificación y evaluación de riesgos en infraestructuras de transporte eléctrico, se puede reducir el número de componentes de riesgo a aquellas que afecten exclusivamente a esta actividad de

transporte en alta tensión. Así, se han podido reducir las componentes de riesgo de 142 a 116. En la Figura 4.6 se indica el número de componentes de riesgo asociadas a los 21 riesgos identificados para el sistema de infraestructura.

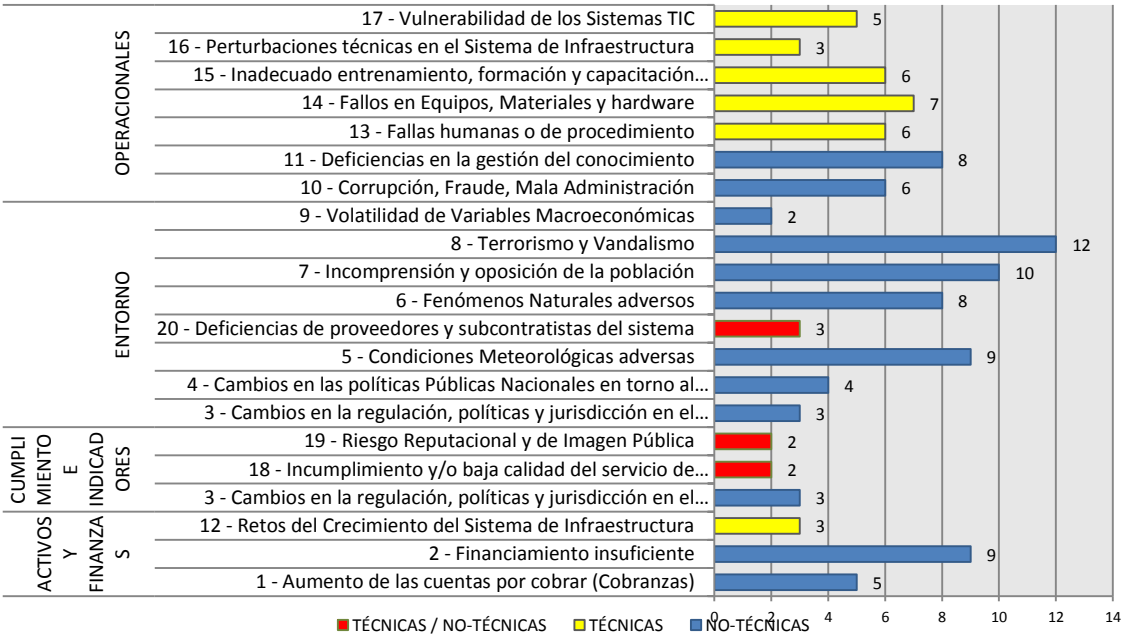


Figura 4.6: Riesgos que afectan el subsistema de transporte en alta y media tensión.

La evaluación de los riesgos identificados en la cadena de valor del subsistema de transporte en alta y media tensión se puede resumir en la *carta de riesgos* de la Figura 4.7.

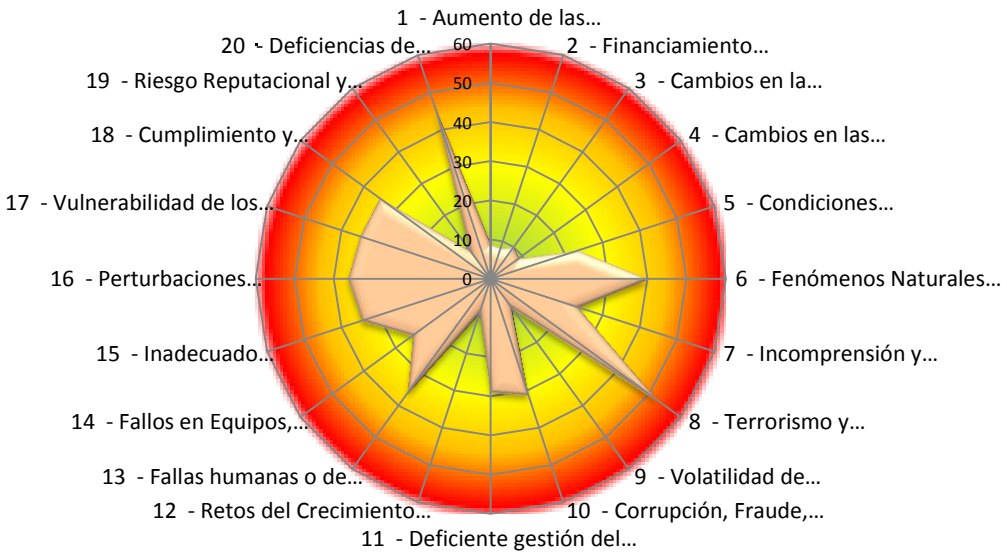


Figura 4.7: Carta de riesgos en el subsistema de transporte en alta y media tensión.

En este caso, la amenaza asociada a "*terrorismo y vandalismo*" es la que tiene mayor calificación y es considerada como el **riesgo más crítico**. Sin embargo, también reciben una calificación de **riesgos importantes**, aquellos relacionados con *perturbaciones técnicas*, *fenómenos naturales, fallos humanos, fallos de los equipos que conforman los activos* y *vulnerabilidad de los sistemas TIC* asociados a la red de transporte de energía eléctrica.

En los capítulos posteriores de esta tesis se pretende desarrollar una estrategia metodológica que permita profundizar en el diagnóstico de los riesgos previamente identificados en el subsistema de transporte de alta tensión y en el estudio de la vulnerabilidad de diferentes topologías de la red ante contingencias.

4.3.4 CICLO DE MEJORA CONTINUA EN EL MARCO DE GESTIÓN DE RIESGOS

Dentro de la filosofía de los planes de *protección de infraestructura crítica* (PIC), como se puede observar en la Figura 4.8, las últimas etapas se refieren a la aplicación de medidas con el fin de disminuir la probabilidad de que se materialicen los riesgos o el impacto de sus consecuencias, teniendo en cuenta los recursos fundamentales de las organizaciones propietarias y operadoras del sistema. Lo anterior, haciendo especial énfasis en aquellos riesgos que han quedado evaluados como "**Críticos**" e "**Importantes**" en las matrices de valoración.

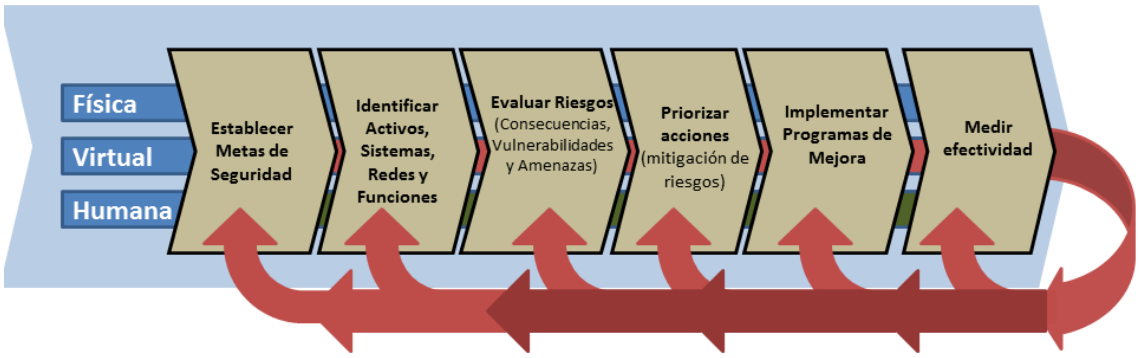


Figura 4.8: Ciclo de mejora continua en PIC

En el caso específico de la protección al sistema de infraestructura, las decisiones respecto a los riesgos incluyen aceptarlos, eliminarlos o gestionarlos (Figura 4.9).

- Aceptar los riesgos implica no definir medidas para mitigarlos.

- Eliminar podría incluir dejar de ejecutar la actividad que genera el riesgo, modificar por completo procedimientos o asignación de recursos, entre otros.
- Gestionar los riesgos se refiere a definir e implementar medidas para administrarlos; éstas pueden ser de prevención, las cuales disminuyen la probabilidad de que se materialicen los riesgos o, de protección, que disminuyen la afectación sobre los recursos fundamentales de la empresa. Entre las medidas de protección se incluyen las de transferencia y retención de riesgos.

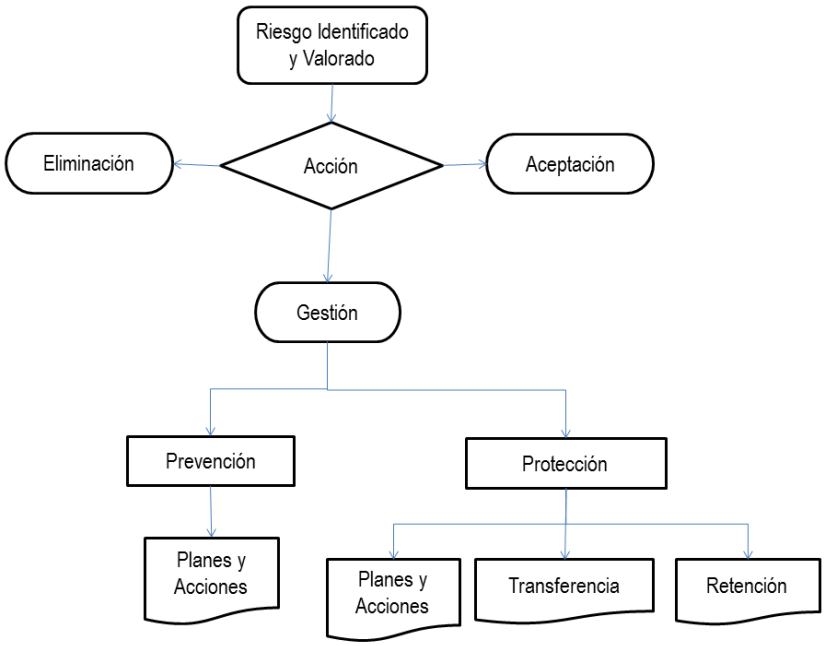


Figura 4.9: Esquema para la etapa de priorización de acciones.

En las siguientes secciones se proponen algunas consideraciones respecto a las etapas que completan el marco de gestión de riesgos, según el ciclo de mejora continua de los planes de protección de infraestructura crítica (Figura 4.8).

4.3.4.1 Priorización de acciones y medidas de salvaguardia

Según el NIPP esta etapa consiste en la aplicación de medidas con el fin de disminuir la probabilidad de que se materialicen los riesgos o el impacto de sus consecuencias frente a los recursos fundamentales en el sistema de infraestructura crítica. Un sistema está constantemente sometido a la manifestación de riesgos en cada uno de los subsistemas que le componen. Este punto requiere una comparación de los niveles relativos de riesgo de los sectores y recursos disponibles, junto con las opciones para lograr los objetivos de seguridad establecidos. De esta manera, las

medidas de protección se aplican donde sea posible reducir el riesgo, resultando en una mejor relación coste-beneficio.

Como complemento a la aplicación de la metodología de evaluación presentada en este capítulo, se ha construido una base de conocimiento que contiene acciones de salvaguardia para el control de cada uno de los riesgos identificados, que se puede consultar en el ANEXO B. El conjunto de medidas y acciones se ha obtenido a partir del conocimiento de fuentes humanas y de literatura especializada en protección de infraestructura [KNIGHT, 2001; SCHNEIDER, 2005; LEWIS, 2006; NESS, 2006; SULLIVANT & NEAVE, 2007; MACAULAY, 2008; RADVANOVSKY & Mc-DOUGALL, 2010]. Se proponen un conjunto de acciones útiles para el sistema de infraestructura eléctrica, que permiten mitigar la probabilidad de los riesgos y el impacto de los mismos.

4.3.4.2 Medición de la Efectividad

En esta etapa del NIPP se realizan las actividades de comprobación, supervisión, observación crítica y registro del progreso de las labores y acciones, en forma integral y periódica, para identificar cambios y retroalimentar oportunidades de mejora dentro de la gestión de riesgos en el sistema de infraestructura energética.

Para medir la efectividad de las medidas de gestión de riesgos en el sistema de infraestructura se puede efectuar un proceso de autoevaluación, realizar una evaluación con personal ajeno al proceso o buscar un análisis independiente que garantice una evaluación crítica respecto a la efectividad de la gestión de los riesgos. Adicionalmente, es útil definir indicadores a través de los cuales se obtenga información relevante sobre el comportamiento de los riesgos.

En esta etapa se identifican recursos humanos encargados tanto de realizar la autoevaluación periódica, como de garantizar que las medidas se apliquen y que sigan siendo efectivas. Para hacer esta autoevaluación, los responsables de la aplicación de las medidas pueden hacer uso de una serie de herramientas de gestión, incluyendo información importante respecto a la ocurrencia de eventos y la gestión de riesgos; entre ellas se encuentran [ERM Initiative, 2010]:

- Iniciativas de plan de desarrollo.
- Indicadores de cuadros de gestión integral.
- Indicadores de gestión de los procesos.

- Indicadores del sistema integrado de gestión (salud ocupacional, gestión ambiental, seguridad de la información, calidad).
- Planes de mejora resultado de auditorías internas.
- Planes de acción resultado de las auditorías del sistema integrado de gestión.
- Planes de trabajo de los equipos.

4.4 COMENTARIOS AL CAPÍTULO

Las actividades de evaluación de riesgos del capítulo 4 dan continuidad a la identificación de riesgos del capítulo 3. En este capítulo se ha profundizado en el diseño y aplicación de una metodología de evaluación semicuantitativa de riesgos, que se fundamenta en las prácticas y en las recomendaciones de las diferentes normas, legislaciones y estándares internacionales de gestión de riesgos.

Se ha propuesto una estrategia de evaluación semicuantitativa sobre cada uno de los recursos organizacionales (técnicos, financieros, humanos y materiales), para asignar una calificación más precisa a cada riesgo, en términos de la probabilidad y el impacto de sus consecuencias. Dicha información se representa gráficamente con la ayuda de *cartas de riesgo*.

Se ha realizado una aplicación de la propuesta metodológica en un caso práctico en el sistema eléctrico colombiano. Dentro del caso de estudio también se ha efectuado una evaluación de riesgos específicos en el subsistema de transporte eléctrico en alta tensión, resultando una valoración *crítica* de las amenazas de “terrorismo y vandalismo” y de aquellos riesgos relacionados con el “desempeño de proveedores y subcontratistas”. También han resultado valorados como riesgos *importantes* la afectación en las redes debidas a fenómenos naturales, fallos humanos, fallos de los equipos y vulnerabilidad de las TIC. Dichos riesgos serán estudiados, desde un punto de vista más técnico con aplicación a las redes eléctricas de transporte, en el capítulo 5.

5 ANÁLISIS ESTRUCTURAL DE VULNERABILIDAD EN REDES ELÉCTRICAS DE ALTA Y MEDIA TENSIÓN

La evaluación de riesgos propuesta en el capítulo 4 ha puesto de manifiesto la percepción de vulnerabilidad de la infraestructura eléctrica, a consecuencia de aquellas amenazas calificadas como *críticas* e *importantes*, entre las que se cuentan actos de terrorismo y vandalismo, fenómenos naturales adversos, condiciones climatológicas adversas y fallos en equipos e instalaciones, que en algunos casos son atribuidos a errores humanos.

En este capítulo se propone una estrategia metodológica que permite evaluar específicamente la vulnerabilidad estructural en redes eléctricas de transporte en alta y media tensión, y su respuesta ante riesgos críticos e importantes. Lo anterior involucra el estudio de los eventos que desencadenan fallos en cascada y desconexión de consumidores. La metodología propuesta puede tener gran utilidad como mecanismo para la explicación de episodios como los apagones o *blackouts*.

5.1 OBJETIVO DEL CAPÍTULO

Según lo estudiado en los capítulos 3 y 4, ha sido posible clasificar los riesgos más críticos e importantes que afectan al sistema de transporte y distribución de energía eléctrica. El impulso a la investigación que permita explicar el impacto de esos riesgos dentro del sistema de infraestructura ha trascendido a la opinión pública. Son recordados algunos episodios relacionados con interrupciones súbitas del servicio de energía eléctrica, cubriendo amplias zonas geográficas, como los **incidentes de apagones o *blackout*** ocurridos en Estados Unidos y Canadá (Agosto de 2003), Alemania, Bélgica, Holanda, Italia, Francia y España (Noviembre de 2006), Brasil (Noviembre de 2009). Así mismo, algunos **actos coyunturales de terrorismo** como los experimentados en Colombia entre los años 1998 y 2003, que impactaron el servicio eléctrico, por el ataque deliberado sobre algunos activos de las infraestructuras de transporte.

En el marco de la gestión de riesgos, que ha inspirado la elaboración de los capítulos anteriores de esta tesis, se han generado resultados que permiten comprender los riesgos más críticos e importantes en el sistema eléctrico a nivel local y nacional. De esta manera, se han definido los pasos fundamentales para identificar y evaluar riesgos de manera cualitativa. Adicionalmente, se ha propuesto la priorización de acciones que permitan responder ante amenazas de desastres naturales, eventos inesperados de interrupción de la operación y ataques deliberados contra la red de infraestructura.

Sin embargo, un análisis más técnico desde el punto de vista de la ingeniería hace necesario trascender la valoración semicuantitativa y generar el marco de evaluación efectiva de la vulnerabilidad de las redes de transporte en alta y media tensión, que debe involucrar el estudio de las relaciones con otros sistemas, su interdependencia y su respuesta ante los riesgos y cambios en las condiciones de operación. Por tanto, este capítulo pretende cumplir con los siguientes objetivos:

- Generar una metodología de modelización de la red de infraestructura crítica basada en teoría de redes complejas (teoría de grafos), que permita evaluar la vulnerabilidad del sistema, determinar la criticidad de cada componente, evaluar los efectos por el ataque en sus nodos y enlaces, y valorar la evolución de los posibles fallos en cascada.
- Presentar el conjunto de indicadores que permiten analizar la vulnerabilidad estructural en redes de transporte de alta y media tensión, y validar su efectividad

en el estudio de las diferentes contingencias a las que se somete estas redes de infraestructuras.

- Comparar la efectividad de las respuestas de los flujos en redes complejas de libre escala frente a técnicas tradicionales de ingeniería eléctrica. Esta comparación permite validar, de manera parcial o total, el uso de metodologías más sencillas que proporcionan resultados equivalentes, a la vez que permiten entender la naturaleza compleja de las redes de infraestructura crítica en el sector eléctrico.

En este capítulo se hace referencia al concepto de ***resiliencia***, término que se refiere a la operación de un sistema de manera estable después de sufrir una perturbación o contingencia en uno o varios de sus elementos. Un sistema ***robusto*** implica que éste mantiene intacta su estructura y sus funciones después de un evento perturbador [HOLMGREN, 2006]. Una red robusta y resiliente equivale a una red de baja ***vulnerabilidad***.

5.2 APLICACIÓN DE LA TEORÍA DE GRAFOS EN SISTEMAS ELÉCTRICOS

En la revisión bibliográfica que se ha presentado a lo largo de este documento de tesis (secciones 2.3.1, 3.2 y 4.2) se ha puesto de manifiesto el interés de valorar el impacto de la pérdida de uno o más componentes de un sistema de infraestructura.

El caso del sistema energético se puede simular como un sistema único (e.g sistema de potencia) o interdependiente (e.g gas natural y generación eléctrica). Como se ha presentado anteriormente en la tesis, los modelos de dinámica de sistemas permiten evaluar el comportamiento físico de los sistemas bajos condiciones de alteración o de eliminación de ciertos nodos, así como la capacidad de ajustarse a las exigencias de demanda de un sistema (e.g. capacidades de almacenamiento, capacidades de transporte, capacidad de distribución, información del sistema). Los sistemas multi-agente permiten simular los efectos de un determinado elemento sobre todo el sistema (e.g. un acuerdo contractual), así como la identificación del impacto como resultado de los cambios en las políticas que lo rigen (e.g. estados de operación, localización, etc). Por su parte, aquellos modelos basados en teoría de grafos permiten simular los sistemas físicos interconectados (e.g. redes de energía eléctrica).

Un modelo de simulación más realista permitirá tener una representación más cercana del sistema en estudio y permitirá representar acertadamente al sistema bajo condiciones extremas. Sin embargo, mayor realismo también implica mayor complejidad en la elaboración de estos modelos [BROWN, 2007].

Alternativamente, un modelo más abstracto, aunque más sencillo, permitirá sentar las bases para construir modelos de mayor nivel de detalle. En ese sentido, los modelos construidos sobre teoría de grafos proporcionan una nueva visión para pensar en los sistemas de infraestructura crítica.

Los campos de aplicación de la **teoría de grafos**, también conocida como **teoría de redes complejas** [NEWMAN, 2003], se caracterizan por la facilidad que proporciona la representación abstracta de un sistema como una red de topología con medidas estadísticas, así como la evaluación de los efectos de esa topología en la robustez del sistema ante diferentes tipos de ataques y fallos.

Hay una gran cantidad de infraestructuras críticas que se pueden representar mediante una red de nodos interconectados a través de enlaces. De esta manera, la aplicación de técnicas matemáticas de optimización puede aplicarse a estas redes para entender su comportamiento bajo situaciones normales o bajo situaciones de fallos. Entre otras áreas, las redes complejas son muy útiles en la evaluación de contingencias en los sistemas de transporte y en la evaluación de las medidas que permitan reducir dichos impactos [BROWN, 2007]. Otras aplicaciones de las redes complejas con énfasis en los sistemas de transporte de alta tensión pueden ser consultados en [JELENIUS, 2004; HOLMGREN, 2007a; JOHANSSON, 2010].

Se ha realizado una revisión bibliográfica sobre la aplicación de la teoría de grafos al análisis de contingencias en redes de infraestructura en los últimos años. La Tabla 5.1 contiene un compendio de las aplicaciones más significativas en el estudio de vulnerabilidad de sistemas eléctricos, a través de redes complejas.

Tabla 5.1: Aplicaciones de la teoría de grafos para el estudio de vulnerabilidad de infraestructura crítica

PUBLICACIÓN	APLICACIÓN
[BARABÁSI & ALBERT, 1999]	Primera definición de las redes de libre escala, a las que se asemejan los sistemas de infraestructura.
[ALBERT & BARABÁSI, 2002]	Primera aplicación de los conceptos de vulnerabilidad y resiliencia en redes de libre escala, con aplicaciones a redes eléctricas y redes informáticas.
[MOTTER & LAI, 2002]	Definiciones de fallos en cascada, mediante el *grado de conexión* en redes de libre escala.
[NEWMAN, 2003]	Tratado sobre redes complejas, donde se determinan sus definiciones y medidas estadísticas, para aplicación en otras áreas.
[JELENIUS, 2004]	Representación de redes eléctricas con redes complejas y análisis de su vulnerabilidad, mediante medidas del grado de conexión
[HOLMGREN, 2006]	Aplicación de indicadores de teoría de grafos (*clustering*, *grado conexión*, *distancia geodésica*, *distribución nodal*) para evaluar la resiliencia y vulnerabilidad de un sistema de potencia, así como posibles fallos en cascada

PUBLICACIÓN	APLICACIÓN
[HOLMGREN, JENELIUS *et al.*, 2007]	Modelo híbrido entre teoría de grafos y teoría de juegos para definir estrategias de protección de redes de transporte
[HOLMGREN, 2007a]	Estudio de los sistemas de potencia, como redes de libre escala, cuyos indicadores permiten predecir sus posibles fallos en cascada y estrategias de protección.
[MURRAY, MATISZIW *et al.*, 2007]	Modelo de libre escala aplicada al flujo en redes de información en territorio de EEUU, su resiliencia y robustez frente a aislamientos puntuales, para identificar los nodos más críticos.
[SOLÉ, CASALS *et al.*, 2008]	Representación topológica del sistema europeo de alta tensión. Indicadores de vulnerabilidad de la red mediante estadísticas de *clusters*, en cada país de la UE.
[ROSAS i CASALS, 2009]	Evaluación de la red de la fiabilidad en la red de infraestructura europea, mediante indicadores topológicos.
[BUITRAGO & TAUTA, 2008]	Representación topológica del sistema interconectado de alta tensión en Colombia. Análisis de vulnerabilidad mediante grados nodales.
[CHEN, DONG *et al.*, 2009]	Evaluación de la vulnerabilidad de redes eléctricas mediante indicadores de *eficiencias geodésicas* y aproximaciones topológicas para diagnosticar fallos en cascada.
[JOHANSSON, 2010]	Aproximación topológica de redes eléctricas y evaluación de su vulnerabilidad mediante indicadores del grafo (*clustering*, *distancia geodésica, eficiencia*), resiliencia y robustez según medidas de *betweenness*.
[CHEN, DONG *et al.*, 2010]	Aproximación topológica para redes de corriente directa y evaluación de su funcionamiento mediante indicadores de *eficiencias geodésicas.*
[WANG, ZHANG *et al.*, 2011]	Evaluación de vulnerabilidad en red eléctrica, mediante indicadores de *betweenness*.
[CHEN, ZHAO *et al.*, 2011]	Modelo híbrido dinámico entre teoría de grafos y teoría de juegos para sugerir estrategias de protección de redes de transporte

En resumen, la teoría de grafos o las redes complejas constituyen un área de conocimiento reciente para estudiar el análisis de las interdependencias en los sistemas de infraestructura crítica, específicamente las redes eléctricas de transporte y distribución de alta y media tensión. La teoría de grafos facilita el análisis y la visualización de los comportamientos físicos de las redes. Por ejemplo, la evaluación de fallos en cascada mediante el estudio de la topología del sistema, la evaluación de los impactos debidos a la eliminación de componentes específicos en un sistema y sus consecuencias en la congestión de los flujos de potencia, entre otras.

5.2.1 CONCEPTOS BÁSICOS DE TEORÍA DE GRAFOS

Los **grafos** son representaciones de sistemas en las que algunas unidades establecen relaciones pareadas entre sí. Algunas de sus aplicaciones se centran en las siguientes áreas: sociales, de información, tecnológicas y biológicas [NEWMAN, 2003].

En el desarrollo de aplicaciones prácticas de la teoría de grafos se ha definido el concepto de *redes de libre escala*, que permite asimilar los sistemas de infraestructuras a una red compleja [BARABÁSI & ALBERT, 1999]. Esto ha proporcionado una nueva perspectiva en el estudio de las condiciones dinámicas en los sistemas de potencia. Adicionalmente, los conceptos de resiliencia, robustez y vulnerabilidad también han sido aplicados en otros ámbitos diferentes a las redes eléctricas (por ejemplo, redes informáticas y redes sociales) [ALBERT & BARABÁSI, 2002]. En resumen, la teoría de grafos constituye una aproximación muy interesante para entender la dinámica de los eventos que generalmente tienen efectos de fallos en cascada. De esta manera se plantea el uso de la teoría de grafos para cuantificar las consecuencias de los riesgos clasificados como *críticos* e *importantes* en el capítulo 4.3.3, sobre el sistema de transporte en alta y media tensión.

5.2.1.1 Definición de grafo

Una red puede modelarse matemáticamente como un conjunto de **enlaces** (aristas), que conectan a conjunto de **nodos** (vértices). Dichos enlaces pueden ser **dirigidos** (cuando se direccionan de un nodo a otro) o **no-dirigidos** (cuando existen flujos en ambas direcciones), como se presentan en la Figura 5.1. A través de los enlaces pasan algunas cantidades de **flujos** que serán distribuidos entre los nodos.

La forma de los enlaces no es relevante, sólo importa a qué nodos están unidos. La posición de los nodos tampoco importa, y se puede variar para obtener un dibujo más claro.

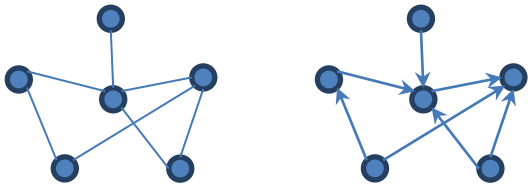


Figura 5.1: Ejemplo de un grafo no-dirigido (izquierda) y dirigido (derecha).

Una representación intuitiva de un sistema eléctrico de potencia permitirá identificar los generadores, subestaciones, consumidores, transformadores y torres de energía como *nodos*, en tanto que las líneas y cables de transporte y distribución se representan como *enlaces*. Resulta útil disponer de una visualización del grafo, como ocurre con el mapa de riesgos de la Figura 3.9. Sin embargo, cuando se manejan grandes conjuntos de puntos, los cálculos deben realizarse de forma computacional, en cuyo caso la visualización del grafo es poco útil.

Desde el punto de vista matemático, un grafo corresponde a la pareja de conjuntos ***G*** = (***N***, ***E***), donde ***N*** es el conjunto de nodos y ***E*** es el conjunto de enlaces. Los enlaces corresponden a un conjunto de pares de la forma (*i*, *j*) tal que *i*, *j* ∈ ***E***. Para simplificar, el enlace (*i*, *j*) se denota como *ij*.

Los grafos se pueden clasificar de acuerdo a la manera cómo se construyan o de acuerdo a la distribución de sus conexiones topológicas. Se distinguen las **redes aleatorias** [NEWMAN, 2003], las **redes de libre escala** (con mayor similitud a las redes del mundo real) [BARABÁSI & ALBERT, 1999] y las **redes de mundo pequeño** referidas a la existencia de una distancia o ruta corta que permite la conexión entre pares de nodos (como ocurre con los fractales, las redes sociales, los mapas digitalizados, etc) [WATTS & STROGATZ, 1998].

5.2.1.2 Matriz de Adyacencias

Corresponde a una matriz cuadrada que representa las relaciones entre los nodos y sus enlaces. Existe una matriz de adyacencia única para cada grafo (sin considerar las permutaciones de filas o columnas), y viceversa [JELENIUS, 2004].

Por cada enlace que une a dos nodos, se denota ***G***(*i*,*j*) = 1 al valor de la ubicación correspondiente del par de nodos, y ***G***(*i*,*j*) = 0 en los demás casos. De esa manera, se obtiene una matriz que representa el número de enlaces (relaciones) entre cada par de nodos (vértices).

5.2.1.3 Grados Nodales

El **grado nodal o valencia (*k*$_i$)**, corresponde a la cantidad de enlaces incidentes (***E***$_i$) en un nodo (***N***$_i$), es decir:

$$k_i = |N_i|, \quad \text{donde} \quad N_i = \{j \in \boldsymbol{N} \mid \{i; j\} \in \boldsymbol{E}\} \qquad [5.1]$$

Un grafo en el que todos los nodos tienen el mismo grado nodal, se conoce como **grafo regular**.

Esta propiedad permite caracterizar la robustez de un grafo, y a partir de ella se identifican algunas medidas que caracterizan a cada grafo en particular. Por ejemplo, el **grado medio de conexión ($\bar{k}$)**, equivale a [BARABÁSI & ALBERT, 1999]:

$$\bar{k} = {}^{2 \cdot E}/_{N} \qquad [5.2]$$

Donde ***N*** es el número total de nodos y ***E*** es la cantidad total de enlaces del grafo.

5.2.1.4 Redes Aleatorias

Los **grafos aleatorios** son redes en las que se definen las conexiones de un nodo (*N*) como un número aleatorio. El modelo **Erdös–Rényi** es el más aceptado en la generación de redes aleatorias [NEWMAN, 2003]; en él se especifica la probabilidad que un nodo tenga un enlace, así como el grado medio de conexión de cada nodo del grafo. De esta manera, se determina la probabilidad (***p***) que estén conectados un par de nodos elegidos aleatoriamente en el grafo, utilizando el grado de conexión de cada nodo **($\bar{k}$)**, según la siguiente relación [ALBERT & BARABÁSI, 2002]:

$$p = \bar{k}/(N-1) \qquad [5.3]$$

La construcción de un grafo aleatorio se establece a partir de un conjunto de ***N*** nodos inicialmente aislados, a los que se les van añadiendo sucesivamente enlaces entre pares de nodos aleatoriamente. Si se define un valor pequeño de $\bar{k}$ respecto a ***N***, muchos de los nodos quedarán desconectados, y algunos otros nodos estarán formando pequeñas islas.

La Figura 5.2 permite apreciar la generación de un **grafo aleatorio de Erdös-Rényi**, con grado medio de conexión $\bar{k}$ = 2.5 y *N* = 50 nodos. La probabilidad que un par de nodos elegidos al azar estén enlazados entre sí, es *p* = 0.051.

Hoy en día, este tipo de grafos se emplea como una base teórica en la generación de otras redes. Desde su concepción, por parte de los matemáticos húngaros *Paul Erdös* y *Alfréd Rényi*, en la década de 1960, se pensaba que las redes con esta característica eran las más adecuadas para describir ciertas redes complejas, y sólo hasta finales de la década de 1990 se evidenció que no era del todo cierto [JELENIUS, 2004].

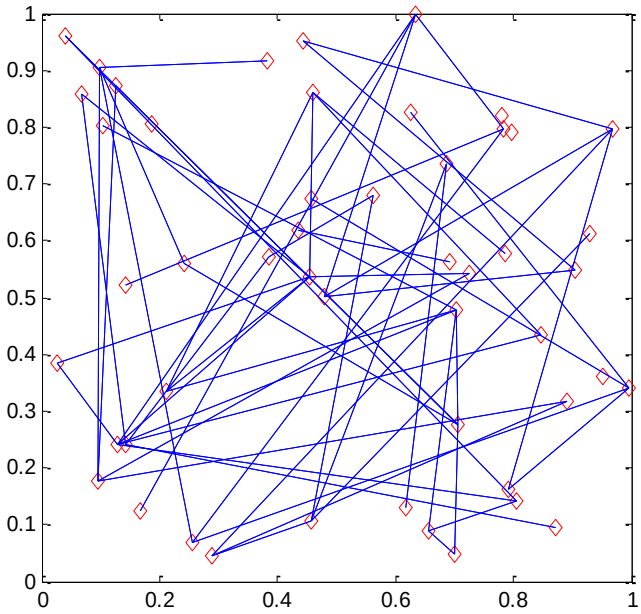


Figura 5.2: Ejemplo de grafo aleatorio, modelo Erdös-Rényi ($N = 50$, $\bar{k} = 2.5$).

Como información, las *redes de mundo pequeño* se generan de la misma manera que las redes aleatorias, pero con valores pequeños de probabilidad, donde se evidencia la efectiva agrupación de sus nodos, y la existencia de rutas entre ellos [WATTS & STROGATZ, 1998; NEWMAN, 2003]. Ese modelo se ha aplicado al estudio de redes sociales, redes biológicas, redes de transferencia de información, etc [ALBERT & BARABÁSI, 2002].

5.2.1.5 Redes de Libre Escala

En una **red libre de escala**, algunos nodos están altamente conectados, es decir, poseen un gran número de enlaces a otros nodos, aunque el grado de conexión de casi todo el grafo es bastante bajo [BARABÁSI & ALBERT, 1999].

Este tipo de redes son las que más similitudes tienen respecto al mundo real. Algunos ejemplos que representan las redes de libre escala son: conexiones en internet, comercio internacional, citaciones bibliográficas, infraestructuras de transporte y distribución de energía eléctrica, infraestructuras de transporte terrestre, redes de interacción de proteínas, etc. En todos los casos, existen nodos de mayor conectividad, a los cuales se adhieren los demás nodos [NEWMAN, 2003].

En las redes de libre escala, un porcentaje bajo de los nodos coleccionan la mayoría de las conexiones. A manera de ejemplo, en la Figura 5.3 se aprecia la representación topológica de una red eléctrica de distribución en media tensión, conformada por 24 buses, a los cuales se adhieren nodos de cargas, líneas de transporte, transformadores y generadores. Algunos de sus nodos poseen una

característica que los hace distinguibles, dado que concentran un mayor número de enlaces.

Este tipo de redes se asemejan más a la realidad, dado que preferencialmente la red crecerá sobre la base de los nodos de mayor conectividad. Dicho resultado es consecuencia de las observaciones experimentales que dieron origen a este tipo de modelos [BARABÁSI & ALBERT, 1999].

La construcción de un grafo de libre escala comienza a partir de un número pequeño de nodos $\boldsymbol{m_0}$ conectados aleatoriamente, y el grado de cada nodo en la red inicial debe ser al menos $k_i \geq 1$. Cada periodo de tiempo se agrega un nuevo nodo con $\boldsymbol{m}$ enlaces, que enlazan el nuevo nodo con la misma cantidad de $\boldsymbol{m}$ nodos en la red, bajo la condición que $\boldsymbol{m} \leq \boldsymbol{m_0}$.

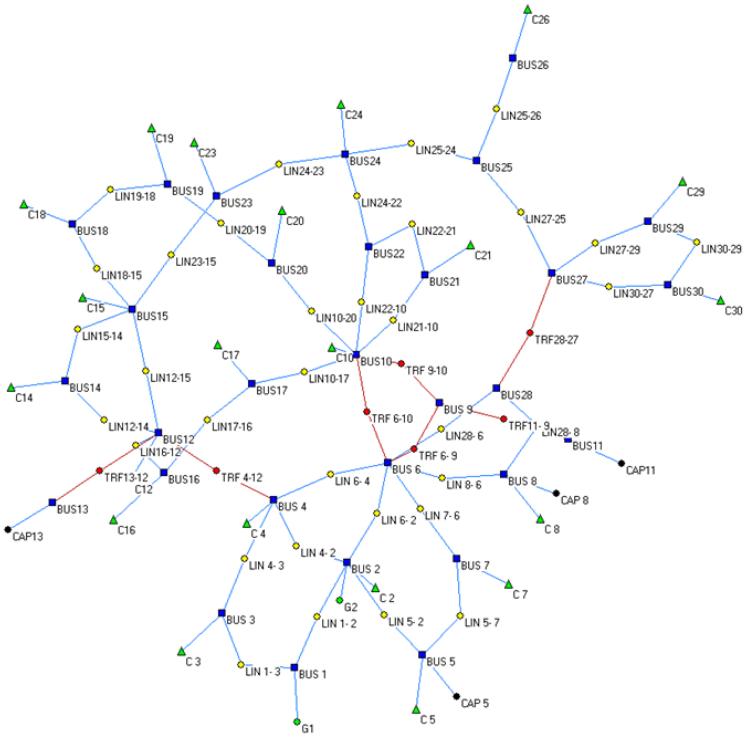


Figura 5.3: Topología red de distribución media tensión, que semeja un grafo de libre escala.

La probabilidad ($\boldsymbol{P_i}$) que un nuevo nodo ($\boldsymbol{j}$) se conecte al nodo ($\boldsymbol{i}$) ya existente, depende de su grado nodal (k_i) [ALBERT & BARABÁSI, 2002]:

$$P_i = {k_i}/{\sum_j k_j} \qquad [5.4]$$

Para visualizar el concepto descrito, a partir del grafo presentado anteriormente en la Figura 5.2 se puede construir un grafo de libre escala, como el que se observa en la Figura 5.4, con la misma distribución de nodos ($\boldsymbol{N}$ = 50 nodos), pero con condición inicial $\boldsymbol{m_0}$ = 44 enlaces, al que se le agregan $\boldsymbol{m}$ = 10 enlaces.

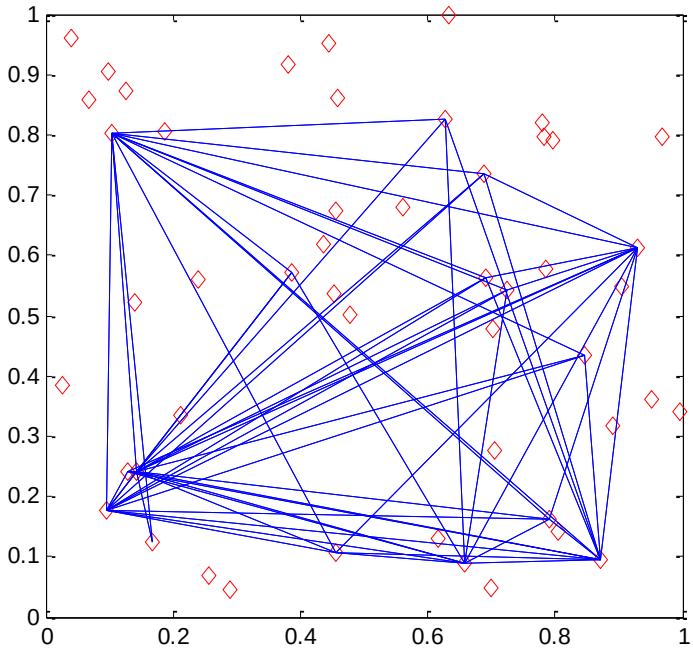


Figura 5.4: Ejemplo de grafo libre escala (*N* = 50, *m* = 10, m_0 = 44, $\bar{k}$ = 2.5).

Los nuevos nodos se enlazan preferiblemente con los nodos más conectados. Los nodos con gran cantidad de conexiones (buses) tienden a acumular rápidamente más enlaces, mientras que los que poseen pocos enlaces rara vez son el origen de nuevas conexiones.

Una ventaja de las redes de libre escala es que cuando falla un nodo, es muy probable que sea uno de los nodos menos conectados. En términos estadísticos aquellos nodos con menos conectividad son los que tienen más probabilidad de ser los que fallen en caso de sucesos aleatorios. Esto permite al sistema mantenerse a sí mismo muy fácilmente, ya que seguirá estando siempre bien conectado.

5.2.1.6 Distribución de Grado Nodal

Una de las propiedades más importantes del análisis de la estructura de las redes es quizás la **distribución de grado, *P*(*k*)**, que indica la probabilidad que un nodo elegido al azar tenga exactamente ***k*** conexiones (o vecinos).

Es decir, si la red posee una cantidad de ***N*** nodos en total y ***nk*** de ellos repartidos en cada grado ***k***, se tiene:

$$P(k_i) = {nk_i}/{N} \qquad [5.5]$$

La misma información se presenta en forma de una **distribución acumulada de grado**, que indica la fracción de nodos con un grado mayor o igual que un determinado grado k_0, según se expresa en [5.6].

$$P(k_i \geq k_0) = \sum_{i=1}^{k_0} P(k_i) \quad , \quad i \in [1,\ k_{máx}] \qquad [5.6]$$

En la ecuación [5.6] se calcula la probabilidad acumulada mediante la suma consecutiva de cada una de las distribuciones de grado nodal [5.5]. Conceptualmente significa la probabilidad de que un nodo elegido al azar tenga más de k_0 enlaces.

Es posible clasificar las redes en función de su distribución de grado nodal. Las más conocidas son:

- **Topología Aleatoria, modelo Erdös-Rényi**: Se ha demostrado que este tipo de grafos de distribución aleatoria tienen una distribución del grado nodal según la función de Poisson [NEWMAN, 2003], es decir:

$$P(k) = \frac{e^{\lambda} \cdot \lambda^{k}}{k!}, \quad \text{donde} \quad \lambda = \bar{k} \qquad [5.7]$$

En la Figura 5.5 se puede observar la comparación de la distribución de grado nodal en un grafo aleatorio, con N = 10000 nodos y diferentes probabilidades de conexión entre sus vértices (P = 0.0006, 0.0010 y 0.0015). Obsérvese que el cálculo del número de nodos con grado nodal ***k***, tiene una distribución de Poisson.

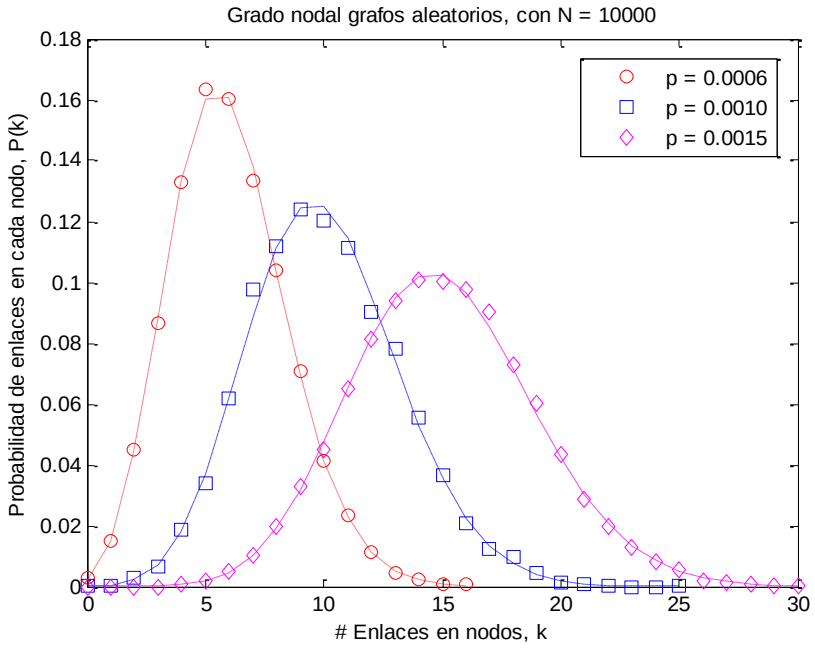


Figura 5.5: Distribución de grado nodal en grafos aleatorios

En la Figura 5.5 se compara la probabilidad de conexión de cada nodo del grafo de la ecuación [5.5] con el ajuste a la *función de probabilidad de Poisson* de la ecuación [5.7].

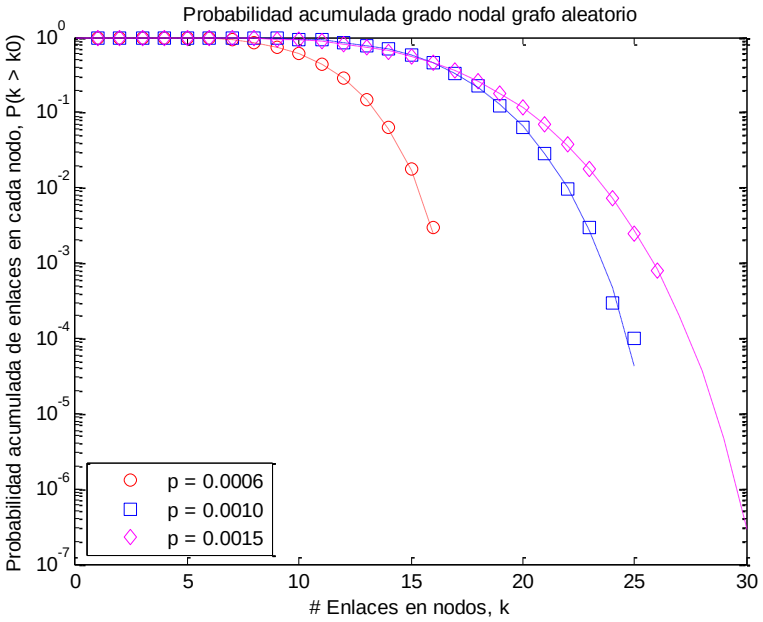


Figura 5.6: Distribución acumulada de grado nodal en grafos aleatorios

En la Figura 5.6 se compara la distribución de probabilidad acumulada de conexión de cada nodo del grafo de la ecuación [5.6] con el ajuste a la *función de probabilidad de Poisson* (ecuación [5.7]). Por ejemplo, $P(k \geq 1) = 1$, significa que la probabilidad que un nodo elegido aleatoriamente en el grafo tenga un grado $k \geq 1$ es del 100%.

- **Topología Libre Escala**: Los estudios presentados en [BARABÁSI & ALBERT, 1999] dieron lugar a demostrar que los grafos de libre escala tienen una distribución de probabilidad de ley de potencias en proporción a la cantidad de nuevos enlaces, especialmente para redes conformadas por una gran cantidad de nodos (Generalmente, N > 1000) según la siguiente expresión:

$$P(k) = (2 \cdot m^2) \times k^{-\gamma} \text{ , donde } \quad 2 < \gamma \leq 3 \qquad [5.8]$$

En la función de potencias [5.8] se ha demostrado que una buena práctica para estas grandes redes es tomar siempre $\gamma = 3$ [ALBERT & BARABÁSI, 2002]. Esto significa que la distribución de grado nodal se ajusta proporcionalmente al inverso del cubo de cada grado nodal, lo cual se suele simplificar como:

$$P(k) \sim k^{-3}, \quad \text{es decir,} \quad P(k) = \alpha \cdot k^{-3} \qquad [5.9]$$

En la Figura 5.7 se presenta una gráfica comparativa de la distribución del grado nodal para redes con diferentes número de nodos (N = 5000, 7500, 10000, 12500), y una segunda gráfica comparativa para diferentes enlaces de crecimiento $m = m_0$ = 1, 3, 5, 7. En todos los casos se aprecia su tendencia según la *distribución*

de probabilidad de ley de potencias, con pendiente $\gamma = -3$ (en línea de tendencia) [BARABÁSI & ALBERT, 1999].

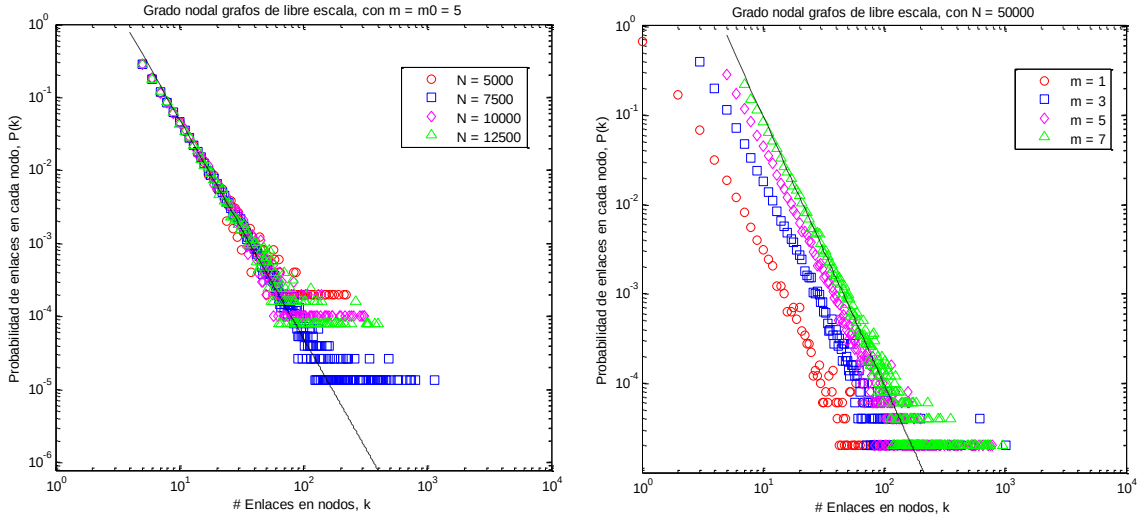


Figura 5.7: Distribución de grado nodal en grafos de libre escala.

A diferencia de los modelos aleatorios, cuya distribución de probabilidad corresponde a una campana donde la mayoría de los nodos comparten la misma cantidad de enlaces y no existen nodos altamente conectados, en estas redes de libre escala la lectura de su distribución de grado nodal indica que la mayoría de los nodos tienen pocos enlaces, pero unos pocos concentran la mayoría de los enlaces.

5.2.2 REPRESENTACIÓN TOPOLÓGICA DE LAS REDES ELÉCTRICAS

Dentro del objetivo propuesto al principio del presente capítulo, consistente en validar la teoría de grafos como método de estudio de vulnerabilidad en redes eléctricas, es preciso demostrar primero la propuesta de representación de las redes eléctricas de transporte y distribución en media y alta tensión como un *grafo de libre escala*. La validación de esta representación se realizará de acuerdo al estudio de la *distribución del grado nodal* de diferentes redes de prueba.

Algunos autores simplifican dicha representación mediante una red compleja donde las subestaciones corresponden a los nodos del sistema, y los enlaces están formados por líneas eléctricas [JELENIUS, 2004; HOLMGREN, 2006; HOLMGREN, 2007b; CHEN, DONG *et al.*, 2010; JOHANSSON, 2010]. Dicha aproximación permite estudiar la conformación de triángulos (clusters) y obtener medidas estadísticas de los grafos con los cuales determinar su vulnerabilidad.

Sin embargo, dicha representación aunque simple es incompleta, pues deja fuera el estudio de la vulnerabilidad de algunos activos muy importantes en la

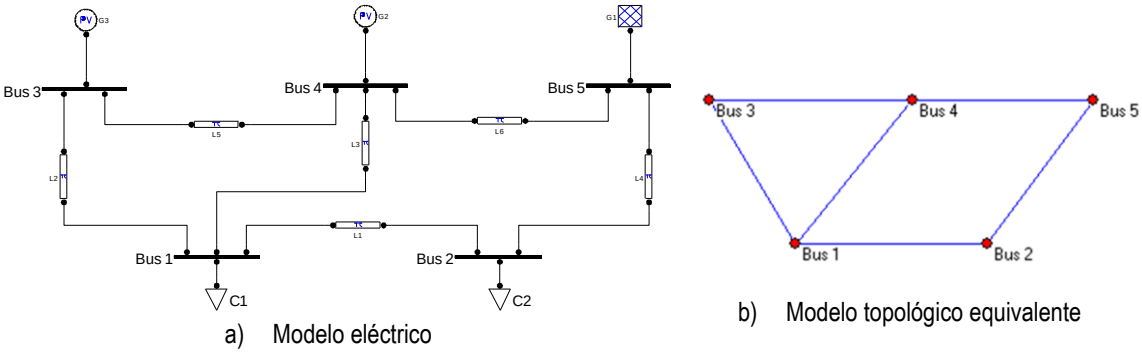
estructura de las redes eléctricas de alta y media tensión, como son las torres de transporte, los transformadores, los centros de generación, los centros de cargas, los bancos de condensadores, etc. Tampoco se ha demostrado hasta el momento que exista afinidad de los resultados estadísticos en teoría de grafos con las soluciones obtenidas mediante los modelos eléctricos, que incluyen flujos de cargas en los sistemas de potencia, correlación que se pretende demostrar posteriormente en este capítulo 5.

5.2.2.1 Topología de Libre Escala para redes de prueba IEEE

La propuesta de representar una red eléctrica como un grafo de libre escala consiste en desarrollar un modelo de la red eléctrica mediante teoría de grafos más completo que los propuestos hasta el momento por los diferentes autores, teniendo en cuenta una mayor cantidad de activos de la red.

La Figura 5.8 permite comparar la propuesta de representación topológica de una red eléctrica, en este caso la **red de prueba IEEE de 14 buses**. La representación eléctrica del sistema de potencia incluye cargas, líneas eléctricas, transformadores, barras, generadores, condensadores, etc. Su equivalente topológico tradicional como un grafo sólo tiene en cuenta los buses y las líneas que los conectan.

El ejemplo presentado en la Figura 5.8 está originalmente compuesto por cinco buses. La representación topológica tradicional de este modelo se refiere a un grafo de cinco nodos y seis enlaces. No se tiene en cuenta la existencia de centros de generación, ni centros de carga.



a) Modelo eléctrico b) Modelo topológico equivalente

Figura 5.8: Representación tradicional del sistema eléctrico (Red IEEE 5 buses).

En la Figura 5.9 se muestra la propuesta original de representación topológica de la red eléctrica como un grafo de libre escala. En este modelo topológico, la red resultante está constituida por un grafo de 16 nodos y 17 enlaces.

En lugar de enlaces, el grafo de libre escala considera las torres que sostienen las líneas eléctricas como nodos del sistema. Los transformadores conectados entre barras en una subestación también se consideran aquí como nodos del grafo.

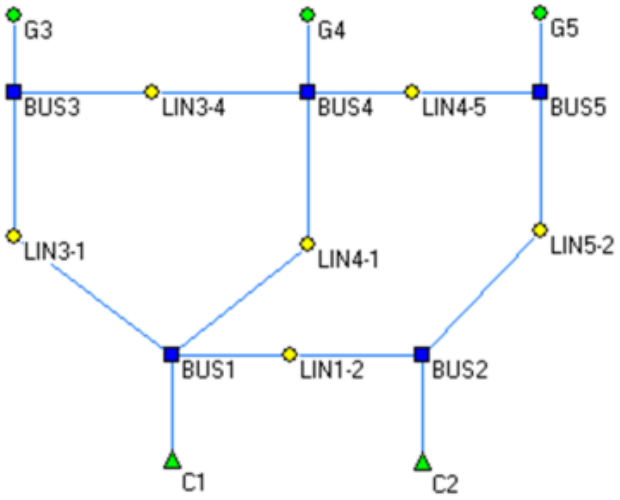


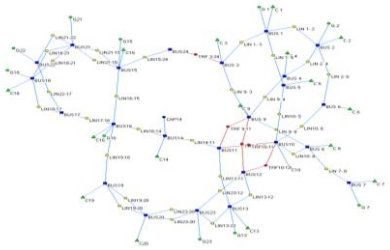
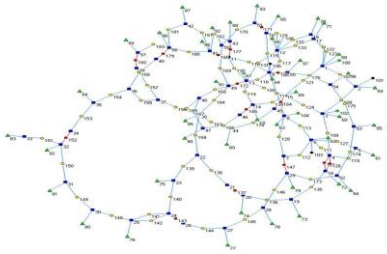
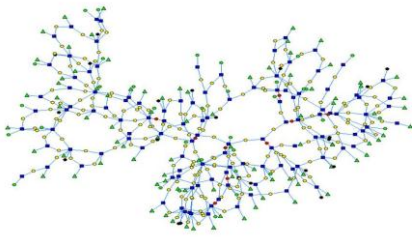
Figura 5.9: Propuesta de representación topológica como grafo de libre escala (Red IEEE 5 buses).

Para la representación topológica de cualquier sistema de potencia, sería natural estudiar la cantidad de activos que conforman una u otra red. Sin embargo, debido a que la información de los sistemas de potencia de cualquier región o país no siempre está disponible o su acceso está restringido, se hace necesario validar las metodologías propuestas mediante datos públicos.

Como aplicación de la metodología que se propone en esta sección para análisis de vulnerabilidad, se propone estudiar las redes de prueba de IEEE. Los archivos de redes de 14, 24, 30, 57 y 118 buses contienen la configuración completa de redes de transporte en alta y media tensión, de conformidad con el estándar IEEE [IEEE-Group, 1973]. Estas redes permitirán evaluar técnicamente los conceptos de robustez y vulnerabilidad del sistema de infraestructura crítica, con aplicación en un caso de estudio.

La Tabla 5.2 contiene la descripción de los modelos de red IEEE y su equivalencia, según la propuesta aquí presentada, como grafo de libre escala. Los grafos se han generado mediante el software *Pajek* [BATAGELJ & MRVAR, 2002].

Tabla 5.2: Representación topológica redes IEEE como grafos de libre-escala.

MODELO RED IEEE	EQUIVALENCIA GRAFO LIBRE-ESCALA	REPRESENTACIÓN GRAFO LIBRE ESCALA
14 buses: 16 líneas, 4 transformadores, 11 cargas, 1 generador, 1 slack, 3 capacitores.	50 nodos, 56 enlaces	
24 buses: 33 líneas, 5 transformadores, 17 cargas, 9 generadores, 1 slack, 1 capacitor.	90 nodos, 104 enlaces	
30 buses: 34 líneas, 7 transformadores, 21 cargas, 1 generador, 1 slack, 4 capacitores.	98 nodos, 109 enlaces	
57 buses: 65 líneas, 15 transformadores, 42 cargas, 3 generadores, 1 slack, 3 capacitores.	186 nodos, 209 enlaces	
118 buses: 177 líneas, 9 transformadores, 91 cargas, 33 generadores, 1 slack, 20 capacitores.	449 nodos, 517 enlaces	

A pesar que estas redes no son tan extensas, es evidente que una pequeña cantidad de los nodos contienen la mayor conectividad.

En resumen, la representación topológica propuesta en esta sección es más ajustada a la realidad del sistema eléctrico, haciendo énfasis en que tanto el conjunto de torres de transporte como los transformadores también deben ser considerados nodos en el sistema. En la siguiente sección 5.2.2.2 se demostrará matemáticamente

que esta representación de las redes eléctricas como grafos de libre escala es adecuada.

5.2.2.2 Distribución del grado nodal en redes de prueba IEEE

Una vez determinada la representación topológica más adecuada para las redes eléctricas, es preciso realizar la validación de la propuesta de representación de una red eléctrica como un grafo de libre escala.

En la Figura 5.10 se presenta la **distribución de grado nodal** de cada una de las redes de prueba descritas previamente en la Tabla 5.2, es decir, la probabilidad que un nodo elegido al azar tenga exactamente *k* conexiones, según se expresa en la ecuación [5.5]. El cálculo de la distribución de grado nodal se debe realizar computacionalmente, por cuya razón, el resultado presentado en dicha figura ha sido calculado con ayuda de las funciones para trabajo computacional con teoría de grafos disponible en la librería *MatlabBGL* [GLEICH, 2008].

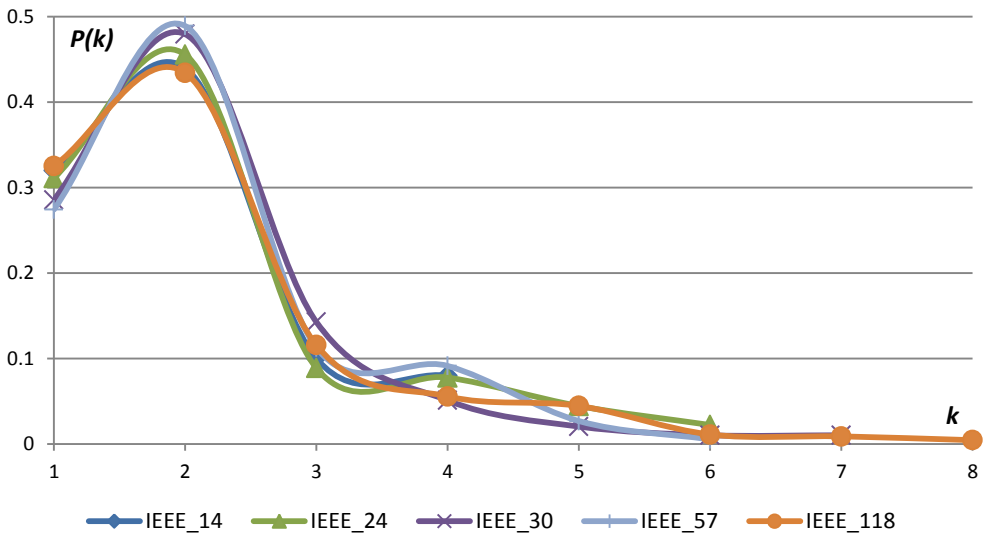


Figura 5.10: Función de distribución de grado nodal, grafos IEEE.

Obsérvese que en la Figura 5.10 la mayoría de nodos tiene grados nodales *k*=1 ó *k*=2. En todos los casos, entre un 40% y 50% de los nodos tienen un grado nodal *k* = 2, lo cual se explica porque la mayoría de éstos representan las torres de transporte, las cuales siempre están unidas a dos enlaces. Los nodos en antena, representados especialmente por condensadores, centros de generación y cargas, conectadas a las subestaciones (buses de flujo puro), tienen grado nodal *k* = 1. En todos los casos, esto representa cerca del 30% de los nodos de las redes de prueba IEEE. Adicionalmente, en cualquiera de las redes, la probabilidad que uno de sus

nodos tenga un grado nodal k= 3 es menor al 10%. La misma condición se cumple para k = 4.

Las redes más grandes tienen mayor probabilidad de tener asociados nodos con alto grado de conectividad. En el caso de la red de 118 buses, existen nodos conectividad k = 7 y k = 8. A priori, dichos activos deben ser considerados como importantes, pues su aislamiento del sistema podrá tener efectos significativos en el funcionamiento de toda la red.

Con el propósito de demostrar la aproximación sugerida en este capítulo (sección 5.2.2.1), para efectuar un tratamiento de los sistemas eléctricos de potencia como un grafo de libre escala, según se presentó anteriormente en la Tabla 5.2, se presenta una comparación entre los resultados obtenidos computacionalmente a través de la herramienta *MatlabBGL* [GLEICH, 2008], y su equivalente analítico como una ecuación de Ley de Potencias según se especifica en la teoría de redes complejas de libre escala [BARABÁSI & ALBERT, 1999; ALBERT & BARABÁSI, 2002].

De acuerdo con la ecuación [5.6] la *probabilidad acumulada* $P(k_i \geq k_0)$ consiste simplemente en la sumatoria de las probabilidades asociadas a la distribución de grados nodales. El cálculo de la probabilidad acumulada se efectúa para el rango $k_i \in [1, k_{máx}]$. Conceptualmente significa la probabilidad de que un nodo elegido al azar tenga más de k_0 enlaces.

$$P_{acum}(k_i) = P(k_i \geq k_0) = \sum_{i=1}^{k_0} P(k_i) \qquad [5.10]$$

Por otro lado, de las expresiones [5.8] y [5.9] es posible obtener la probabilidad de distribución de grado nodal $P(k_i)$ de forma analítica, como una **distribución en ley de potencias**, donde el valor de la probabilidad es proporcional a $k^{-\gamma}$ (con γ =3), teniendo en cuenta que el resultado $P_{acum}(k_i) \in [0, 1]$ debe estar normalizado.

$$P_{acum}(k_i) = \frac{\sum_{i=1}^{k_0} 2 \cdot m^2 / k_i^3}{\sum_{i=1}^{k_{máx}} 2 \cdot m^2 / k_i^3} \qquad [5.11]$$

Al simplificar la ecuación [5.11] se obtiene una expresión analítica que permite representar la probabilidad acumulada de la distribución del grado nodal en ley de potencias, donde el coeficiente α permite normalizar la expresión en el rango $P_{acum}(k_i) \in [0, 1]$, con $k_i \in [1, k_{máx}]$, $k_0 \in [1, k_{máx}]$.

$$P_{acum}(k_i) = P(k_i \geq k_0) = \underbrace{\sum_{i=1}^{k_{máx}} k_i^{-3}}_{\alpha} \cdot \sum_{i=1}^{k_0} \frac{1}{k_i^3} = \alpha \cdot \sum_{i=1}^{k_0} \frac{1}{k_i^3} \qquad [5.12]$$

La Tabla 5.3 contiene cálculos comparativos de la probabilidad acumulada en los diferentes grafos de libre escala que caracterizan algunas de las redes de prueba IEEE, obtenidos por un lado mediante cálculo computacional de la librería *MatlabBGL* y por otro lado mediante la expresión [5.12].

La información presentada en las columnas de la parte izquierda en la Tabla 5.3 contiene los mismos datos presentados anteriormente en la Figura 5.10, con la diferencia que se muestran en forma de probabilidad acumulada, es decir, la sumatoria de las probabilidades de cada grado nodal. En la parte derecha de la tabla se presenta el cálculo directo de la función de potencias presentada en la ecuación [5.12].

Tabla 5.3: Cálculo de probabilidad acumulada del grado nodal en redes IEEE de libre escala

	$P_{acum}(k_i) = P(k_i > K_0) = \Sigma(P(k_i))$				$P_{acum}(k_i) = \alpha \cdot \left(\sum_{i=1}^{k_0} \frac{1}{k_i^3}\right)$			
k_i	IEEE 118	IEEE 57	IEEE 30	IEEE 14	IEEE 118	IEEE 57	IEEE 30	IEEE 14
1	1.00000	1.00000	1.00000	1.00000	1.00000	1.00000	1.00000	1.00000
2	0.99555	0.99462	0.98980	0.94000	0.99837	0.99611	0.99756	0.99325
3	0.98664	0.96774	0.97959	0.86000	0.99593	0.98939	0.99368	0.98007
4	0.97550	0.87634	0.95918	0.76000	0.99205	0.97626	0.98697	0.94884
5	0.93096	0.76344	0.90816	0.32000	0.98536	0.94515	0.97388	0.84341
6	0.87528	0.27419	0.76531		0.97229	0.84013	0.94284	
7	0.75947		0.28571		0.94130		0.83808	
8	0.32517				0.83671			

Como información complementaria, se puede observar en la Figura 5.11 la alta correlación existente entre el cálculo computacional de la distribución de grado nodal y la función de potencias de la ecuación [5.12], para todas las redes IEEE bajo análisis.

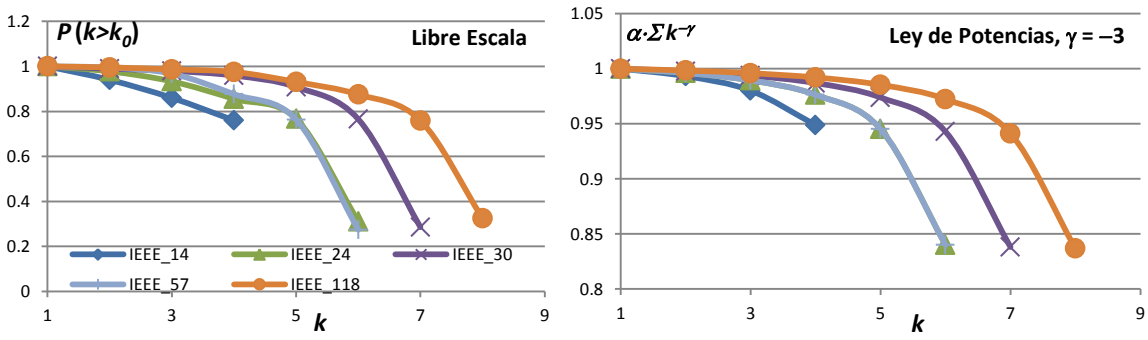


Figura 5.11: Función de probabilidad acumulada del grado nodal en redes de prueba IEEE.

En ambos resultados se puede leer $\boldsymbol{P}(k \geq 1) = 1$, lo cual simplemente significa que todos los nodos en los grafos tienen más de una conexión. Además la probabilidad de tener nodos con más de dos conexiones ($k \geq 2$) es elevada en todos los casos con probabilidad cercana a 1, y así sucesivamente con los demás grados nodales $\forall\ k_i \in [1, 8]$.

Es posible observar la alta similaridad existente entre ambas curvas de la Figura 5.11. Para corroborar esta afirmación se presenta en la Tabla 5.4 el cálculo del coeficiente de correlación de Pearson entre las dos curvas.

Tabla 5.4: Coeficiente de correlación entre funciones de probabilidad acumulada

Red	IEEE 14	IEEE 24	IEEE 30	IEEE 57	IEEE 118
Coeficiente Pearson	0.99720	0.99791	0.99931	0.99911	0.99964

Para una mayor información sobre el coeficiente de Pearson, se puede consultar la sección 5.3.5, en la que se explica más detalladamente dicho cálculo. En todos los casos, dado que el coeficiente es cercano a uno, se puede inferir que ambas curvas están altamente correlacionadas, y por tanto, es correcta la aseveración que se hizo al principio de esta sección, en el sentido de considerar las redes eléctricas como un grafo de libre escala con parámetro $\gamma = 3$.

En consecuencia, es correcta la aproximación de representación del sistema eléctrico como grafo de libre escala, donde las torres de transporte y los transformadores también constituyen nodos en la topología de la red.

5.2.3 INDICADORES EN GRAFOS DE LIBRE ESCALA

Los conceptos de desintegración de redes de libre escala fueron introducidos inicialmente por [ALBERT & BARABÁSI, 2002]. Dichos estudios demuestran la evolución de ciertos indicadores estadísticos de las redes complejas en caso de eventos de eliminación sistemática de sus nodos como consecuencia de sucesos aleatorios (tolerancia a los errores) o por acciones deliberadas (tolerancia a los ataques). El análisis de contingencias que ocasionan fallos en cascada en redes de libre-escala requiere el uso de parámetros que permitan medir la evolución en la conectividad, así como la funcionalidad de la red.

Esto puede realizarse mediante iteraciones sucesivas que representen la eliminación de nodos específicos de la red. Cada eliminación se asocia con una contingencia y se considera como un paso de iteración en el proceso de desintegración de la red.

La eliminación de un nodo también implica la desaparición de todos los enlaces que se conectan a él, y por tanto, los respectivos caminos geodésicos también desaparecen.

En esta sección se exponen algunas medidas estadísticas que describen los grafos de libre escala y que permitirán analizar la desintegración de las redes, es decir, su evolución ante la eliminación sucesiva de nodos. A partir de estas medidas, se propone el uso de un nuevo indicador de *vulnerabilidad geodésica*, el cual se comparará posteriormente en la sección 5.3 con otros indicadores para validar la equivalencia del uso de los grafos de libre escala respecto de las técnicas de flujos de carga en el análisis de vulnerabilidad de redes eléctricas.

5.2.3.1 Distancia geodésica

El concepto describe la menor distancia directa entre dos nodos, d_{ij}, mediante el conteo del número mínimo de nodos que deben recorrerse para unirlos.

Formalmente, dado un grafo $\boldsymbol{G} = (\boldsymbol{N}, \boldsymbol{E})$, un elemento $i \in \boldsymbol{N}$ encuentra un camino mínimo d_{ij} desde i hasta $j \in N$, tal que [JOHANSSON, 2010]:

$$\underset{i=2\cdots N}{d_{ij}} = \min_{j \in N(i)} \left(d_j\right)_i \qquad [5.13]$$

Si no hubiera conexión alguna entre dos nodos se dice que la distancia es infinita.

Las distancias de todos los vértices de un grafo se computan en lo que se denomina **matriz de distancias**. La generación de esta medida del grafo también es conocida como el *problema de las distancias más cortas* entre dos nodos [NEWMAN, 2003].

En la literatura es frecuente encontrar diferentes algoritmos que permiten solucionar este problema y cuya aplicación es evidente en aspectos de la vida diaria, como los dispositivos GPS o los mapas callejeros informatizados, que informan a sus usuarios las rutas más óptimas.

A partir del cálculo de las distancias geodésicas es posible establecer el **indicador de distancia media geodésica**, que describe cuán compacta es una red. Tiene en cuenta el número total de nodos del grafo N y las respectivas distancias geodésicas $d(i,j)$ entre los nodos del grafo [HOLMGREN, 2006; JOHANSSON, 2010]

$$\overline{d} = \frac{1}{N \cdot (N-1)} \sum_{i \neq j} d_{ij} \qquad [5.14]$$

Como información, los procedimientos más usuales en el cálculo de las distancias geodésicas son los algoritmos Dijkstra, Bellman–Ford, Floyd-Warshall y Johnson [GROSS & YELLEN, 2004].

5.2.3.2 Coeficiente de agrupamiento (Clustering)

Esta medida estadística cuantifica cómo está agrupado (o interconectado) con sus vecinos un determinado grafo. Es una medida muy útil cuando se evidencia que la conformación de enlaces forma triángulos (conocidos como **cliques** o **clusters**).

La medida de agrupamiento ***C*** se calcula mediante los coeficientes locales de agrupamiento $\boldsymbol{C_i}$, los cuales tienen en cuenta el número de enlaces $\boldsymbol{E_i}$ que existen entre los nodos vecinos de un vértice particular (*i*), así como el grado nodal $\boldsymbol{k_i}$ de esos nodos vecinos [WATTS & STROGATZ, 1998]:

$$C = \frac{1}{N}\sum_{i=1}^{N} C_i \ , \text{ donde } \ C_i = \frac{2 \cdot E_i}{k_i \cdot (k_i - 1)} \qquad [5.15]$$

Cuanto mayor sea este índice, mayor es la densidad de grupos o *clusters* dentro del grafo, en forma de triángulos. Dicha medida tiene gran aplicabilidad en el estudio de *grafos de mundo pequeño*, aunque también se suele emplear en el estudio topológico de los demás tipos de grafos [NEWMAN, 2003].

5.2.3.3 Intermediación (Betweenness)

Es una medida estadística de los grafos que trata de capturar la importancia de un determinado nodo. Indica la frecuencia con la que un nodo aparece en el camino más corto que conecta a otros dos nodos [WANG, ZHANG *et al.*, 2011]. A dicho camino se le suele denominar *distancia geodésica*.

La medida de *intermediación* o *betweenness* indica tanto el control del flujo, como la capacidad de mantener separadas las diversas partes de una red [JOHANSSON, 2010]. Existe una definición formal en la teoría de grafos donde la intermediación C_B para un grafo con ***N*** nodos [CHEN, DONG *et al.*, 2009] se expresa como:

$$C_B = \sum_{i \in N} \sum_{j \in N} \frac{d_{ij}(N)}{d_{ij}} \qquad [5.16]$$

El cálculo de los coeficientes de intermediación de cada uno de los nodos del grafo, se puede realizar por medio de algoritmos Bellman-Ford, Floyd-Warshall (grafos estándares), o Johnson (para grafos más dispersos) [GROSS & YELLEN, 2004]

5.2.3.4 Eficiencia geodésica

Este indicador fue propuesto inicialmente por [LATORA & MARCHIORI, 2001], con la intención de cuantificar la eficiencia con que se puede intercambiar información dentro de una red. Se asume que el flujo entre dos nodos debe realizarse a través de la distancia geodésica más corta [CHEN, DONG *et al.*, 2009; CHEN, DONG *et al.*, 2010]. Por tanto, la eficiencia entre un par de nodos e_{ij} se define como la inversa de su distancia. Si no hubiera conexión alguna entre dos nodos, $d_{ij} \approx \infty$, $e_{ij} = 0$.

Al conocer la eficiencia entre los pares de nodos de una red, entonces se puede calcular la *eficiencia geodésica del grafo* como:

$$\bar{e} = \frac{1}{N \cdot (N-1)} \sum_{i \neq j} \frac{1}{d_{ij}} \qquad [5.17]$$

En un sistema eléctrico de potencia, una baja eficiencia geodésica significa que el flujo de energía eléctrica debe circular a través de un mayor número de nodos, y en consecuencia, pueden aumentar los problemas de capacidad o de sobrecargas.

5.2.3.5 Índice de Vulnerabilidad Geodésica ($\bar{v}$)

De manera alternativa se propone utilizar el índice de ***vulnerabilidad geodésica media***, que está directamente relacionado la *eficiencia geodésica* (ecuación [5.17]). Esta propuesta de indicador permite medir mejor la funcionalidad de una red cuando está sujeta a eventos de contingencias, dado que permite estandarizar la eficiencia geodésica y hacer una comparación efectiva en la evolución de las sucesivas iteraciones de eliminación de nodos en una red eléctrica respecto de su condición en estado estable (caso base, previo a la aparición de contingencias)

$$\bar{v} = 1 - \frac{\sum_{i \neq j} \left(\frac{1}{d_{ij}^{LC}} \right)}{\sum_{i \neq j} \left(\frac{1}{d_{ij}^{BC}} \right)} \qquad [5.18]$$

d_{ij}^{LC}: distancia geodésica entre los pares de nodos del grafo de libre escala, después de cada iteración de eliminación de un nodo.

d_{ij}^{BC}: distancia geodésica entre los pares de nodos del grafo de libre escala, para el caso base.

El índice $\bar{v}$ varía entre cero y uno. Cuanto mayor sea el valor del índice $\bar{v}$, mayor es el impacto en la red, debido a problemas de congestión y por fallos en cascada, dada la interrupción de varias rutas geodésicas.

5.2.3.6 Índice de Impacto en la conectividad (S)

Este indicador se relaciona con el funcionamiento de la topología del sistema, cuando se aísla o se elimina un nodo específico. Está relacionado con las medidas estadísticas de grado nodal, y se calcula fácilmente, determinando la cantidad de nodos que quedan conectados al grafo, durante los eventos de contingencias [MOTTER & LAI, 2002].

$$S = 1 - \frac{N^{LC}}{N} \qquad [5.19]$$

N^{LC}: cantidad de nodos conectados en el grafo de libre escala residual, después de cada iteración de eliminación de un nodo.

N : número total de nodos del grafo de libre-escala.

La funcionalidad y el funcionamiento de la red cuantificadas en [5.18] y [5.19] se miden como función de la *fracción de nodos eliminados* (*f*).

5.2.4 CÁLCULO DE PARÁMETROS MEDIANTE FLUJOS DE CARGA

La manifestación de uno o de múltiples riesgos (como aquellos evaluados previamente en el capítulo 4) pueden ocasionar la salida de operación de uno o varios elementos del sistema de potencia (de manera programada o fortuita). Adicionalmente, la salida de un elemento puede dar origen a la salida de otros elementos, pudiéndose producir un efecto en cascada que eventualmente conduce al colapso del sistema [GÓMEZ-EXPÓSITO, 2002].

Aunque el análisis estructural de vulnerabilidad puede desarrollarse mediante el estudio de la evolución de los índices de teoría de grafos especificados en [5.18] y [5.19] (que permiten describir la tolerancia a los errores y ataques de las redes), dichas evaluaciones no tienen en cuenta valores eléctricos en sus cálculos. Por tanto, es preciso utilizar herramientas clásicas de ingeniería como los flujos de carga para comparar sus resultados en el análisis de contingencias con resultados de la teoría de grafos. Los cálculos de las potencias y tensiones en cada bus del sistema de potencia se desarrollan a partir de rutinas estándares (*SPF – Standard Power Flow*) [GÓMEZ-EXPÓSITO, 2002] y continuadas (*CPF – Continuation Power Flow*) [MILANO, 2003; MILANO, 2009].

Con el objetivo de medir el impacto en la cantidad de demanda eléctrica no suministrada como consecuencia de las contingencias sucesivas generadas por los fallos en cascada, se propone el uso del *índice de desconexión de cargas* PLS, según

se explica más adelante en esta sección, calculado a partir de los resultados obtenidos con la ejecución de flujos de carga.

5.2.4.1 Rutina de flujos de carga estándar (SPF)

Un sistema de potencia normalmente es operado bajo condiciones de equilibrio, donde el balance energético cumple la siguiente condición:

Potencia_Cargas + Potencia_Pérdidas = Potencia_Generación [5.20]

En ocasiones, el sistema requerirá mayor generación de potencia activa para compensar los desbalances de tensión debido a la súbita desconexión de carga, o por la necesidad de proporcionar más energía cuando se aíslan otros generadores.

Una rutina SPF (Standard Power Flow) requiere la selección arbitraria de un bus como generador de referencia (*generador slack*). La ecuación no lineal en [5.21] se soluciona iterativamente mediante el método Newton-Raphson, según se muestra en el diagrama de la Figura 5.12 [GÓMEZ-EXPÓSITO, 2002].

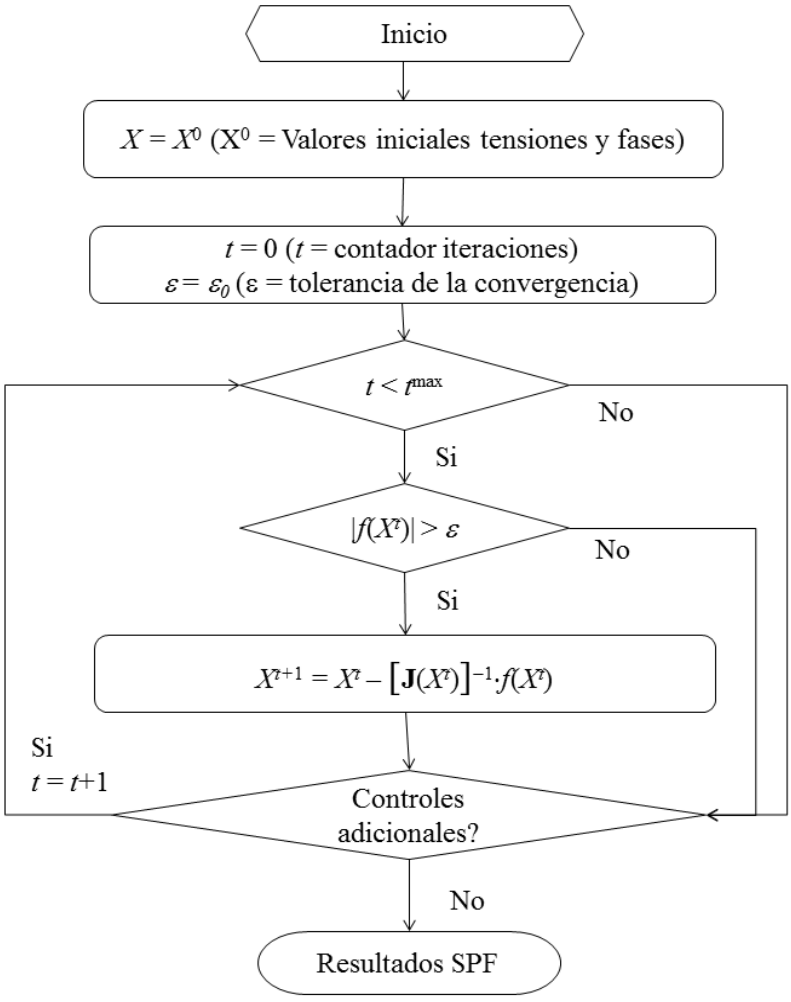


Figura 5.12: Diagrama de flujo rutina SPF.

En [5.21] se asigna al principio valores iniciales para todos los parámetros desconocidos (magnitud de la tensión y ángulo en buses de carga y de generación).

$$X^{t+1} = X^{t} - [\mathbf{J}(X^{t})]^{-1} \cdot f(X^{t}) \quad [5.21]$$

$$|f(X^{t})| > \varepsilon \quad [5.22]$$

t: contador de iteraciones

t^{max}: número máximo de iteraciones

ε: tolerancia de la convergencia (en p.u.)

X^{t}: Tensiones/Fases en la t^{o} iteración.

$$X^{t+1} = \begin{bmatrix} \theta^{t} + \Delta\theta \\ |V|^{t} + \Delta|V| \end{bmatrix} \quad [5.23]$$

$f(X^{t})$: Ecuaciones de desequilibrio

$$\Delta P_i = -P_i + \sum_{j=1}^{N} |V_i||V_j|\left(G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}\right) \quad [5.24]$$

$$\Delta Q_i = -Q_i + \sum_{j=1}^{N} |V_i||V_j|\left(G_{ij}\sin\theta_{ij} + B_{ij}\cos\theta_{ij}\right) \quad [5.25]$$

$\mathbf{J}(X^{t})$: Matriz Jacobiana

$$J = \begin{bmatrix} \dfrac{\partial\Delta P}{\partial\theta} & \dfrac{\partial\Delta P}{\partial|V|} \\ \dfrac{\partial\Delta Q}{\partial\theta} & \dfrac{\partial\Delta Q}{\partial|V|} \end{bmatrix} \quad [5.26]$$

En [5.24] y [5.25] P_i es la potencia activa neta y Q_i es la potencia reactiva neta inyectada en el bus i.

G_{ij}: parte real en la matriz de admitancias (diferente a la matriz de adyacencias).

B_{ij}: parte imaginaria en la matriz de admitancias (fila i^{o} y columna j^{o}).

θ_{ij}: ángulo entre las tensiones del nodo i^{o} y el nodo j^{o} .

5.2.4.2 Rutina de flujos de carga continuados (CPF)

Una rutina de **flujos de carga continuados** (CPF – Continuation Power Flow) permite resolver el flujo de cargas en un sistema de potencia, cuando no existe convergencia de la respuesta de una rutina estándar SPF. Es decir, el parámetro de tolerancia ε en [5.22] no converge dentro de los valores definidos en el Método de

Newton-Raphson. Esta condición ocurre cuando la matriz jacobiana $\mathbf{J}(X^t)$ [5.26] encuentra singularidades en la solución de los flujos de carga en puntos críticos de operación.

La rutina CPF implementada en PSAT consiste en la ejecución de un continuo de soluciones predictivas-correctivas mediante flujos de carga para determinar las tensiones en los buses y el flujo de potencias en las líneas, que garantizan el **punto crítico de operación** de manera que el sistema alcance su estado estable [AJJARAPU & CHRISTY, 1992]. Un resultado interesante en la ejecución de esta rutina es que se generan valores intermedios que permiten identificar una curva P-V en cada uno de los buses, que caracteriza la operación del sistema [MILANO, 2003].

El cálculo del punto crítico de operación en la rutina CPF incluye la formulación de un parámetro de carga λ. Como se muestra en la Figura 5.13, el cálculo parte de una solución conocida y usa una línea **tangente predictiva** para estimar la siguiente solución, correspondiente a otro valor del parámetro λ. Dicha estimación se perfecciona con una **línea correctiva** utilizando el mismo algoritmo Newton-Raphson para SPF [AJJARAPU & CHRISTY, 1992]. Dicha parametrización local proporciona el método para eludir las singularidades en el cálculo del jacobiano.

La rutina CPF es más general que la rutina SPF, aunque demanda mayor tiempo de computación. La Figura 5.14 permite identificar el procedimiento requerido para desarrollar una rutina CPF [AJJARAPU & CHRISTY, 1992], que se debe ejecutar cuando no converge la rutina SPF, teniendo en cuenta la generación de datos con la tangente predictiva y línea predictiva en cada punto de la curva PV.

El algoritmo de cálculo tiene en cuenta la introducción del parámetro de carga. En el caso que $\lambda = 0$, corresponde a la solución del caso base y $\lambda = \lambda_{máx}$, significa la operación en el punto crítico de la curva P-V.

$$0 \leq \lambda \leq \lambda_{máx} \qquad [5.27]$$

En consecuencia, la ecuación de desequilibrio del sistema aumentadas con el parámetro de carga λ, se representan en [5.28]

$$F(X,\lambda) = 0 \qquad [5.28]$$

En [5.28], la variable X^t hace referencia a la magnitud de las tensiones y ángulos de fases en la t° iteración.

$$X^{t+1} = \begin{bmatrix} \theta^t + \Delta\theta \\ |V|^t + \Delta|V| \end{bmatrix} \qquad [5.29]$$

La linealización de [5.28] se realiza con la ejecución del algoritmo de pasos correctivos y predictivos.

$$d\mathbf{F}(\mathbf{X},\lambda) = \mathbf{F}_X \cdot d\mathbf{X} + \mathbf{F}_\lambda \cdot d\lambda = 0 \qquad [5.30]$$

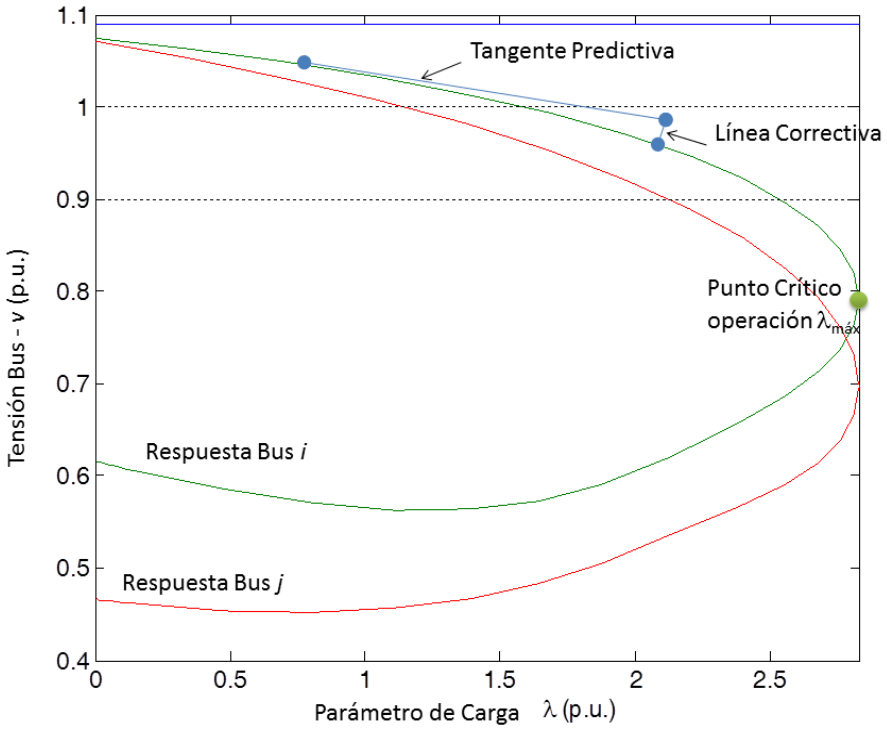


Figura 5.13: Esquema de soluciones predictivas-correctivas en rutina CPF.

La solución de [5.30] requiere de una variable auxiliar asociada al vector de la tangente predictiva, $k^t = \pm 1$, siendo k^t un número diferente de cero, del vector tangente $d\mathbf{X}$. La solución del vector de predicción $d\mathbf{X}$ y $d\lambda$ requerirá entonces la solución de la ecuación de desequilibrio aumentada.

$$\begin{bmatrix} F_X & F_\lambda \\ \varepsilon^t & \end{bmatrix} \begin{bmatrix} dX \\ d\lambda \end{bmatrix} = \begin{bmatrix} 0 \\ \pm 1 \end{bmatrix} \qquad [5.31]$$

ε^t es un vector con elementos iguales a cero, excepto el correspondiente a la posición de la tº iteración que se sugiere sea asignado como ± 1 [AJJARAPU & CHRISTY, 1992], dependiendo si se ha alcanzado el punto crítico de operación. Al solucionar [5.31], la predicción del punto en la curva PV queda dada por [5.32], donde σ es un escalar que representa el paso de la iteración.

$$\begin{bmatrix} X^{t+1} \\ \lambda^{t+1} \end{bmatrix} = \begin{bmatrix} X^t \\ \lambda^t \end{bmatrix} + \sigma \begin{bmatrix} dX \\ d\lambda \end{bmatrix} \qquad [5.32]$$

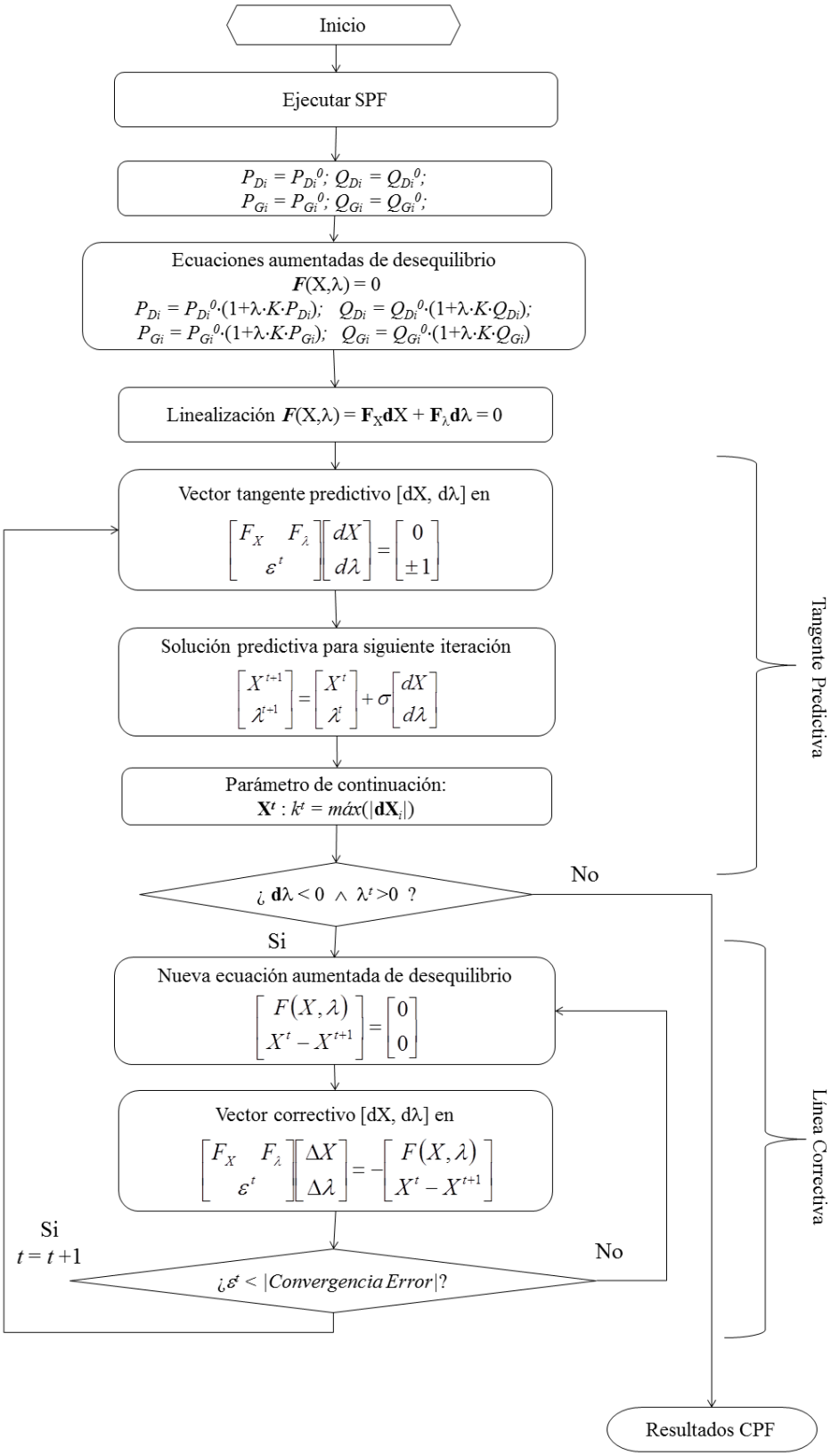


Figura 5.14: Diagrama de flujo rutina CPF.

Finalmente, el cálculo del vector de corrección en la rutina CPF, consistente en un conjunto de ecuaciones no-lineales aumentadas con el parámetro λ, se solucionan iterativamente con el método de Newton [AJJARAPU & CHRISTY, 1992; MILANO, 2009], a partir de la ecuación [5.33]

$$\begin{bmatrix} F_X & F_\lambda \\ \varepsilon^t & \end{bmatrix}\begin{bmatrix} \Delta X \\ \Delta\lambda \end{bmatrix} = -\begin{bmatrix} F(X,\lambda) \\ X^t - X^{t+1} \end{bmatrix} \qquad [5.33]$$

5.2.4.3 Índice de Desconexión de Cargas (PLS)

El análisis de **contingencias N-1** en sistemas de potencia está ampliamente documentado. Algunos de los parámetros más usuales para evaluar su impacto corresponden a: *Condiciones Máximas de Carga* [MILANO, 2003], *Información Comprensiva del Sistema* [HAIDAR, MOHAMED *et al.*, 2008], *Pérdidas de Potencia en el Sistema* [HAIDAR, MOHAMED *et al.*, 2007; BRANCUCCI, BOLADO *et al.*, 2012] y los *Índices de Severidad* [GÓMEZ-EXPÓSITO, 2002]. Como información, en el ANEXO C se presentan algunas formulaciones metodológicas con las cuales se puede realizar el análisis de contingencias N-1 en sistemas de potencia. Los modelos que se evalúan corresponden a las redes de prueba de IEEE de 14, 24, 30, 57 y 118 buses [IEEE-Group, 1973].

Para el estudio de **fallos en cascada** es necesario efectuar el cálculo de la funcionalidad del sistema de potencia mediante la estimación de las cargas en servicio en eventos de contingencias. Un índice intuitivo para comprender la evolución de estos eventos en cascada corresponde al *Índice de Desconexión de Cargas*, que originalmente ha sido propuesto como ***PLS*** (*Power Load Shedding*) [SALMERON, WOOD *et al.*, 2004]

$$PLS = 1 - \frac{\sum_i \sqrt{\left(P_{Di}^{LC} + Q_{Di}^{LC}\right)^2}}{\sum_i \sqrt{\left(P_{Di}^{BC} + Q_{Di}^{BC}\right)^2}} \qquad [5.34]$$

P_{Di}^{LC}: potencia activa que permanece eléctricamente conectada, después de cada iteración de eliminación de un nodo.

Q_{Di}^{LC}: potencia reactiva que permanece eléctricamente conectada, después de cada iteración de eliminación de un nodo

P_{Di}^{BC}: potencia activa en el caso base.

Q_{Di}^{BC}: potencia reactiva en el caso base.

El índice *PLS* en [5.34] se calcula como porcentaje de la carga que se desconecta después de cada eliminación de un nodo y varía entre cero y uno. Cuanto mayor sea el valor de *PLS*, mayor será el impacto de *energía no suministrada* a los consumidores.

5.3 TOLERANCIA CONTRA ATAQUES Y ERRORES EN REDES

Como se explicó al comienzo de este capítulo (sección 5.2.2), se ha despertado un notable interés por investigar el comportamiento de las redes complejas, su robustez, su resiliencia y vulnerabilidad ante los diferentes riesgos que afecten su funcionamiento. Adicionalmente, bajo el objetivo de validar la aplicación de teoría de grafos como herramienta adecuada para el análisis de vulnerabilidad en el sector de infraestructura eléctrica, es posible cuantificar las consecuencias asociadas a los riesgos críticos e importantes establecidos anteriormente en la sección 4.3.3 (riesgos sobre sistemas de transporte de alta y media tensión).

El estudio de la vulnerabilidad de los sistemas de potencia ha sido liderado por las empresas propietarias y operadoras de la red de infraestructura crítica. La mayoría de estos estudios se realizan después de eventos de gran impacto (por ejemplo, un *blackout* generalizado), mediante la determinación de sus causas en un sistema de potencia específico. Dichos estudios pueden conducirse a través del *análisis estructural de la vulnerabilidad* en redes de transporte, que exigen metodologías bien definidas para guiar la toma de decisiones en la prevención y recuperación de dichos eventos. Por ejemplo, los estudios de contingencias *N*-1 y *N*-*t* [GÓMEZ-EXPÓSITO, 2002; MILANO, 2003; QIMING & McCALLEY, 2005] se encuentran entre los criterios más generalizados en la industria eléctrica.

El énfasis propuesto en esta tesis se fundamenta en los modelos de contingencias aplicados con teoría de grafos. Muchas redes complejas ostentan una notable tolerancia contra errores y ataques a sus estructuras. Se ha podido demostrar que la topología de la red juega un papel importante en la tolerancia a los errores en sistemas complejos. Por ejemplo, el funcionamiento de internet (una red compleja de comunicaciones) presenta una buena robustez: a pesar que exista un mal funcionamiento de algunas componentes claves del sistema, los fallos locales raramente conducen a la pérdida de información o a la capacidad de permitir el flujo de información en toda la red. La estabilidad de este sistema (y también, otras redes complejas) normalmente se atribuye a las rutas redundantes de sus estructuras [MURRAY, MATISZIW *et al.*, 2007].

Los conceptos sobre desintegración de las redes de libre escala fueron inicialmente introducidos por [ALBERT & BARABÁSI, 2002], cuyos estudios presentan el funcionamiento de las redes complejas en eventos de eliminación sistemática de nodos de manera **aleatoria** (“tolerancia contra errores”) o de manera **deliberada** (“tolerancia contra ataques”). En la Tabla 5.1 se presentan otros estudios documentados sobre la comparación de tolerancias de redes complejas aplicadas al sector de los sistemas eléctricos de potencia.

5.3.1 ESTRATEGIAS DE ELIMINACIÓN Y AISLAMIENTO DE NODOS

Partiendo de una red conectada, en cada iteración se elimina un nodo. El aislamiento (o desaparición) de ese nodo implica la eliminación de todos los enlaces conectados a él, tal y como se ilustra en la Figura 5.15, con la consiguiente desaparición de los caminos existentes entre ellos.

Obsérvese que inicialmente la distancia geodésica entre *Bus 3* y *Bus 5* es $d_{3-5} = 3$, pero después que se eliminan dos nodos del sistema, la distancia geodésica se hace infinita ($d_{3-5} \approx \infty$), al tiempo que la red se divide en 7 grupos independientes (de ellos, cuatro nodos sin enlaces).

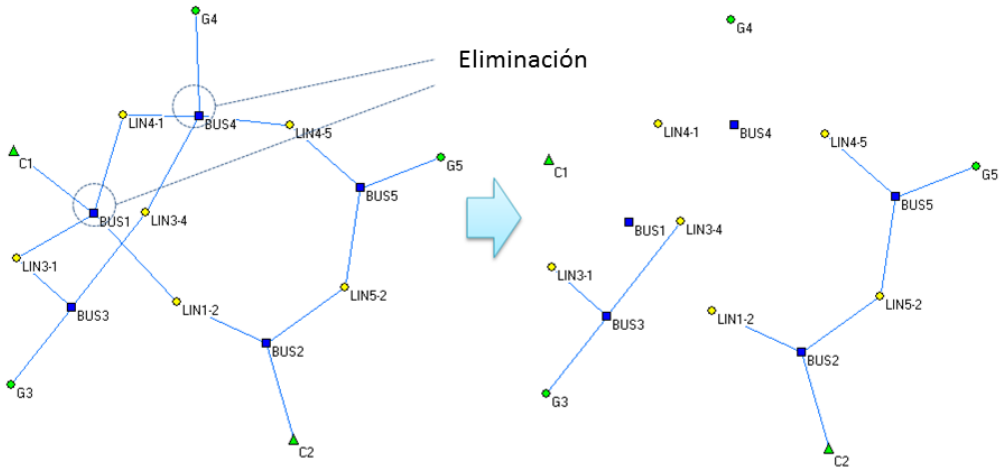


Figura 5.15: Efectos de la eliminación o aislamiento de dos nodos en una red inicialmente conectada.

La medición del funcionamiento de la red se obtiene mediante el tamaño relativo del grupo de mayor tamaño, es decir, su índice de conectividad [5.19]. Igualmente, se recomienda medir la *distancia geodésica media* del sistema, o como alternativa, la *eficiencia geodésica* del grafo resultante [5.17].

Hasta la fecha no se conocen estudios sobre la efectividad de los procedimientos de la teoría de grafos, y su comparación con los procedimientos

tradicionales en el análisis de sistemas de potencia (flujos de carga, análisis de estabilidad, etc), que permitan corroborar su validez en el estudio de fallos en cascada. Aunque los índices de conectividad y de eficiencia geodésica no reflejan idealmente la sensibilidad de un sistema de potencia, sí pueden ser de mucha utilidad cuando se comparan diferentes redes en distintas configuraciones.

Los análisis detallados de las redes eléctricas de transporte a nivel local y nacional suelen estar ceñidos exclusivamente al interés de las empresas propietarias y operadoras del sistema. Algunos procedimientos de sus estudios internos determinan la capacidad de transferencia de potencia entre los nodos de generación y de carga. Adicionalmente, se aplican las técnicas tradicionales de cuantificación de variables en contingencias N-1 y N-2, pero los fallos en cascada se analizan usualmente mediante estudios a-posteriori a la ocurrencia de eventos de alto impacto, como un *blackout* extendido.

En esta sección, el análisis estructural de vulnerabilidad en sistemas de potencia se centra en el estudio de su funcionamiento, por la eliminación o aislamiento de los nodos y enlaces que componen la red de infraestructura. Lo anterior, mediante la comparación entre la estructura y la topología de las diferentes redes de prueba IEEE. Adicionalmente, se analiza cómo el cambio en su estructura afecta la vulnerabilidad de las redes. Dos estrategias de eliminación de nodos serán tenidas en cuenta: por fallos aleatorios en la red y por ataques deliberados.

5.3.1.1 Estrategia de eliminación por errores y fallos aleatorios

La tolerancia al error corresponde a aquellos daños ocasionados en los sistemas de infraestructuras relacionadas con contingencias aleatorias, por ejemplo, fenómenos naturales, fallos en equipos o fallos humanos y de procedimiento.

La metodología propuesta para estudiar los errores aleatorios se realiza sobre la base de múltiples simulaciones que permiten construir un muestreo con el valor de cada uno de los indicadores del sistema de potencia.

También se pretende validar la hipótesis según la cual existe una equivalencia entre los resultados obtenidos mediante teoría de grafos y los resultados de los flujos de carga, para lo cual se analiza la evolución de los indicadores planteados al inicio del capítulo (secciones 5.2.3 y 5.2.4.3).

5.3.1.2 Estrategia de eliminación por ataques deliberados

El sistema de infraestructura puede estar sometido a amenazas de terrorismo y vandalismo, que infringen daños malintencionados en el sistema de potencia, haciéndolo más vulnerable. Este tipo de ataques a la red se pueden modelar mediante la eliminación de los vértices que tienen el mayor grado nodal [ALBERT & BARABÁSI, 2002; HOLMGREN, 2006]. En este tipo de estudios, en cada iteración se elimina cada vértice según el orden descendiente de los grados nodales. En algunos otros estudios también se analiza la tolerancia a los ataques calculando nuevamente los grados nodales en cada iteración, planteando un escenario dinámico, donde los ataques a la estructura de la red pueden ser más dañinos que aquellos dirigidos al valor inicial del grado de conexión [JELENIUS, 2004; HOLMGREN, 2006]

En la propuesta de ataques deliberados según los grados nodales que aquí se define, los blancos de la red se escogen de manera determinística por parte del atacante, aunque dicha estrategia sea desconocida por quienes lleven a cabo la protección del sistema. Un escenario extremo, pero posible, es aquel en el que los blancos de la red son aquellos definidos como los más importantes, sea por su grado de conexión [HOLMGREN, JENELIUS *et al.*, 2007], o también por su grado de intermediación (*betweenness)* [JOHANSSON, 2010; CHEN, ZHAO *et al.*, 2011].

Dada la aproximación según la cual las redes eléctricas de transporte en alta y media tensión se asemejan a una red de libre escala, la estrategia metodológica de estudio para los ataques deliberados tendrá en cuenta el grado nodal del caso base, para estudiar sus posibles fallos en cascada.

5.3.2 ALGORITMO PARA COMPARACIÓN DE ÍNDICES DE TEORÍA DE GRAFOS VERSUS PARÁMETROS DE FLUJOS DE CARGA

En esta sección se ha establecido la hipótesis que plantea la equivalencia entre índices de la teoría de grafos y parámetros de flujos de carga. Para corroborar dicha aseveración, se elabora un algoritmo que permita analizar sucesivamente los indicadores planteados al inicio del capítulo (secciones 5.2.3.5, 5.2.3.6 y 5.2.4.3).

Partiendo de un sistema que opera en condiciones estables (caso base), se desarrolla un modelo dinámico que tiene en cuenta los efectos de fallos en cascada para simular la evolución de los índices del sistema eléctrico de potencia. En la Figura 5.16 se ilustra el procedimiento diseñado para el estudio de las estrategias de fallos aleatorios y ataques deliberados en sistemas eléctricos de potencia, representados en redes de prueba IEEE.

Para el caso de ataques delibrados se necesita sólo una muestra, pero se realizan múltiples muestreos para los fenómenos aleatorios. Por su naturaleza aleatoria, la distribución de los resultados asociados a estas perturbaciones son altamente asimétricos, es decir, los valores obtenidos tienen muy poco parecido a una distribución normal. Para estos casos, se sugiere tomar el enunciado del **teorema central del límite**, según el cual, es posible hacer una aproximación como *distribución normal* para todos los valores, si el tamaño de las muestras es relativamente grande. Puede concluirse que la aproximación será suficientemente buena si el número de muestras es superior a 30 [ANDERSON & SWEENEY, 2008].

Los eventos de eliminación de fallos en cascada se determinan de acuerdo a la estrategia de eliminación de nodos. Básicamente se realizan iteraciones sucesivas de contingencias N−1 sobre una red que cambia constantemente su estructura con la eliminación de cada nodo. Dado que no es posible realizar flujos de carga sin la existencia del generador de referencia, entonces los nodos se eliminan alrededor del *bus generador slack*.

El algoritmo de la Figura 5.16 se ha implementado en lenguaje ***Matlab*** ®. Para su implementación, en la programación del algoritmo se han tenido en cuenta las funciones de análisis de sistemas eléctricos de potencia, proporcionadas por la herramienta ***PSAT*** (Power System Analysis Toolbox) [MILANO, 2005; MILANO, 2012].

Este programa cuenta además con funciones de la herramienta ***MatlabBGL*** para teoría de grafos [GLEICH, 2008], que entre otras, incluye diferentes algoritmos para el cálculo de distancias geodésicas (en este programa en particular, se emplea el *algoritmo Bellman-Ford para cálculo de distancias más cortas* [GROSS & YELLEN, 2004]).

La constante reconfiguración de la red, como consecuencia de la eliminación sucesiva de nodos, genera divergencias en los resultados de los flujos de carga cuando se ejecuta la rutina de ***flujos de carga estándar*** (SPF). Para esos casos, una conveniente función de PSAT permite obtener resultados de los flujos de potencia en la red mediante la ejecución de ***flujos de carga continuados*** (CPF), sin necesidad de ejecutar rutinas de optimización. De esta manera, es posible calcular la tolerancia de la red, mediante la obtención de la proporción de cargas que se desconectan en cada contingencia.

Así es posible calcular la vulnerabilidad del sistema de potencia, mediante la valoración de la evolución de los parámetros especificados en las ecuaciones [5.18], [5.19] y [5.34].

Otra funcionalidad de la herramienta PSAT es que permite determinar los buses que quedan eléctricamente aislados, es decir, sin conexión alguna al generador de slack. En cada iteración se tiene en cuenta la existencia de estas islas para el cálculo correcto del *índice de conectividad S* en [5.19].

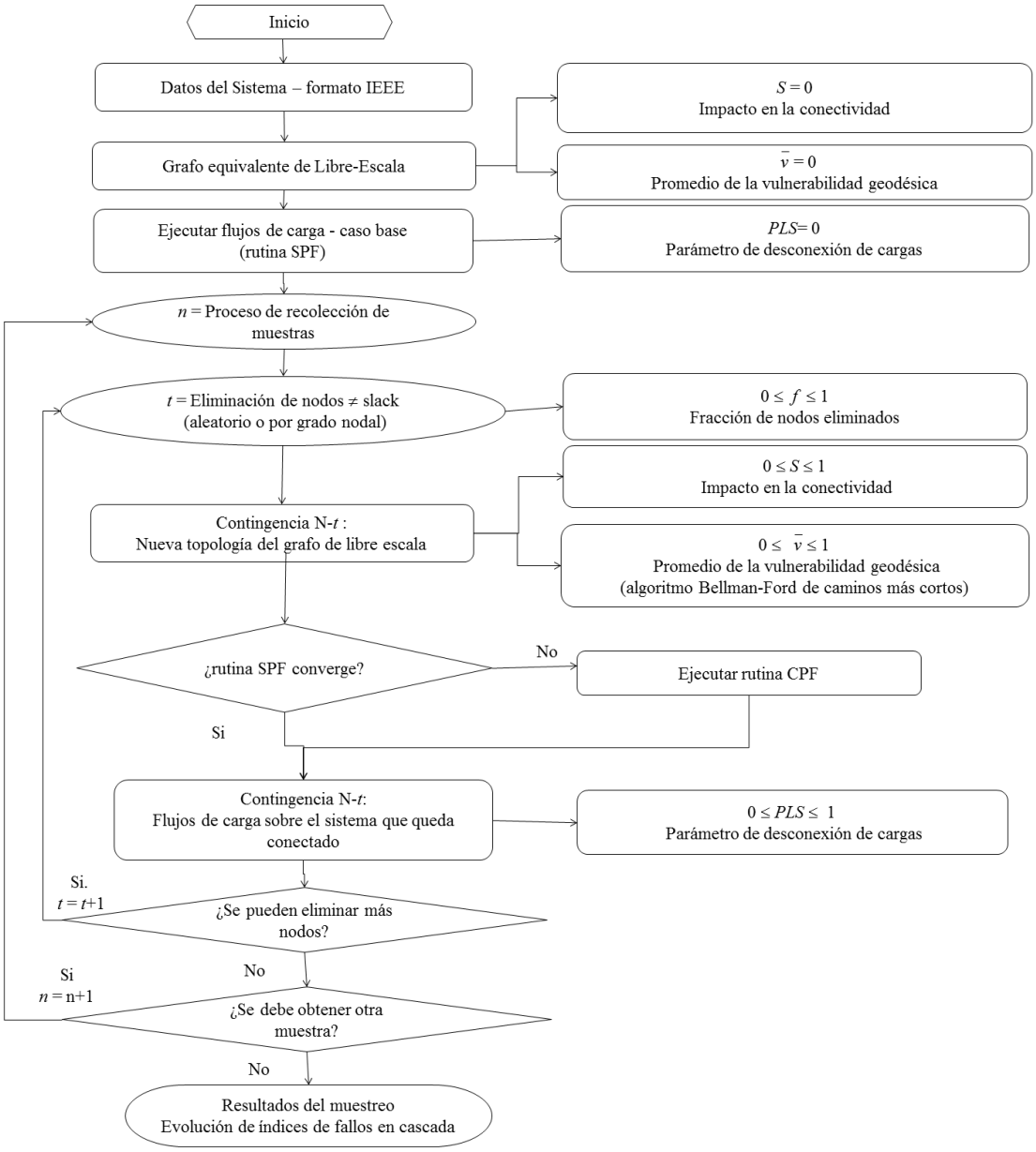


Figura 5.16: Diagrama de flujo del algoritmo para errores aleatorios y ataques deliberados.

El programa finaliza su ejecución después de una determinada cantidad de iteraciones (*t*), debido a que no es posible retirar más nodos del sistema, es decir, todos los nodos quedan aislados, o debido a que no existen circuitos eléctricos que permitan ejecutar más flujos de carga.

El código generado en ***Matlab*** ® para la ejecución del algoritmo descrito en la Figura 5.16 contiene funciones, subrutinas y secuencias de comandos en diferentes archivos, los cuales se extienden en más de 7000 líneas de código fuente, razón por la que no se ha incluido en este documento.

5.3.3 TIEMPO DE COMPUTACIÓN

Uno de los objetivos del análisis de vulnerabilidad consiste en evaluar las condiciones del sistema y realizar un seguimiento a la evolución de sus cambios que generan fallos en cascada. Los escenarios realistas que se han aplicado para probar la utilidad de los modelos de teoría de grafos corresponden a los modelos de prueba IEEE de 14, 24, 30, 57 y 118 buses [IEEE-Group, 1973].

La ejecución del algoritmo se ha realizado en un ordenador personal, con versión *Matlab 7.2* ® y cuyo hardware corresponde a un procesador *Intel Core Duo* de 2.33 GHz, y 2GB de memoria RAM.

La Tabla 5.5 contiene algunas estadísticas relevantes a la simulación de los ataques deliberados y errores aleatorios en redes IEEE. Las iteraciones corresponden a la cantidad de eliminación sucesiva de nodos, es decir, la última contingencia $N-t$ del análisis de fallos en cascada, incluyendo la ejecución del caso base. Obsérvese que el número de iteraciones por cada muestra es mayor en el caso de eliminaciones aleatorias, que las dirigidas deliberadamente a los nodos con mayor grado nodal.

Tabla 5.5: Resumen del proceso iterativo para cálculo de tolerancia errores aleatorios y ataques deliberados en redes IEEE.

Estrategia de Eliminación	Ejecución del Algoritmo	IEEE 14	IEEE 24	IEEE 30	IEEE 57	IEEE 118
Aleatoria (35 muestras)	Nº promedio iteraciones por muestra	33	62	67	120	293
	Tiempo (min)	35’	80’	90’	570’	1140’
Deliberada (1 muestra)	Nº promedio iteraciones por muestra	10	18	26	42	107
	Tiempo (min)	1’	2’	2’	4’	12’

Para evaluar la tolerancia en errores aleatorios se efectúa el promedio de 35 muestras. En cada muestra se efectúa la eliminación aleatoria de un número de nodos de la red, correspondiente a la cantidad de iteraciones que se indica en la Tabla 5.5. El caso de evaluación en ataques aleatorios, sólo requiere eliminar en orden los nodos según su grado nodal. De esta manera, se obtiene una evaluación de todas las

condiciones técnicas que ocurren en el sistema de potencia en durante la evolución de los eventos que desencadenan fallos en cascada.

5.3.4 RESULTADOS DE LAS SIMULACIONES

En las figuras 5.17, 5.19 y 5.21 se observan los resultados tanto de indicadores eléctricos, como medidas estadísticas del grafo equivalente (*PLS* [5.34], *S* [5.19], $\bar{v}$ [5.18]), para una estrategia de **eliminación por errores aleatorios**. Igualmente las figuras 5.18, 5.20 y 5.22 corresponden a la respuesta en una **estrategia de ataques deliberados**.

Estos resultados reflejan la evolución de los índices *PLS* [5.34], *S* [5.19], $\bar{v}$ [5.18] y representan un modelo de los eventos de fallos en cascada por la eliminación sucesiva de nodos de la red. En el eje de las abscisas se muestra la **fracción de nodos eliminados** del sistema (*f*)

5.3.4.1 Índice de Desconexión de Cargas (PLS)

El índice de *Desconexión de Cargas* es apropiado para cuantificar el funcionamiento estructural de la red, ya que muestra el porcentaje de demanda no suministrada en una red particular. En la Figura 5.17 se observa la evolución del indicador para el caso de errores aleatorios. La Figura 5.18 presenta el caso específico de ataques deliberados a la red según el grado nodal. El indicador es igual a uno cuando no se existan cargas conectadas al sistema de potencia (colapso de la red).

Tratándose de una red libre de escala, al eliminar o aislar un nodo aleatoriamente, el efecto es mucho menor que el aislamiento de un vértice de mayor grado nodal. En cada iteración se remueve un nodo, y se calculan sucesivamente los *flujos de carga estándares y continuados* (SPF y CPF). La curva de la Figura 5.17 se obtiene después de promediar 35 muestras. De esta manera, es posible estimar la cantidad de carga conectada en la red en tiempo real.

En la Figura 5.17 se evidencia que la evolución del fallo en cascada hasta ocasionar el colapso del servicio de la red (*blackout*) ocurre cuando se aísla el 20% de los nodos. En este caso, la red de 118 buses es la más vulnerable de todas (colapsa totalmente por la eliminación del 20% de los nodos). Por su parte, en la red de 57 buses, el 90% de la carga del sistema queda desconectada cuando se remueve el 20% de los nodos de la red. En las redes de 14, 24 y 30 buses el aislamiento del 90% de la carga ocurre después de eliminar el 35% de los nodos.

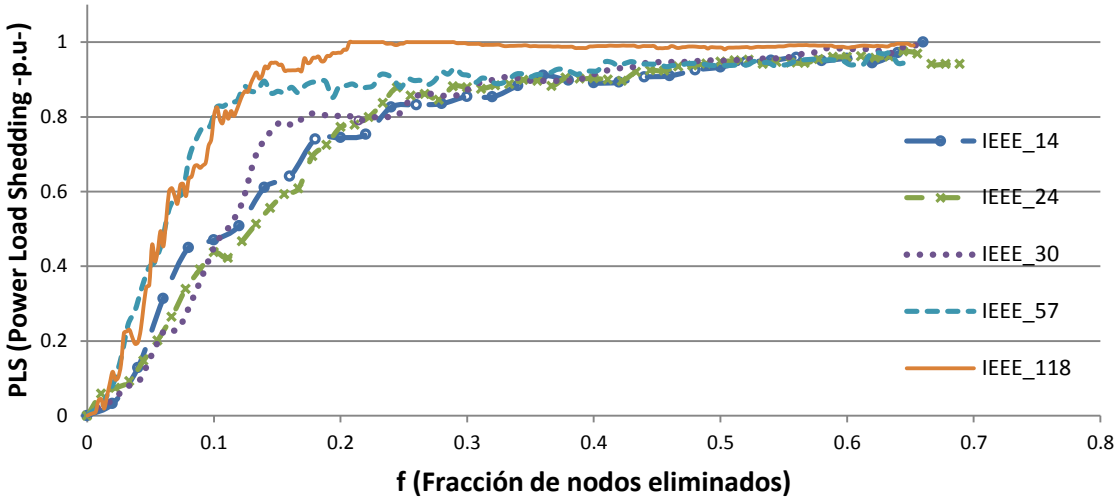


Figura 5.17: Errores aleatorios: *Índice de Desconexión de Cargas (PLS)*

Las curvas de la Figura 5.18 se obtienen por la eliminación de nodos según el grado nodal decreciente de cada vértice de la red. Al observar la evolución del índice *PLS* para ataques deliberados, se deduce que la intervención en sólo el 2% de los nodos genera un *blackout* masivo (redes de 30, 57 y 118 buses). Existe un poco más de robustez en los sistemas de 14 y 24 buses, que colapsan por la eliminación del 5% de sus nodos del sistema.

En consecuencia, las redes más vulnerables a los ataques deliberados en los nodos de mayor grado de conectividad son las redes de 118 buses y de 30 buses (colapsan con aislamiento del 1% de los nodos), mientras que la red de 57 buses colapsa con aislamiento del 2% de los nodos, la red de 24 buses con el aislamiento del 4% de los nodos y la red de 14 buses con el 6% de los nodos.

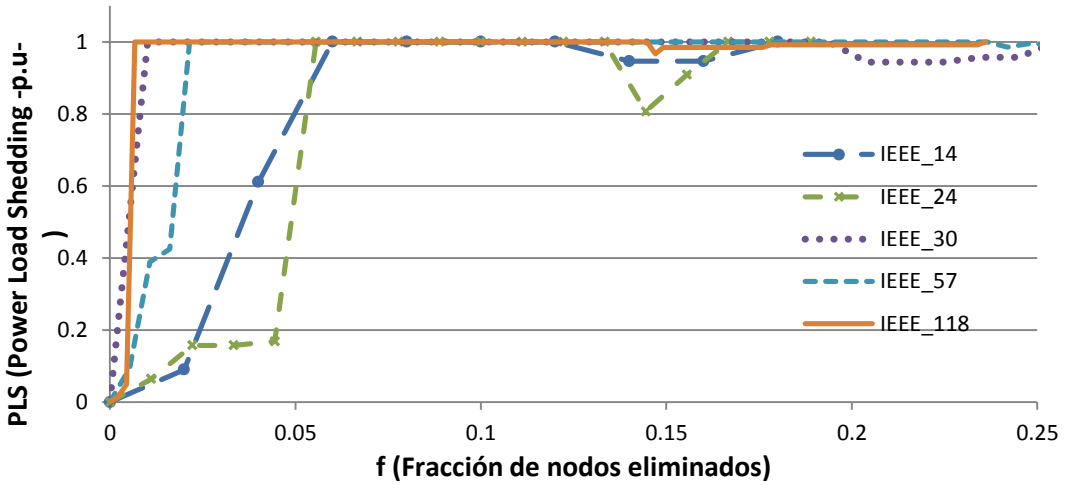


Figura 5.18: Ataques deliberados: *Índice de Desconexión de Cargas (PLS).*

Llama la atención que la evolución en la estructura del sistema genera una leve recuperación de la carga cuando se eliminan cerca del 15% de los nodos (Figura 5.18). Esto puede explicarse dado que, en estos casos particulares, queda conectado eléctricamente un circuito alrededor del generador de slack, que permite la circulación de flujos de potencia, pero una nueva iteración de estos fallos en cascada ocasiona un nuevo colapso en la red.

5.3.4.2 Índice de Impacto en la Conectividad (S)

El índice de impacto en la conectividad es quizás el más citado en toda la literatura de redes complejas para analizar la tolerancia a los ataques y a los errores en los grafos. El índice *S* tiende a un valor de uno cuando se desintegra totalmente la conectividad de la red. Las figuras 5.19 y 5.20 permiten apreciar la evolución del tamaño relativo de la red que queda conectada alrededor del *generador slack*.

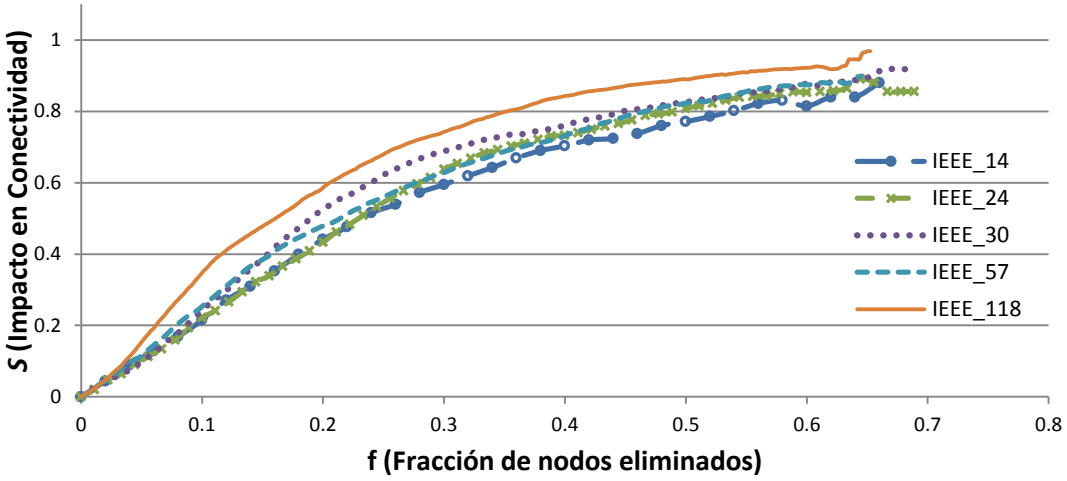


Figura 5.19: Errores aleatorios: *Índice de Impacto en la Conectividad (S).*

Una comparación entre las figuras 5.17 y 5.19 (errores aleatorios) muestran que *la conectividad de la red* evoluciona de manera diferente que los indicadores eléctricos del sistema de potencia.

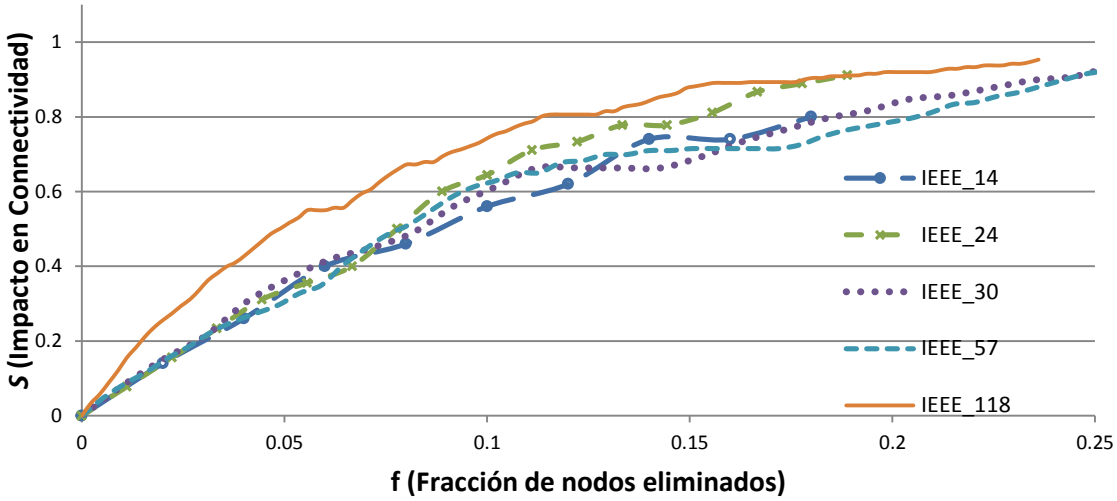


Figura 5.20: Ataques deliberados: *Índice de Impacto en la Conectividad (S).*

La conectividad nodal, no está relacionada proporcionalmente con la conectividad eléctrica, es decir, la tendencia del *PLS* es diferente a la del índice *S*. La misma deducción se aplica a la comparación en el caso de ataques deliberados (Figura 5.18 vs 5.20). Esto es debido a que no existe una relación proporcional entre la evolución del índice y los flujos eléctricos. Tampoco se puede deducir qué red es más vulnerable (sólo se evidencia una coincidencia en la red de 118 buses).

A diferencia de las simulaciones de ataques deliberados, en el caso de los fallos por errores aleatorios la desintegración de la red es más gradual y se evidencia la total desintegración cuando se eliminan más del 70% de los nodos.

5.3.4.3 Vulnerabilidad Geodésica ($\bar{v}$)

A diferencia de la *distancia geodésica* $\bar{d}$ [5.13], el índice de ***vulnerabilidad geodésica media*** $\bar{v}$ [5.18], que es una medida relacionada directamente con la *eficiencia geodésica* (ecuación [5.17]), demuestra ser un indicador bien definido, a la vez que facilita la comparación de los resultados entre indicadores eléctricos y topológicos.

La evolución de la *vulnerabilidad geodésica* para fallos en cascada en redes IEEE se puede observar en las figuras 5.21 y 5.22. En general, se aprecia que la clasificación de las redes más vulnerables coincide con la respuesta obtenida en el índice *PLS.*

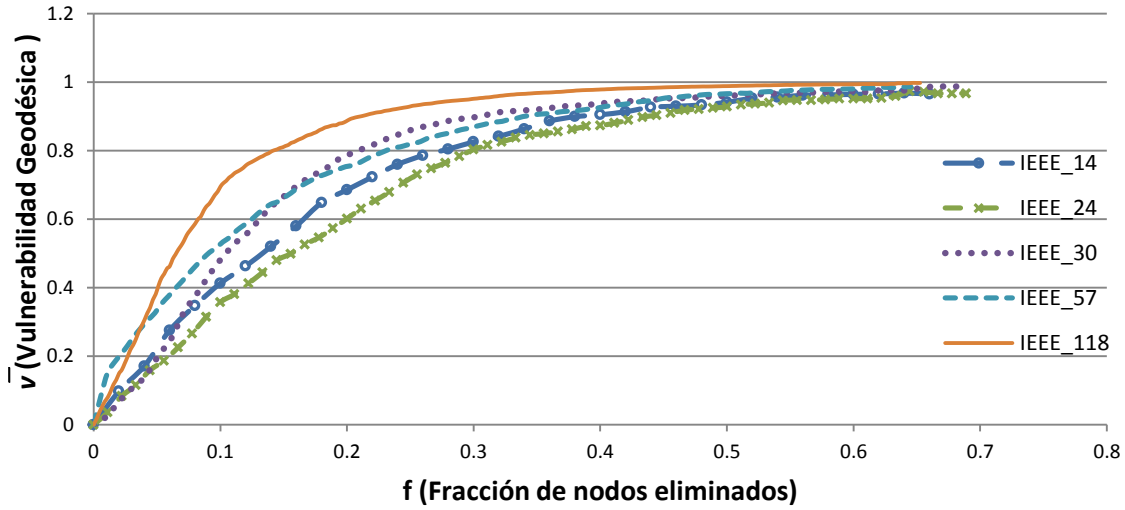


Figura 5.21: Errores aleatorios: *Índice de Vulnerabilidad Geodésica* ($\bar{v}$).

Al comparar el índice *PLS* y el índice $\bar{v}$ en los eventos de errores aleatorios (Figura 5.17 vs Figura 5.21) se verifica que la red de 118 buses es la más vulnerable de todas, seguida por la de 57, 30, 24 y 14 buses; esto coincide completamente con el pronóstico de las desconexiones del índice *PLS*. Resultados similares se obtienen para el caso de ataques deliberados en la red (Figura 5.18 vs Figura 5.22). Por esta razón, se infiere la existencia de un grado de correlación entre ambos indicadores.

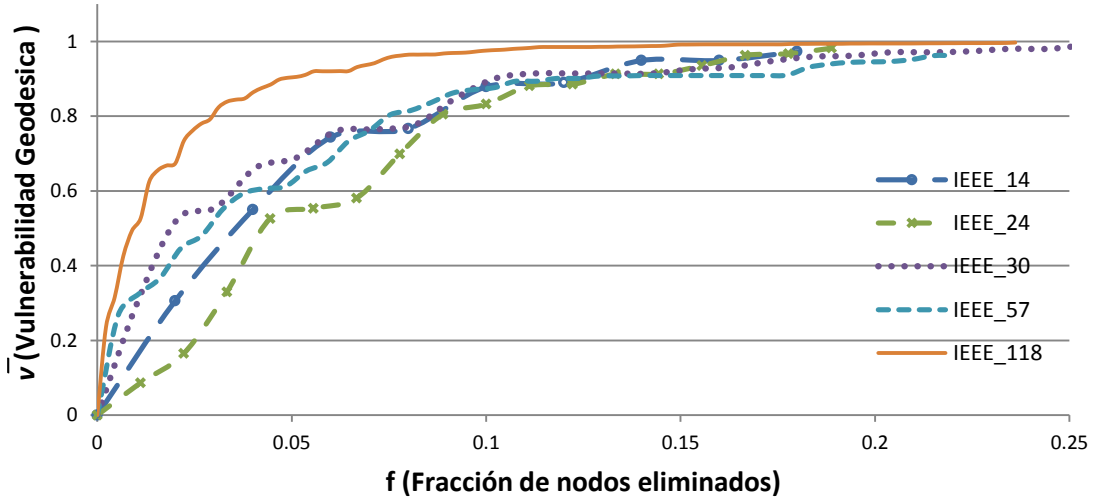


Figura 5.22: Ataques deliberados: *Índice de Vulnerabilidad Geodésica* ($\bar{v}$).

Cuando el índice de *vulnerabilidad geodésica* tiene un valor cercano a uno, implica una mayor fragmentación de la red, y en consecuencia los flujos entre generadores y cargas deben pasar a través de más rutas, lo cual implica una menor resiliencia y menor robustez. Esto es consistente con el aislamiento de cargas y de usuarios en los eventos que desencadenan los fallos en cascada.

5.3.5 EFECTIVIDAD DE LA EVALUACIÓN DE VULNERABILIDAD ESTRUCTURAL

Aunque el uso de la teoría de grafos es insuficiente para determinar la capacidad de transferencia de potencia entre generadores y cargas, la metodología presentada permite comprender los mecanismos generales de cómo funcionan las redes complejas.

Una medida práctica para determinar la dependencia entre el índice eléctrico *PLS* y la teoría de grafos (*S*, $\bar{v}$) es mediante el *coeficiente de correlación de Pearson* ρ, el cual se obtiene mediante el cociente entre la covarianza de dos variables y el producto de sus desviaciones estándar σ, según la formulación en [5.35]

$$\rho_1 = \frac{\mathrm{cov}(PLS, S)}{\sigma_{PLS}\sigma_S} \;;\; \rho_2 = \frac{\mathrm{cov}(PLS, v)}{\sigma_{PLS}\sigma_v} \qquad [5.35]$$

ρ_1 : Coeficiente de correlación entre el índice *PLS* y el indicador de impacto en la conectividad del grafo de libre-escala *S*.

ρ_2 : Coeficiente de correlación entre el índice *PLS* y la vulnerabilidad geodésica del grafo de libre-escala $\bar{v}$.

La Tabla 5.6 presenta los resultados de la correlación entre los diferentes índices. Este coeficiente de correlación confirma la comparación entre las tendencias de los resultados presentados entre las figuras 5.17 vs 5.21 y las figuras 5.18 vs 5.22.

Tabla 5.6: Correlación de Pearson entre índice *PLS* y medidas de teoría de grafos *S*, $\bar{v}$.

Estrategia de eliminación	Red de prueba IEEE	ρ_1	ρ_2
Errores aleatorios	14 buses	0.9485	0.9903
Errores aleatorios	24 buses	0.9532	0.9826
Errores aleatorios	30 buses	0.9503	0.9920
Errores aleatorios	57 buses	0.8047	0.9099
Errores aleatorios	118 buses	0.8584	0.9828
Ataques deliberados	14 buses	0.8566	0.9491
Ataques deliberados	24 buses	0.8268	0.8780
Ataques deliberados	30 buses	0.3941	0.6586
Ataques deliberados	57 buses	0.6266	0.7897
Ataques deliberados	118 buses	0.4264	0.7321

Para el caso de la estrategia de eliminación de nodos por errores aleatorios, el coeficiente de correlación ρ_2 es cercano a +1, lo cual implica una relación lineal positiva entre el índice *PLS* y la vulnerabilidad geodésica $\bar{v}$. De acuerdo con esta

comparación el índice $\bar{v}$ es muy útil para determinar la proporción de carga desconectada P_{Di} del sistema de potencia en los eventos de fallos en cascada.

Sin embargo, una comparación sobre el índice de impacto en la conectividad *S*, correspondiente al coeficiente ρ_1, deja en evidencia que la evolución de dicho índice es diferente a la del índice *PLS*. En consecuencia, no debería ser considerado como un indicador preciso para evaluar la vulnerabilidad de la red.

En el caso de ataques deliberados, el coeficiente de correlación ρ_2 (índice $\bar{v}$) es más débil que el coeficiente ρ_1 (indicador *S*). Por tanto, la vulnerabilidad geodésica $\bar{v}$ es de gran interés para realizar comparaciones entre diferentes sistemas de potencia, y determinar cuál es más vulnerable.

Como resultado de la confirmación de correlación entre la *vulnerabilidad geodésica* $\bar{v}$ y la *desconexión de carga eléctrica PLS*, se ha validado por primera vez en el ámbito investigador la utilidad de combinar las metodologías de sistemas eléctricos de potencia y teoría de grafos, para el estudio de fallos en cascada.

5.4 COMENTARIOS AL CAPÍTULO

La falta de estudios de validación que permitan corroborar la efectividad de las respuestas de los modelos de teoría de grafos y las técnicas tradicionales de flujos de carga en AC, constituyeron la motivación para abordar esta parte del trabajo de investigación. Se ha confirmado la utilidad de las técnicas de teoría de grafos para analizar las respuestas de los sistemas eléctricos de potencia. Dentro de los enfoques estudiados para determinar la vulnerabilidad de las redes de transporte, se ha evaluado la tolerancia de las redes de prueba IEEE tanto a los errores aleatorios, como a los ataques deliberados.

Con la propuesta metodológica es posible asociar índices numéricos (*PLS*, *S*, $\bar{v}$) de la teoría de grafos y de las técnicas de flujos de carga para evaluar la vulnerabilidad de cualquier sistema de potencia. Se ha demostrado la utilidad de combinar modelos de flujos de carga y medidas de grafos de libre-escala. También se ha validado dicha correlación numérica y gráficamente. De esta manera, es posible sustituir herramientas de alto coste computacional (rutinas de flujos de carga) con técnicas más eficientes (medidas estadísticas de teoría de grafos), con la finalidad de evaluar la vulnerabilidad estructural de una red, en función de los eventos que pueden desencadenar fallos en cascada.

6 ESTUDIO DE CASO EN REDES DE TRANSPORTE

Como aplicación de la metodología desarrollada en el capítulo 5, se plantea evaluar la vulnerabilidad de algunas redes de transporte en alta tensión, según la topología real en infraestructuras de países como Colombia y España. Se medirá la efectividad de los planes de expansión, entendiéndose como la construcción y puesta en marcha de nuevos activos dentro de los sistemas de infraestructura, que finalmente deben reforzar la robustez de la red de potencia o permitir la instalación de nuevos buses como consecuencia del crecimiento requerido por la infraestructura.

De esta manera, se expone una metodología de evaluación cuantitativa de la vulnerabilidad de redes eléctricas, que permitirá determinar el impacto de las inversiones para cumplir los horizontes de planificación de expansión de las redes o para mejorar la robustez del sistema.

6.1 OBJETIVO DEL CAPÍTULO

En este capítulo se desarrolla una aplicación de la metodología propuesta en el capítulo 5 para evaluar la vulnerabilidad de los sistemas de transporte en alta tensión en países como Colombia o España, caracterizando el modelo de libre escala y simulando su comportamiento según la tolerancia a errores aleatorios y ataques deliberados, a partir de información básica sobre la topología de la red.

En esta sección se aplica el algoritmo diseñado previamente en el apartado 5.3.2 modelando los sistemas interconectados como una red compleja (tanto en Colombia como en España), sometiendo la topología de las redes a fallos en cascada y analizando la robustez de los respectivos planes de expansión en las redes eléctricas de ambos países. Esta aplicación involucra a los nodos (subestaciones, torres eléctricas, transformadores, puntos de conexión, etc) y enlaces (líneas aéreas, líneas subterráneas, etc), sin tener en cuenta las distancias físicas que existen, ni los parámetros eléctricos de los mismos (impedancias de las líneas, regulación de tensión, perdidas de energía, etc.). En consecuencia, en este capítulo se desarrollan los siguientes aspectos con el objetivo de evaluar la vulnerabilidad de las redes:

- Utilización de la topología de red para describir la respuesta ante eventos de fallos en cascada en redes de transporte de países como Colombia y España, según los indicadores formulados en el capítulo 5.
- Evaluación de la vulnerabilidad de los sistemas actuales y comparación frente a la planificación de la expansión de la infraestructura de transporte eléctrico.

De esta manera se demuestra la utilidad de los modelos fundamentados en grafos de libre escala como una técnica eficiente para evaluar la vulnerabilidad estructural de las infraestructuras eléctricas en dos países diferentes, así como la efectividad de los planes indicativos gubernamentales para expandir las redes.

6.2 PROCEDIMIENTO DE EVALUACIÓN DE VULNERABILIDAD ESTRUCTURAL EN LA RED DE TRANSPORTE

La metodología desarrollada en el capítulo 5 tiene aplicabilidad en escenarios que requieran cuantificar la vulnerabilidad estructural de redes de alta tensión y comparar los resultados entre sí, tal y como se requiere en las etapas de evaluación de los PIC. Una aplicación práctica de la metodología se lleva a cabo en redes de 400kV en España y en redes de 220kV y 500kV en Colombia incluyendo el análisis de los respectivos planes indicativos de expansión publicados por los ministerios

encargados de dicha planificación. Se pretende aportar una visión más técnica que permita cuantificar de manera más precisa los efectos de los riesgos sobre las redes de transporte en alta tensión. De esta manera, será posible aplicar medidas en aspectos como la planificación, la gestión y la operación de sistemas de potencia, con el objetivo de minimizar los efectos asociados a los riesgos y amenazas de tipo técnico y no-técnico, su frecuencia y su duración.

En la Figura 6.1 se presenta el algoritmo que permite calcular la vulnerabilidad geodésica $\bar{v}$, partiendo de la topología del sistema, en función de la cantidad de nodos aislados *f*. Obsérvese que la base para la generación de esta metodología corresponde a la propuesta construida previamente en la sección 5.3.

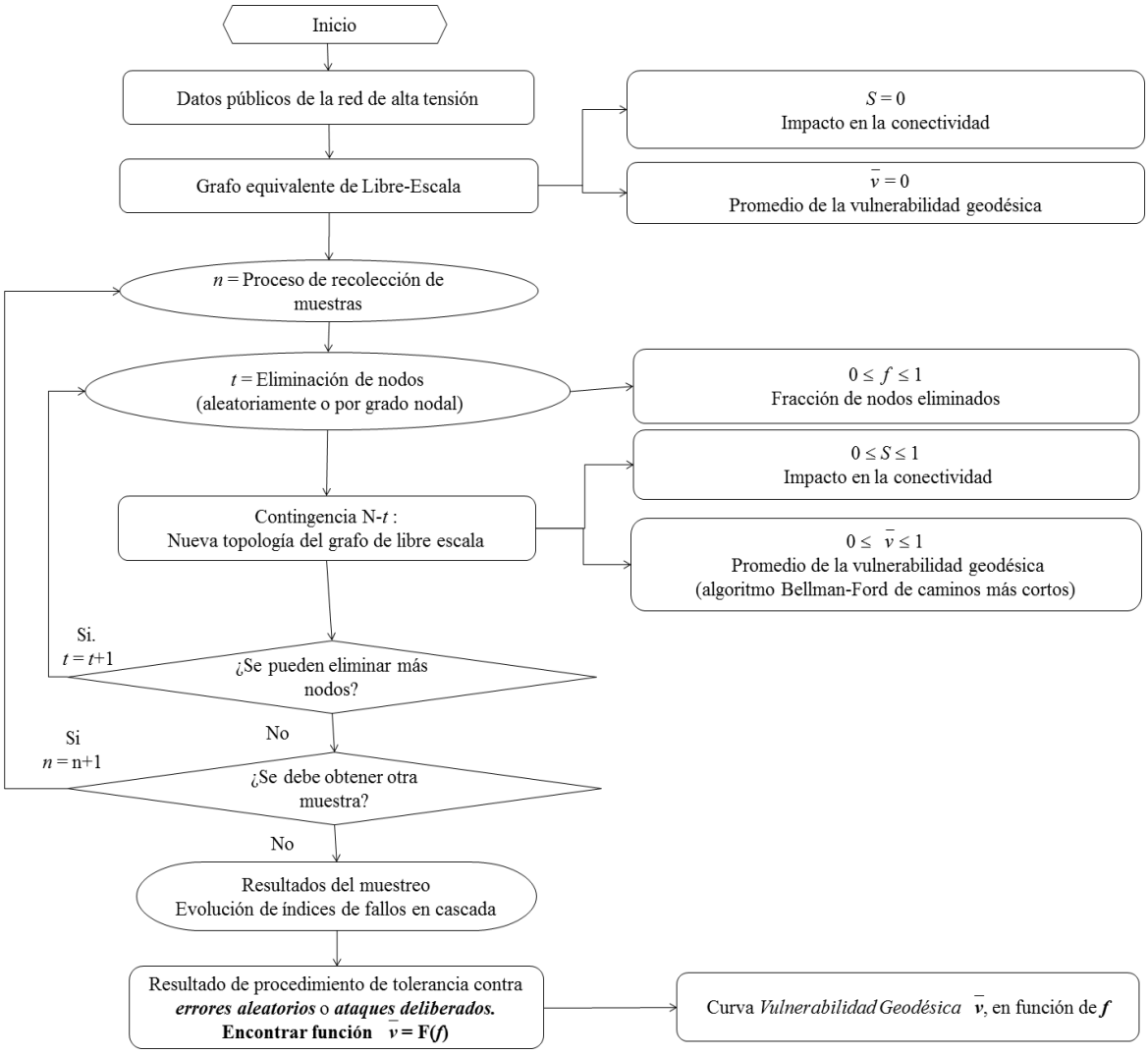


Figura 6.1: Diagrama de flujo para calcular la vulnerabilidad estructural en redes de alta tensión

Una observación importante respecto a la ejecución del procedimiento presentado en la Figura 6.1 tiene que ver con que no es necesario incluir toda la información de parámetros eléctricos de las redes bajo análisis. Por lo tanto, la metodología que se aplica constituye una ventaja, dado que aunque mayor parte de la información relacionada con la topología de las redes es pública, no existe disponibilidad de los datos eléctricos de las mismas.

Los eventos de eliminación de fallos en cascada se determinan de acuerdo a la estrategia de eliminación de nodos. Para tomar una muestra, se realizan iteraciones sucesivas de contingencias N−1, sobre una red que cambia constantemente su estructura con la eliminación de cada nodo. No se necesita ejecutar flujos de carga, sino que sólo se requiere calcular los parámetros asociados a la red compleja (teoría de grafos), lo cual permite reducir el tiempo de computación y de esta manera, efectuar el análisis comparado de vulnerabilidad entre infraestructuras eléctricas de transporte.

Los estudios de vulnerabilidad estructural que se presentan en las secciones subsiguientes incluyen el análisis de tolerancia de la red frente a errores aleatorios, en cuyo caso se presenta el promedio de 35 muestras para describir el índice de fallos en cascada. La selección del número de muestras tiene en cuenta la recomendación del *teorema central del límite*, el cual sugiere tomar más de 30 muestras para realizar un adecuado tratamiento estadístico. Cada **muestra** contiene el conjunto de resultados obtenidos en la ejecución del algoritmo de la Figura 6.1 por la ejecución sucesiva de contingencias N−1. Por su parte, el análisis de tolerancia frente a ataques deliberados se especifica únicamente por la ejecución del algoritmo mediante eliminación de los buses con mayor grado nodal.

El algoritmo de la Figura 6.1 se ha implementado en lenguaje ***Matlab*** ®, utilizando funciones de la herramienta ***MatlabBGL*** para teoría de grafos [GLEICH, 2008], que entre otras, incluye diferentes rutinas para el cálculo de distancias geodésicas (en este programa en particular, se emplea el *algoritmo Bellman-Ford para cálculo de distancias más cortas* [GROSS & YELLEN, 2004]) tal y como se explicó previamente en la sección 5.2.1.

6.3 TOPOLOGÍA DE CASOS DE ESTUDIO EN SISTEMAS DE TRANSPORTE ALTA TENSIÓN

En esta sección se realiza una breve descripción de la topología de algunos sistemas de alta tensión, así como el impacto sobre su robustez. El estudio se aplica en un sistema de infraestructura que comprende el conjunto de líneas, módulos de

conexión y demás activos que operan a tensiones de 220 kV y 500 kV para el caso de Colombia y 400 kV para el caso de España. La topología de la red se obtiene a partir de información pública, como la presentada en Figura 2.3, Figura 6.2 y Figura 6.4.

Para el caso de estudio de la vulnerabilidad de redes de transporte se pretende representar inicialmente la aproximación del sistema de potencia como una red de libre escala, según la propuesta formulada en 5.2.2.1. La vulnerabilidad estructural del sistema de transporte se evalúa de acuerdo a las condiciones actuales del sistema, y de acuerdo a la posible ejecución de los planes gubernamentales de expansión y desarrollo en España y en Colombia. Básicamente, se consideran los siguientes tres casos de estudio

Caso 1: Evaluación de vulnerabilidad sobre el caso base, o estado actual de la red.

Caso 2: Evaluación de vulnerabilidad sobre los planes de mejora de robustez de la red actual, según se estipula en los planes de desarrollo de las redes de transporte. Sólo se considera el efecto de construir nuevas líneas de transporte, sin adicionar nuevas subestaciones.

Caso 3: Evaluación de vulnerabilidad sobre los planes de expansión de la red actual, según se estipula en los horizontes de planificación de las redes de transporte. En este caso se considera el efecto de construir nuevas líneas de transporte, así como la adición de nuevas subestaciones en la red eléctrica.

6.3.1 RED DE TRANSPORTE 400kV EN ESPAÑA

El sistema interconectado de España está compuesto por más de 40.000 kilómetros de líneas de alta tensión, más de 4.000 posiciones de subestaciones y cerca de 75.000 MVA de capacidad de transformación [REE, 2012a]. Los activos que gestiona la empresa *Red Eléctrica de España*, responsable de la operación y mantenimiento de la red de transporte en alta tensión, tanto dentro de la península ibérica, como en los archipiélagos baleares y canarios, supone la consolidación definitiva del modelo de transportista único y operador del sistema eléctrico en toda España.

6.3.1.1 Caso 1: Condición actual de la Red de Transporte a 400kV

La Figura 6.2 permite apreciar la red de alta tensión en la península española incluyendo la planificación indicativa de expansión [REE, 2012b]. Los trazos con líneas grises representan las redes eléctricas del circuito a 400kV existentes al año 2012, las

cuales constituyen el objetivo del análisis en esta sección. El análisis de la expansión para los años 2014 y 2016, identificada con trazos verdes y rojos, se presentará en las subsiguientes secciones.

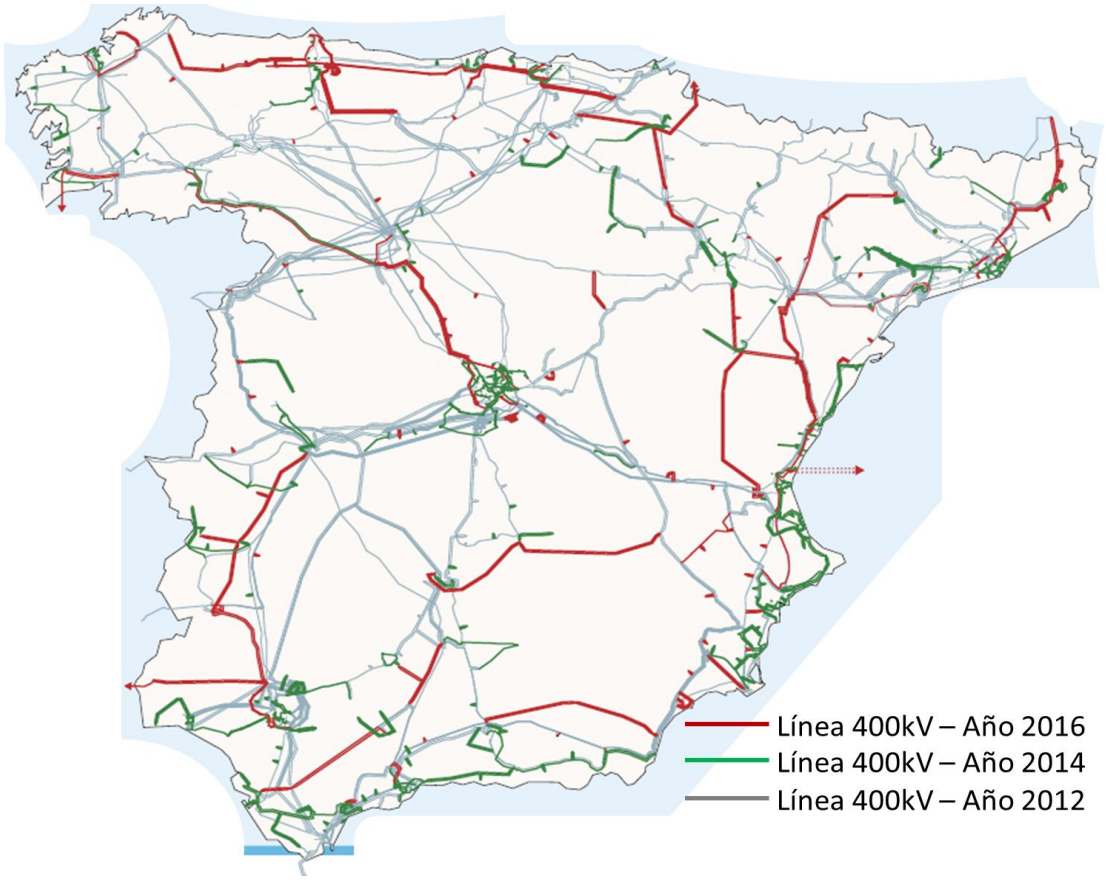


Figura 6.2: Representación de la red peninsular de alta tensión 400kV en España [REE, 2012b]

La representación de la Figura 6.2 no incluye los sistemas insulares de las islas canarias, ni las islas baleares, cuyas líneas corresponden a tensiones inferiores a 220kV. La Tabla 6.1 presenta un resumen de la totalidad de activos que componen la infraestructura eléctrica de transporte en alta tensión en España [REE, 2012a].

Tabla 6.1: Características de la Red de Transporte Peninsular y Extra-Peninsular de España, actualizada al año 2011

Red de transporte	Km de circuito	Posiciones de subestaciones
400 kV	19.622	1.241
220 kV	18.218	2.820
150-132 kV	295	52
<132 kV	1.998	741
Total	40.133	4.854

Aunque es posible acceder a información pública sobre la topología de la red de alta tensión en España, como aquella contenida en los mapas de las redes [REE, 2012b] donde se incluye un esquema de la mayor parte de los activos, para el propósito de esta sección y como ilustración del ejemplo de aplicación de la metodología se propone enfocar el trabajo en la red de 400 kV, incluyendo aquellas subestaciones determinadas como más importantes y estratégicas.

Esta información, tomada de [BESCANSA, 2007] se representa en el grafo de libre escala en la Figura 6.3 compuesto por 48 subestaciones y 70 líneas de transporte (conjunto torre + cable) que interconectan las subestaciones.

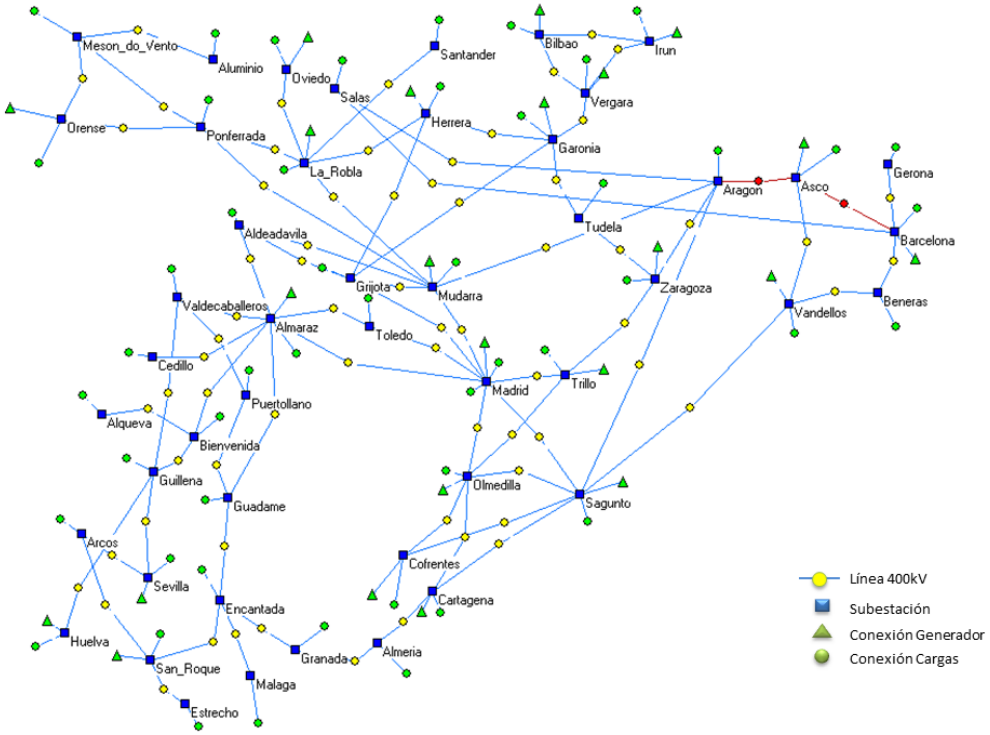


Figura 6.3: Grafo de Libre Escala representativo de la red de transporte peninsular en alta tensión a 400kV

La Tabla 6.2 contiene el conjunto de subestaciones que permiten representar la topología del sistema [BESCANSA, 2007]. En la Figura 6.3 se han indicado los diferentes puntos de conexión a otras cargas, así como generadores que inyectan potencia activa en la red. Para estudiar la *vulnerabilidad geodésica* de la red ($\bar{v}$) no son necesarios los parámetros eléctricos de carga, generación, ni los parámetros de líneas (resistencia, reactancia). No obstante, como información, se ha indicado la cantidad aproximada de carga y de generación que converge en cada bus. La tensión base es de 400kV y la potencia base es de 1000MVA.

Tabla 6.2: Conjunto de subestaciones a 400kV consideradas en el modelo topológico

Nº BUS	NOMBRE	CARGA -P.U-	GENERACIÓN -P.U-
1	Aldeadavila	0.25	0
2	Almaraz	0.09	1.9
3	Almería	0.4	0
4	Alqueva	0.09	0
5	Aluminio	0.7	0
6	Aragón	0.6	0
7	Arcos	0.4	0
8	Asco	0.9	2
9	Barcelona	0.9	1.1
10	Beneras	0.9	0
11	Bienvenida	0.09	0
12	Bilbao	1.5	0.5
13	Cartagena	0.9	0.9
14	Cedillo	0.09	0
15	Cofrentes	1.9	1
16	Encantada	0.4	0
17	Estrecho	0.4	0
18	Garoña	0.25	0.4
19	Gerona	0.9	0
20	Granada	0.4	0
21	Grijota	0.25	0
22	Guadame	0.4	0
23	Guillena	0.4	0
24	Herrera	0.25	0.6

Nº BUS	NOMBRE	CARGA -P.U-	GENERACIÓN -P.U-
25	Huelva	0.4	1
26	Irún	1.5	0.2
27	La_Robla	0.25	0.5
28	Madrid	4	0.5
29	Málaga	0.4	0
30	Meson_do_Vento	0.7	0
31	Mudarra	0.25	0.5
32	Olmedilla	0.35	1
33	Orense	0.7	1.7
34	Oviedo	1.6	1.2
35	Ponferrada	0.25	0
36	Puertollano	0.35	0
37	Sagunto	1.9	1.9
38	Salas	0.9	0
39	San_Roque	0.4	0.2
40	Santander	0.7	0
41	Sevilla	0.4	1.2
42	Toledo	0.35	0
43	Trillo	0.35	1
44	Tudela	0.65	0
45	Valdecaballeros	0.09	0
46	Vandellos	0.9	1
47	Vergara	1.5	0.5
48	Zaragoza	0.6	1.3

En conclusión, para el **caso 1** se pretende realizar el estudio de vulnerabilidad de una red de 48 buses a 400kV, cuyos enlaces se presentan en la Figura 6.3.

6.3.1.2 Caso 2: Mejora en la Robustez de la Red Española 400kV

Con el objetivo de mejorar la ***vulnerabilidad*** de la red original (caso 1), los planes gubernamentales sugieren realizar inversiones en una estrategia de mayor robustez de la infraestructura. En España los documentos de planificación del sector eléctrico en los sectores de generación y transporte son emitidos por el Ministerio de Industria, Comercio y Turismo.

En el documento de planificación para el periodo 2008-2016 [MINETUR, 2008], en lo que tiene que ver con la expansión de la red de 400kV, se propone consolidar el mallado de la red entre aquellas subestaciones más cercanas. De esta manera, se busca garantizar el despacho de la energía generada en los parques

eólicos que se construyen en las diferentes comunidades autónomas, y aumentar la fiabilidad del sistema.

Las modificaciones que se toman en esta aplicación se relacionan con las siguientes inversiones [MINETUR, 2008]:

- Anillo de 400 kV alrededor de Sevilla.
- Anillo de 400 kV en la costa de Levante.
- Conexión de circuito de 400 kV entre subestaciones en Asturias.
- Conexión de circuito de 400 kV entre subestaciones en la Coruña.

El programa de planificación indicativa del ministerio incluye muchísimos otros planes, relacionados con las redes de 220kV, construcción de nuevas subestaciones a 400kV y a 220kV, instalación de nuevos transformadores. Sin embargo, para efectos de aplicación de la propuesta metodológica, nos concentramos en estudiar la decisión de aumentar el mallado en la red, sin adicionar nuevos buses.

En resumen, para este **caso 2**, se realizará análisis de vulnerabilidad sobre la misma red de 48 buses, pero con los enlaces adicionales descritos en esta sección.

6.3.1.3 Caso 3: Planificación de la Expansión de la Red Española de 400kV

En los planes de expansión previstos en [MINETUR, 2008] la cobertura eléctrica se analiza bajo las condiciones e hipótesis de crecimiento de la demanda y desarrollo del parque generador, tanto en régimen ordinario como en régimen especial. Al realizar planificación para expandir la red de transporte en alta tensión se hace especial énfasis en conectar los nuevos desarrollos de parques de generación eólicos, así como las nuevas centrales de gas, en un horizonte al año 2016. La conexión de grandes cargas, como los trenes de alta velocidad, constituye uno de los puntos que se tienen en cuenta en la proyección de las nuevas líneas eléctricas en el país.

La representación establecida anteriormente en la Figura 6.2 constituye un resumen de la construcción de nuevas líneas de transporte en 400kV. De acuerdo con el documento gubernamental [MINETUR, 2008], se ha propuesto instalar nuevas subestaciones en el periodo 2011-2016 de acuerdo en las ubicaciones geográficas anotadas en la Tabla 6.3.

Tabla 6.3: Plan de expansión de nuevas subestaciones de 400kV en España

N° BUS	NOMBRE	PROVINCIA	N° BUS	NOMBRE	PROVINCIA
49	Puebla de Guzmán	Huelva	63	Almazan	Soria
50	Balboa	León	64	Velilla	Valladolid
51	San Serván	Badajoz	65	Penagos	Cantabria
52	Pazosborben	Pontevedra	66	Mondragón	Guipúzcoa
53	Cartelle	Orense	67	Magallón	Zaragoza
54	Cornido	La Coruña	68	Castejón	Navarra
55	Trives	La Coruña	69	Muruarte	Navarra
56	Tordesillas	Valladolid	70	Turis	Valencia
57	Otero	Cantabria	71	Mezquita	Orense
58	Cartuja	Cádiz	72	Fuendetodos	Zaragoza
59	Rodandal	León	73	Pallars	Lérida
60	Manzanares	Ciudad Real	74	Els Aubals	Tarragona
61	Romica	Albacete	75	Baixas	Tarragona
62	Medinaceli	Soria	76	Bescano	Girona

En resumen, para este **caso 3**, se realizará análisis de vulnerabilidad sobre una nueva red de 76 buses a 400kV, que se ha modificado a partir del caso 1, pero con nuevos buses y nuevos enlaces, según se definen en el plan de expansión de [MINETUR, 2008].

6.3.2 RED DE TRANSPORTE A 220kV Y 500kV EN COLOMBIA

A diferencia de lo que ocurre en los países de la Unión Europea, donde prácticamente el 100% del territorio de cada país está conectado a la red de suministro centralizado, en Colombia el 75% del territorio no está conectado a la red nacional de transporte. Este amplio territorio comprende regiones declaradas reservas ecológicas y medioambientales con protección especial (selva Amazónica, selvas del Caguán, selvas del Pacífico, selvas del Darién, altillanura de la Orinoquía, zonas desérticas en el norte y centro del país, así como reservas ecológicas en páramos y nevados), que a su vez son regiones con muy baja densidad poblacional. Las islas en el Caribe y en el Pacífico tampoco están conectadas a la red. [1]

[1] Aunque el suministro eléctrico en esas regiones se efectúa mediante generación descentralizada con tecnologías híbridas, aún existen grandes retos para garantizar el suministro eléctrico para la población en esas zonas no interconectadas, con un servicio de electricidad sostenible y confiable. Para mayor información sobre el acceso a la energía eléctrica en las zonas no interconectadas de Colombia, se recomienda la referencia bibliográfica [PEREZ BEDOYA, 2010].

6.3.2.1 Caso 1: Condición actual de la Red de Transporte a 220kV y 500kV

La red de transporte de alta tensión en Colombia se extiende principalmente a través de la región de las cordilleras andinas, así como en la región de la costa Caribe y los grandes núcleos urbanos sobre las costas del océano Pacífico, correspondientes a los territorios donde se concentra la mayor parte de la población y la vida económica del país, según se muestra en la Figura 6.4. [UPME, 2012]

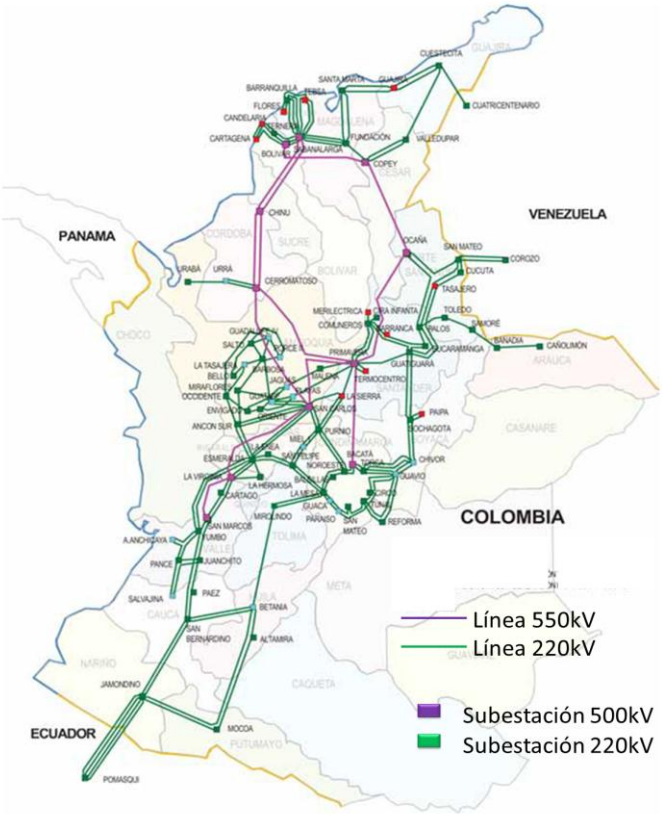


Figura 6.4: Redes de transporte 220kV y 500kV en Zonas Interconectadas de Colombia [UPME, 2012]

La capacidad efectiva neta instalada en el sistema interconectado colombiano al finalizar el año 2011 fue 14420 MW, de los cuales 9200MW (64%) provienen de generación hidroeléctrica [XM, 2012]. La mayor parte de las centrales hidroeléctricas se ubican en la cordillera andina, desde donde se atienden las necesidades de consumo de las regiones interconectadas. Las centrales de generación térmica (gas y carbón), en su mayoría están ubicadas en la región caribe y en el altiplano cundi-boyacense, donde existe disponibilidad de combustibles de gas y carbón para la operación de estas centrales.

La topología de la red de alta tensión en Colombia es información usualmente clasificada como de seguridad nacional. Sin embargo, para efectos académicos, es

posible encontrar datos de trabajos previos [BUITRAGO & TAUTA, 2008] y en informes gubernamentales colombianos [UPME, 2012] para obtener un mapa de la topología de la red, según se muestra en la Figura 6.5.

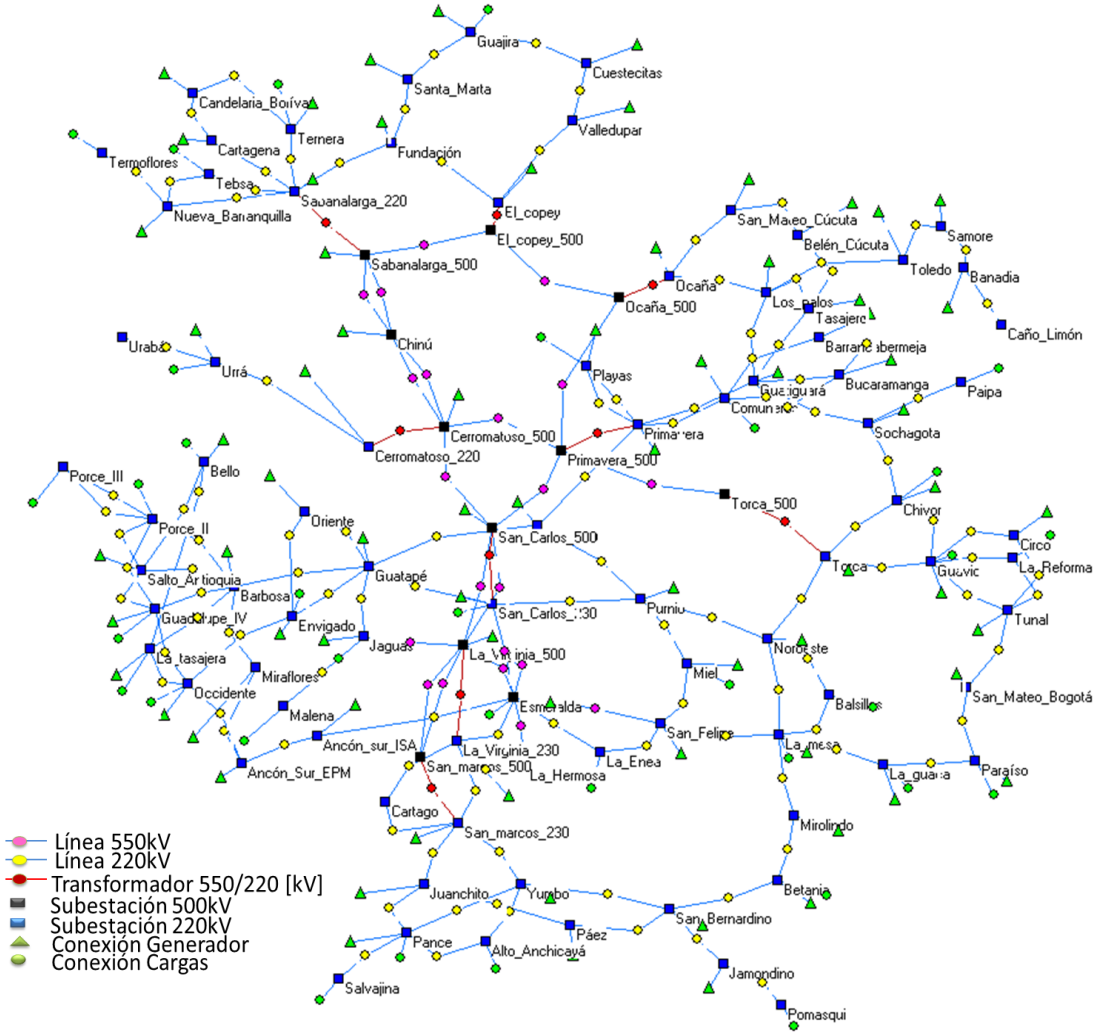


Figura 6.5: Grafo de Libre Escala representativo de la red de transporte colombiana en alta tensión a 220kV y 500kV

Los activos del sistema interconectado nacional los gestiona la *empresa ISA (Interconexión Eléctrica S.A)*, responsable de la operación y mantenimiento de la red de transporte en alta tensión en las zonas interconectadas de Colombia[2].

La Tabla 6.4 presenta un resumen de la totalidad de activos que componen la infraestructura eléctrica de transporte en alta tensión [XM, 2012].

[2] Como información, la empresa ISA es propiedad mayoritaria del estado Colombiano y también gestiona las redes de transporte en países como Bolivia, Perú, Brasil y Chile.

Tabla 6.4: Características de la Red de Transporte del Sistema Interconectado Colombiano

Red de transporte	Km de circuito
500 kV	2.646
220-230 kV	11.654
138 kV	15
110-115 kV	10.089
Total	24.405

La Tabla 6.5 contiene el conjunto de subestaciones que permiten representar la topología del sistema interconectado colombiano en niveles de 220kV y 500kV [BUITRAGO & TAUTA, 2008]. En la Figura 6.5 se han indicado los diferentes puntos de conexión a otras cargas, así como generadores que inyectan potencia activa en la red. Para estudiar la *vulnerabilidad geodésica* de la red ($\bar{v}$) no se requieren especificar los parámetros eléctricos de carga, generación, ni los parámetros de líneas (resistencia, reactancia). No obstante, como información se ha indicado la cantidad aproximada de carga y de generación que converge en cada bus. La tensión base es de 220kV y 500kV. La potencia base es de 1000MVA.

Tabla 6.5: Conjunto de subestaciones a 220kV y 500kV consideradas en el modelo topológico

Nº BUS	NOMBRE	TENSIÓN -kV-	CARGA -P.U-	GENERACIÓN -P.U-	Nº BUS	NOMBRE	TENSIÓN -kV-	CARGA -P.U-	GENERACIÓN -P.U-
1	Alto Anchicayá	220	0	0.439	48	Mirolindo	220	0.08533	0
2	Ancón Sur EPM	220	0.09583	0	49	Noroeste	220	0.62533	0
3	Ancón sur ISA	220	0.1415	0	50	Nueva Barranquilla	220	0.09817	0
4	Balsillas	220	0	0.132	51	Ocaña	220	0.099	0
5	Banadia	220	0.06483	0	52	Occidente	220	0.05017	0.045
6	Barbosa	220	0.35283	0	53	Oriente	220	0.01767	0
7	Barrancaberm eja	220	0.0005	0	54	Páez	220	0.01217	0
8	Belén Cúcuta	220	0.093	0	55	Paipa	220	0	0.165
9	Bello	220	0.0005	0.075	56	Pance	220	0.11167	0.026
10	Betania	220	0.068	0.54	57	Paraíso	220	0.12217	0.27
11	Bucaramanga	220	0.0145	0	58	Playas	220	0.47583	0.318
12	Candelaria Bolívar	220	0.0005	0	59	Pomasqui	220	0	0.135
13	Caño Limón	220	0	0	60	Porce II	220	0	0.411
14	Cartagena	220	0.04767	0	61	Porce III	220	0	0.6
15	Cartago	220	0	0	62	Primavera	220	1.11167	0
16	Cerromatoso 220	220	0.19633	0	63	Purnio	220	0.96717	0
17	Cerromatoso 500	500	1.30383	0	64	Sabanalarga 220	220	0.96383	0

Nº BUS	NOMBRE	TENSIÓN -kV-	CARGA -P.U-	GENERACIÓN -P.U-
18	Chinú 500	500	1.03667	0
19	Chivor	220	0.21167	1
20	Circo	220	0.03583	0
21	Comuneros	220	0.0485	0.072
22	Cuestecitas	220	0.002	0
23	El copey	220	0.14583	0
24	Envigado	220	0.04817	0
25	Esmeralda	500	1.30483	0.03
26	Fundación	220	0.4285	0
27	Guadalupe IV	220	0.00517	0.495
28	Guajira	220	0.05067	0.56
29	Guatapé	220	1.594	0
30	Guatiguará	220	1.0125	0
31	Guavio	220	0.2705	1.15
32	Jaguas	220	0.07883	0.17
33	Jamondino	220	0.08433	0
34	Juanchito	220	0.0375	0
35	La Enea	220	0	0.27
36	La guaca	220	0.173	0.315
37	La Hermosa	220	0	0
38	La mesa	220	0.4785	0.295
39	La Reforma	220	0	0.125
40	La sierra	220	0.9655	0
41	La tasajera	220	0.05667	0.309
42	La Virginia 230	220	0.22367	0
43	La Virginia 500	500	0.42383	0
44	Los palos	220	0.51417	0
45	Malena	220	0	0.021
46	Miel	220	0.0235	0.396
47	Miraflores	220	0.01667	0

Nº BUS	NOMBRE	TENSIÓN -kV-	CARGA -P.U-	GENERACIÓN -P.U-
65	Sabanalarga 500	500	0.973	0
66	Salto Antioquia	220	0.0425	0
67	Salvajina	220	0	0.285
68	Samore	220	0.12267	0
69	San Bernardino	220	0.28717	0
70	San Carlos 230	220	2.09383	1.24
71	San Carlos 500	500	1.455	0
72	San Felipe	220	0.31033	0
73	San marcos 230	220	0.13067	0
74	San marcos 500	500	0	0
75	San Mateo Bogotá	220	0.01033	0
76	San Mateo Cúcuta	220	0.001	0
77	Santa Marta	220	0.12183	0
78	Sochagota	220	0.2535	0
79	Tasajero	220	0.15083	0
80	Tebsa	220	0	0.7
81	Termoflores	220	0	0.61
82	Ternera	220	0.04767	0.3
83	Toledo	220	0.22117	0
84	Torca	220	0.36467	0
85	Tunal	220	0.04783	0
86	Urabá	220	0	0
87	Urrá	220	0.09917	0.345
88	Valledupar	220	0.05067	0
89	Yumbo	220	0.60267	0
90	Torca 500	500	0	0
91	Primavera 500	500	0	0
92	Ocaña 500	500	0	0
93	El copey 500	500	0	0
94	Chinú 220	220	0	0

En resumen, para el **caso 1** en el sistema colombiano se pretende realizar el estudio de vulnerabilidad de una red de 94 buses en tensiones de 220kV y 500kV.

6.3.2.2 Caso 2: Mejora en la Robustez de la Red Colombiana – 220kV y 500kV

Los planes de inversiones en infraestructuras para mejorar la robustez del sistema colombiano se especifican en [UPME, 2012]. Esto significa la construcción de nuevas líneas de transporte en alta tensión para unir las subestaciones existentes, y de esta manera, mejorar el mallado de la infraestructura.

La Unidad de Planeación Minero Energética (UPME) es un organismo adscrito al Ministerio de Minas y Energía de Colombia, a través del cual se planifican las nuevas inversiones y la expansión del sistema interconectado nacional colombiano.

En el documento de planificación para el periodo 2010-2024 [UPME, 2012], en lo que tiene que ver con la expansión de la red de alta tensión 220kV y 500kV se propone consolidar el mallado de la red para hacerla más robusta frente a ataques deliberados y fallos específicos, especialmente la interconexión entre la región andina y la región caribe. Además, al surgir nuevos centros de desarrollo en la altillanura Orinoquia, también se busca mejorar el mallado del sistema interconectado en estas regiones donde crece la demanda de energía eléctrica.

Las modificaciones que se toman en esta aplicación se relacionan con las siguientes inversiones [UPME, 2012]:

- Instalación de nuevo transformador 500kV/220kV en subestación Chinú.
- Conexión de circuito a 220kV entre Chinú y Urabá (Región Caribe).
- Conexión de circuito a 220kV entre Guavio y Tunal (Centro del país).
- Anillo a 220kV entre Salto-Bello y Ancón (Región Andina, Medellín)
- Anillo a 220kV entre Cartagena, Subestación Bolívar y Subestación Tebsa (Región Caribe)
- Conexión Caño Limón y Paipa a 220kV (Región andina y Arauca) por su interrelación con el desarrollo petrolero.
- Anillo a 220kV alrededor de subestación Malena (región andina – eje cafetero).

El programa de planificación de la UPME incluye muchísimos otros planes, relacionados con las redes de 220kV, construcción de nuevas subestaciones a 220 kV y 500kV, instalación de nuevos transformadores, etc. Todo ello implica la construcción de nuevas obras asociadas a los circuitos de transporte y distribución. Sin embargo, para efectos de aplicación de la propuesta metodológica, nos concentramos en

estudiar la decisión de aumentar el mallado en la red según los planes indicados previamente, sin adicionar nuevos buses.

La evaluación de las estrategias de mejora en la robustez, y su efecto sobre la vulnerabilidad estructural de la red constituye el principal desarrollo de esta sección. En resumen, para este **caso 2** se pretende realizar análisis de vulnerabilidad sobre la misma red de 94 buses, pero con los enlaces adicionales descritos en esta sección.

6.3.2.3 Caso 3: Planificación de la Expansión de la Red Colombiana de 220kV y 500kV

De acuerdo al documento [UPME, 2012] para desarrollar el Plan de Expansión de Transporte de Colombia se realiza inicialmente un diagnóstico de la red actual, correspondiente al caso 1 en la Figura 6.4, el cual sirve como marco de referencia. Posteriormente, se establece la red objetivo como visión de largo plazo, orientando así la expansión horizonte de planeamiento de largo, medio y corto plazo con ventanas de 15, 10 y 5 años, respectivamente

Se realizan los balances entre generación y demanda, estudios eléctricos de flujo de carga, corto-circuito, estabilidad transitoria y de tensiones. Igualmente se determinan transferencias entre áreas, límites de importación o exportación, energía dejada de suministrar por las diferentes causas, y generaciones de seguridad, entre otros [UPME, 2012]. Teniendo en cuenta el plan de expansión definido en el horizonte 2010-2024, para la red de alta tensión en 220kV y 500kV, se ha propuesto instalar nuevas subestaciones en las ubicaciones geográficas recogidas en la Tabla 6.6.

Tabla 6.6: Plan de expansión de nuevas subestaciones de 220kV y 500kV en Colombia

N° BUS	NOMBRE	kV	DEPARTAMENTO	N° BUS	NOMBRE	kV	DEPARTAMENTO
95	Panamá	220	Conexión Internac	106	Alferez 220	220	Valle
96	Silencio	220	Atlántico	107	Infantas	220	Santander
97	Cuatricentenario	220	Conexión Internac	108	Sogamoso	220	Boyacá
98	Chocó	220	Chocó	109	Armenia	220	Quindío
99	Miel II	220	Caldas	111	Ecuador 500	500	Conexión Internac
100	Nueva Granada	220	Santander	112	Jamondino	500	Nariño
101	Salitre	220	Cundinamarca	113	Alferez 500	500	Valle
102	Chivor II	220	Cundinamarca	114	Ituango	500	Antioquia
103	Jaguar	220	Meta	115	Porce 4	500	Antioquia
104	Bacatá 220	220	Cundinamarca	116	Nueva Esperanza	500	Cundinamarca
105	Quimbo	220	Huila	117	Envigado 500	500	Antioquia

En resumen, para este **caso 3**, se realizará análisis de vulnerabilidad sobre la una nueva red de 117 buses a 220kV y 500kV, que se ha modificado a partir del caso 1, pero con nuevos buses y nuevos enlaces, según se definen en el plan de expansión de [UPME, 2012].

6.4 RESPUESTAS DE VULNERABILIDAD ESTRUCTURAL

Al cuantificar la vulnerabilidad estructural de las redes es necesario evaluar la tolerancia de la red frente a errores aleatorios y ataques deliberados, según se explicó previamente en la sección 5.3. En las siguientes subsecciones se analiza la evolución de la topología de las redes, así como su respuesta frente a riesgos que originan fallos en cascada. El análisis de vulnerabilidad se realiza en función de la cantidad de nodos aislados *f*, los cuales se relacionan con determinados escenarios de riesgos; por ejemplo, un fenómeno natural que deje aislado un cierto porcentaje del territorio donde está ubicada la infraestructura.

La ejecución del algoritmo se ha realizado en una computadora personal, con versión *Matlab 7.2* ® y cuyo hardware corresponde a un procesador *Intel Core Duo* de 2.33 GHz, y 2GB de memoria RAM. Algunas estadísticas relevantes a la simulación de los ataques deliberados y errores aleatorios en las redes bajo estudio, se presentan en la Tabla 6.7.

Tabla 6.7: Resumen del proceso iterativo tolerancia errores aleatorios y ataques deliberados en Redes de Colombia y España.

Estrategia Eliminación	Red bajo estudio	N° muestras	N° iteraciones por muestra
Aleatoria	España (Caso 1)	35	128
Aleatoria	España (Caso 2)	35	131
Aleatoria	España (Caso 3)	35	184
Aleatoria	Colombia (Caso1)	35	218
Aleatoria	Colombia (Caso 2)	35	232
Aleatoria	Colombia (Caso 3)	35	271
Deliberada	España (Caso 1)	1	40
Deliberada	España (Caso 2)	1	42
Deliberada	España (Caso 3)	1	100
Deliberada	Colombia (Caso1)	1	82
Deliberada	Colombia (Caso 2)	1	92
Deliberada	Colombia (Caso 3)	1	104

Las muestras contienen los resultados de iteraciones por la eliminación sucesiva de nodos, es decir, la última contingencia *N–t* del análisis de fallos en cascada, incluyendo la realización del caso base. En la Tabla 6.7 el número de

iteraciones por cada muestra es mayor en el caso de eliminaciones aleatorias, que aquellas dirigidas por su grado nodal.

6.4.1 DISTRIBUCIÓN DE GRADO NODAL E INDICADORES DEL GRAFO DE LIBRE ESCALA

La distribución de grado nodal permite tipificar las redes complejas, donde varios nodos con gran número de conexiones se convierten en pilares fundamentales de la red. En la Figura 6.6 se observa la *distribución del grado nodal P*(*k*) para los casos de la red colombiana a 220kV y 500 kV, y de la red española a 400kV. También se incluye la representación de las distribuciones de grado nodal para los casos 2 y 3 (descritos en 6.3.1 y 6.3.2), de acuerdo con los planes indicativos de expansión de las redes [MINETUR, 2008; UPME, 2012]. Se han calculado utilizando funciones de la herramienta *MatlabBGL* para grafos [GLEICH, 2008].

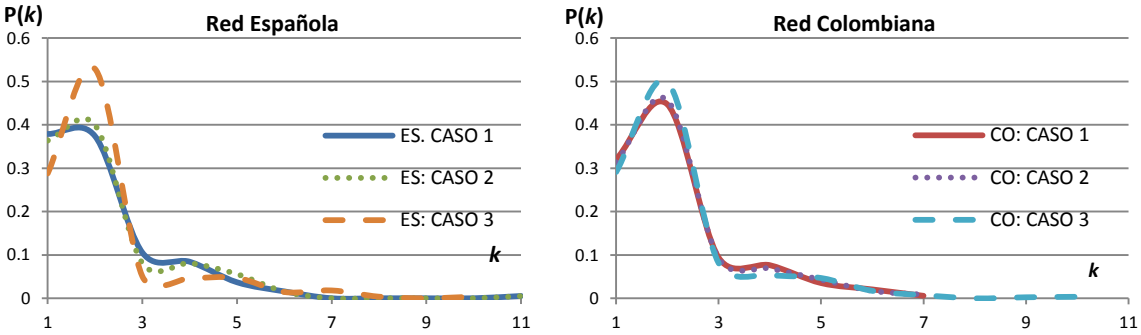


Figura 6.6: Distribución de grado nodal. Comparación según casos de modificación de la red

La distribución de grado nodal *P*(*k*) presentada en la Figura 6.6 indica la probabilidad de que un nodo de las redes bajo análisis que sea elegido al azar tenga exactamente *k* conexiones (o vecinos). Como se puede observar en la Figura 6.6, para el caso 1 de la red española, la probabilidad de que un nodo del grafo tenga un grado de conexión *k*=2 es *P*(*k*)=0.4, lo que significa que el 40% de los nodos de la red tiene sólo dos conexiones con otros nodos de la red. Sin embargo, un 10% de nodos de la red tienen grado de conexión *k*=3 (subestaciones en las que convergen 3 líneas de transporte).

Para facilitar la comprensión del significado del grado nodal en la topología de la red eléctrica, se presenta en la Figura 6.7 una parte del sistema eléctrico del noroeste de España, con los respectivos valores del grado nodal en los elementos que lo conforman.

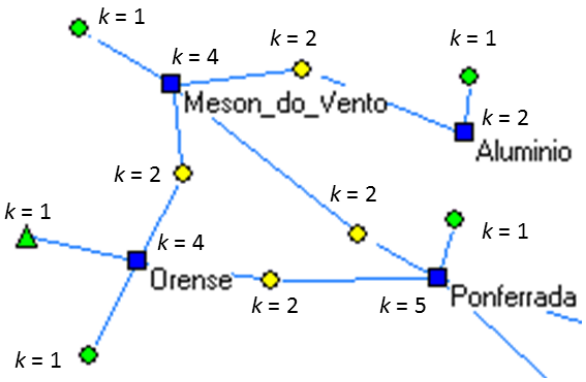


Figura 6.7: Valor de grado nodal en cada elemento del sistema de potencia

El valor *k*=2 corresponde típicamente a la representación en el grafo de las líneas de transporte eléctrico (enlaces que unen dos subestaciones). El valor *k*=1 se refiere a los nodos en el grafo que quedan en antena, situación que corresponde normalmente a centrales de generación o centros de carga. Analizando en la Figura 6.6 la distribución de grado nodal *P(k)* de la red española para *k*=2, se observa el incremento de *P(k)* en el caso 2 respecto al caso base 1, lo que cuál es coherente ya que la expansión de la red en el caso 2 se realiza añadiendo algunas nuevas líneas eléctricas, lo que incrementa la proporción de enlaces en el grafo de tipo *k*=2.

Sin embargo, comparando el caso 3 con el caso 1, el incremento ahora más significativo de *P(k)* se explica por el crecimiento en un 36% del número de subestaciones y de más del 50% en líneas de transporte en los planes de expansión de la red (se pasa de 48 a 76 subestaciones y de 212 a 332 enlaces de 400 kV).

Por otro lado, en los casos de la red española 2 y 3, la distribución de grado nodal *P(k)* disminuye para *k*=3 y *k*=4 pero aumenta ligeramente para *k*>4, lo que significa que las nuevas líneas y subestaciones se conectan preferentemente en subestaciones más importantes.

Los resultados obtenidos para la red colombiana son muy similares en los tres casos al análisis realizado para la red española. No obstante, se observa que en la situación actual de la red de transporte (caso 1), el máximo grado de conexión es *k*=7 y no se alcanzará el grado *k*=10 hasta que no se implementen los nuevos proyectos de construcción de líneas y subestaciones del caso 3. La red de transporte eléctrico colombiana es una red menos mallada que la española, tal como se puede deducir gráficamente en las figuras 6.2 y 6.4, y como se corrobora numéricamente de los resultados en la Figura 6.6.

Es posible ajustar analíticamente los resultados presentados en dichas curvas, siguiendo una distribución de ley de potencias [ALBERT & BARABÁSI, 2002], como se explicó previamente en la sección 5.2.1.6, mediante la relación siguiente:

$$P(k) \sim k^{-3} \qquad [6.1]$$

Según la distribución presentada en [6.1], la topología de las redes en España y Colombia corresponde a un grafo de libre-escala. Desde el punto de vista de la infraestructura eléctrica, esto significa que existe una pequeña cantidad de subestaciones que por su gran cantidad de conexiones son una parte fundamental de la red, y su ausencia podría representar un fallo en cadena sobre el resto de la red. Por ejemplo, la *subestación Madrid* en la red española tiene un grado k = 11, y debe considerarse como un bus de alto impacto en la vulnerabilidad de la red.

Otras medidas estadísticas que caracterizan los grafos de libre escala representativos de las redes de transporte en alta tensión se presentan en la Tabla 6.8.

Tabla 6.8: Medidas estadísticas de los grafos de libre escala

RED	BUSES	NODOS	ENLACES	GRADO MEDIO ($\bar{k}$)	DISTANCIA MEDIA GEODÉSICA ($\bar{d}$)	EFICIENCIA MEDIA ($\bar{e}$)
España (Caso 1)	48	190	212	2.23	923	0.025
España (Caso 2)	48	198	228	2.30	1134	0.029
España (Caso 3)	76	278	332	2.39	2100	0.027
Colombia (Caso 1)	93	340	389	2.29	2201	0.019
Colombia (Caso 2)	94	348	403	2.32	2306	0.019
Colombia (Caso 3)	117	405	471	2.32	4107	0.025

En la Tabla 6.8 se hace referencia a los siguientes indicadores de los grafos de libre escala:

- *Buses, Nodos, Enlaces*: constituyen la medida de cada uno de las redes bajo análisis, según los casos descritos en la sección 6.3. Obsérvese que el caso 2 corresponde a una estrategia de aumento en el mallado de las redes de España y Colombia, en tanto que el *caso 3* corresponde a la nueva topología de las redes según los planes indicativos de expansión de cada país.
- *Grado medio de conexión*: recordando la ecuación [5.2] ($\bar{k} = 2 \cdot E/N$), este indicador permite dar una idea relativa sobre cuán mallada está la red. En la Tabla 6.8 se destaca que el grado medio de conexión aumenta para el caso 2. Al cambiar la topología de la red haciéndola más mallada, se evidencia un valor mayor en el

promedio del grado nodal de la red, es decir, existe mayor interconexión entre los nodos de cada red.

- *Distancia media geodésica*: a partir de la definición [5.15] estudiada en la sección 5.2.3.1 se observa la medida que describe qué tan compacta es una red. Este indicador constituye la base para calcular la *vulnerabilidad geodésica* ($\bar{v}$) de la red (ver 5.3.4.3) y mide la accesibilidad de un nodo respecto a otro, es decir, el camino del flujo de potencia desde un determinado nodo hasta cualquier otro nodo del sistema. Los casos 2 y 3 muestran un valor mayor de la *distancia geodésica* teniendo en cuenta que al aumentar el tamaño de la red, ésta se hace menos compacta.
- *Eficiencia media*: Según se ha explicado previamente en la ecuación [5.17], cuando la eficiencia es un valor bajo, entonces el flujo de energía eléctrica debe circular a través de un mayor número de nodos, y en consecuencia, pueden existir problemas de sobrecargas. En una comparación entre el caso 1 y el caso 3 en ambas redes, correspondiente a la aplicación de los planes de expansión, se mejora la *eficiencia*, dado que existe mayor grado de conexión, aunque se aumente notablemente la *distancia geodésica media*.

Como se demostró en el capítulo 5 en la construcción de la propuesta metodológica, se puede asumir la premisa que el índice de desconexión de cargas *PLS* [5.34] está correlacionado con el índice de vulnerabilidad $\bar{v}$ [5.18]. En consecuencia, será más práctico utilizar el índice de *vulnerabilidad geodésica*, por tratarse de un índice que se puede obtener de manera más rápida y eficiente que el índice *PLS*, con la ventaja de que no es necesario ejecutar flujos de carga.

6.4.2 TOLERANCIA ANTE ERRORES ALEATORIOS

Recuérdese que los errores aleatorios se asocian con aquellos escenarios de riesgos de naturaleza aleatoria, como fenómenos naturales, fallos humanos involuntarios o fallos técnicos en equipos y hardware de la red. La comparación de resultados para cada uno de los casos de las redes en Colombia y España se explica a continuación.

6.4.2.1 Curva de Vulnerabilidad Errores Aleatorios

Una vez obtenida la información topológica de cada una de las redes bajo estudio, así como los respectivos casos considerados dentro de los planes de

expansión se aplica el algoritmo descrito en la sección 6.2, con el objetivo de modelar la vulnerabilidad geodésica en función de la proporción de nodos aislados del sistema.

Según se ha demostrado en el capítulo 5, la curva de vulnerabilidad geodésica representa el impacto ocasionado sobre la red eléctrica por la ocurrencia de riesgos a los cuales se asocia el aislamiento de un porcentaje de nodos de la red (*f*). Dicho impacto se relaciona con la cantidad de carga desconectada de la red *PLS*.

Al ejecutar el algoritmo de cálculo sucesivo de contingencias N-1, según se ha descrito en sección 6.2 se obtienen los resultados que se representan en la Figura 6.8. Como resultado de los indicadores calculados, al realizar una comparación a simple vista entre la curva de vulnerabilidad de la red española y la red colombiana se deduce que ésta última es relativamente más vulnerable, pues en todos los casos, para la misma fracción de nodos aislados existe mayor impacto en el índice de vulnerabilidad para la red colombiana.

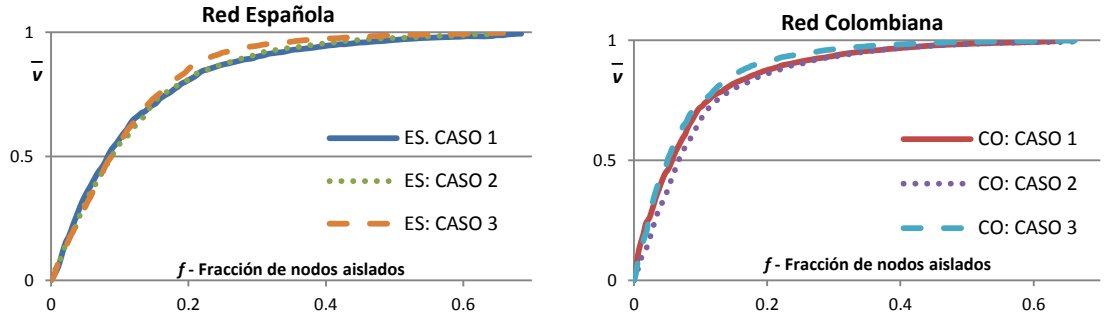


Figura 6.8: Vulnerabilidad Geodésica en Errores Aleatorios. Comparativo según casos de modificación de la red de cada país

La construcción de las curvas de vulnerabilidad de las redes españolas y colombianas de la Figura 6.8, contiene el cálculo de los tres diferentes casos explicados previamente en la sección 6.3. En total existen seis curvas, cada una corresponde al promedio del conjunto de resultados del muestreo de 35 escenarios en contingencias sucesivas N-1, los cuales se describieron previamente en la Tabla 6.7.

Una comparación entre el caso 1 (correspondiente a las redes originales) y el caso 2 (estrategia de mayor mallado) revela una leve mejora de la vulnerabilidad de las redes de ambos países.

Sin embargo, las comparaciones entre el caso 1 y el caso 3 (planes gubernamentales de expansión) evidencian que la red expandida es más vulnerable. Una explicación para esta situación tiene que ver con la construcción de una red menos compacta en la que aumenta la distancia geodésica entre los nodos.

Las políticas de los planes gubernamentales para construir las nuevas líneas de transporte tienen objetivos muy claros: en España se pretende atender el incremento de la demanda y aumentar la capacidad de evacuación al sistema eléctrico de los nuevos centros de generación con renovables, en tanto que en Colombia se busca brindar mayor fiabilidad para atender el incremento de la demanda y evitar el aislamiento de las zonas interconectadas en caso de que algún suceso deje fuera de operación alguna línea de transporte.

6.4.2.2 Ajuste Polinómico $\bar{v}$ =F(f)

Para cada una de las curvas de la Figura 6.8 (casos 1, 2, 3) es posible ajustar la relación $\bar{v}$ = **F**(*f*); es decir, la *vulnerabilidad geodésica* en función de la cantidad de *nodos aislados* en la red. De esta manera se puede conocer la respuesta de la infraestructura según la cantidad de nodos que se aíslan $\bar{v}$ =**F**(*f*), mediante aproximación polinómica de acuerdo a las expresiones de la Tabla 6.9.

Tabla 6.9: Aproximación polinómica de vulnerabilidad. Comparativo España–Colombia

Red	Ecuación Polinómica (Orden 6)	Correlación R^2
España (Caso 1)	$\bar{v}$ = -7.3334·f^6 + 46.396·f^5 - 85.576·f^4 + 73.934·f^3 - 34.245·f^2 + 8.6378·f - 0.0171	0.9998
España (Caso 2)	$\bar{v}$ = 133.47·f^6 - 254.03·f^5 + 164.73·f^4 - 27.976·f^3 - 13.914·f^2 + 7.0313·f - 0.0035	0.9998
España (Caso 3)	$\bar{v}$ = 182.39·f^6 - 387.49·f^5 + 299.12·f^4 - 89.608·f^3 - 1.6912·f^2 + 6.3555·f - 0.001	0.9999
Colombia (Caso 1)	$\bar{v}$ = -147.4·f^6 +391.09·f^5 - 418.73·f^4 + 232.12·f^3 - 71.242·f^2 + 12.02·f + 0.0219	0.9993
Colombia (Caso 2)	$\bar{v}$ = 29.62·f^6 +12.575·f^5 -108.76·f^4 + 112·f^3 - 49.858·f^2 + 10.862·f - 0.0362	0.9987
Colombia (Caso 3)	$\bar{v}$ = -239.27·f^6 +584.9·f^5 -578.49·f^4 + 297.79·f^3 - 85.506·f^2 + 13.526·f - 0.0022	0.9997

En todas las aproximaciones polinómicas de 6º orden $\bar{v}$ =**F**(*f*) de la Tabla 6.9, se verifica que el coeficiente de correlación es cercano a uno ($R^2 \approx 1$), por lo que estadísticamente es una aproximación muy efectiva para describir los fallos en cascada y, en general, la tolerancia de la red de infraestructura frente a errores aleatorios. Esta aproximación polinómica permitirá evaluar los diferentes escenarios de riesgos, en los cuales se involucra conocimiento experto que tiene en cuenta la cantidad de usuarios afectados, así como los posibles tiempos requeridos en el restablecimiento del servicio, en caso de un evento de *blackout* de la red de transporte.

En la Tabla 6.10 se muestran algunos resultados del aislamiento de una determinada cantidad de nodos en la red (*f*), y su impacto sobre la desconexión de cargas del sistema (vulnerabilidad $\bar{v}$).

Tabla 6.10: Impacto en la desconexión de usuarios (Vulnerabilidad $\bar{v}$)

RED	*f* = 5%	*f* = 10%	*f* = 20%	*f* = 30%
España (Caso 1)	0.34	0.57	0.81	0.90
España (Caso 2)	0.31	0.55	0.81	0.91
España (Caso 3)	0.30	0.54	0.86	0.95
Colombia (Caso 1)	0.47	0.71	0.88	0.93
Colombia (Caso 2)	0.40	0.65	0.87	0.93
Colombia (Caso 3)	0.51	0.73	0.91	0.96

Muchos escenarios de riesgo tienen asociados la consecuencia de aislar un área geográfica que comprometa una pequeña cantidad de nodos (5% ó 10% de los nodos de la red). Una mayor ilustración respecto de esta afirmación puede consultarse directamente en la carta de riesgos para la infraestructura eléctrica de la Figura 4.6 (sección 4.3.3), que presenta las componentes de riesgo de mayor impacto en el sistema de infraestructura de transporte eléctrico en alta tensión. En ella se definen los escenarios de riesgos de errores aleatorios cuyo efecto conlleva al aislamiento de una determinada proporción de nodos del sistema (*f*).

Un resultado interesante en esta respuesta se refiere a la efectividad de la planificación para hacer más robusta la red, lo cual se puede corroborar en la comparación del caso 1 con el caso 2, en ambos países. Se evidencia menor vulnerabilidad de la red $\bar{v}$ cuando se aumenta el valor promedio del grado de conexión $\bar{k}$ (una red más mallada construyendo nuevas líneas de transporte pero sin aumentar el número de subestaciones). En los resultados de la Tabla 6.10 se observa el efecto notable de disminución en la vulnerabilidad $\bar{v}$ de la red colombiana para aquellos casos de aislamiento $f \approx 5\%$ y $f \approx 10\%$. En la red española la mejora en la vulnerabilidad $\bar{v}$ es ligeramente menor pero en todo caso positiva.

Sin embargo, una comparación entre el caso 1 y el caso 3, que representa la aplicación del plan de expansión completo propuesto por los respectivos gobiernos, muestra un posible empeoramiento en la vulnerabilidad de la red, como se deduce de los valores de la Tabla 6.10. Esto se explica con ayuda de los resultados mostrados anteriormente en la Tabla 6.8. En España, la necesidad de aumentar el número de buses en un 36% (al pasar de 48 a 76), pero sólo un 3% en el grado de conexión (al pasar de 2.32 a 2.39) tiene el efecto del aumento de la vulnerabilidad $\bar{v}$. En Colombia,

el crecimiento del 26% requerido en el sistema (desde 93 a 117 buses), con sólo un 1% de aumento en el grado de conexión (al pasar de 2.29 a 2.32), explica la formación de una red menos compacta, pero también más vulnerable.

6.4.3 TOLERANCIA A LOS ATAQUES DELIBERADOS

La construcción de la curva de vulnerabilidad en ataques deliberados se realiza según la eliminación de nodos en la red de acuerdo a su grado nodal, comenzando por los que estén más conectados. De esta manera se representan los escenarios de riesgo relacionados con ataques de personas malintencionadas, como actos de terrorismo, ciberataques o actos de vandalismo. En este caso sólo se ejecuta una simulación para obtener los resultados, a diferencia de los errores aleatorios, en que se recolectan 35 conjuntos de resultados. El procedimiento de cálculo se ha descrito previamente en la Tabla 6.7.

6.4.3.1 Curva de Vulnerabilidad Ataques Deliberados

La Figura 6.9 contiene el resultado del cálculo de vulnerabilidad de acuerdo al aislamiento de los nodos según su grado nodal. Se puede observar que en ambos casos, el aislamiento de un pequeño número de nodos (f < 5%) tiene impacto muy alto sobre todo el sistema ($\bar{v}$ > 85%). Lo anterior significa que un ataque dirigido contra subestaciones con alta conectividad representará una caída de funcionamiento de la mayor parte de la infraestructura eléctrica y en consecuencia, se genera un *blackout* con amplia extensión geográfica.

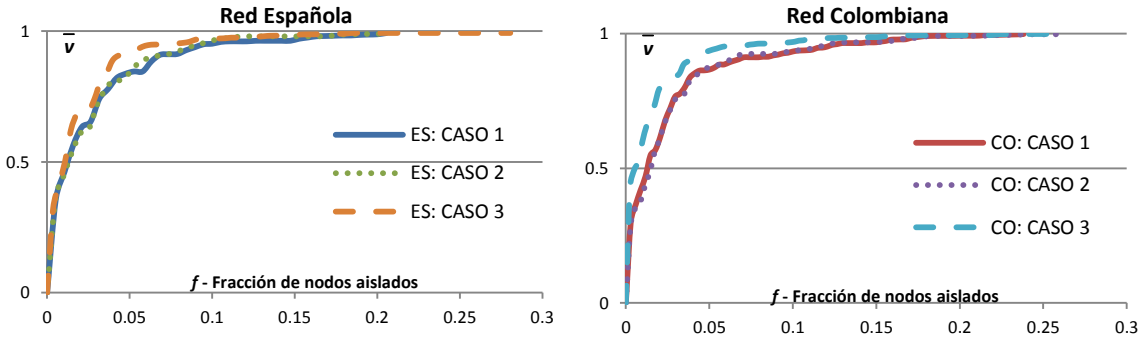


Figura 6.9: Vulnerabilidad Geodésica en Ataques Deliberados. Comparativo según casos de modificación de la red de cada país

Los resultados de vulnerabilidad de la Figura 6.9 evidencian un comportamiento muy similar en ambas redes frente a los ataques deliberados, cuyos valores son levemente mayores en el caso de la red colombiana respecto de la española (para la misma fracción de nodos aislados).

Al comparar el caso 1 (correspondiente a las redes originales) y el caso 2 (estrategia de mayor mallado) prácticamente las curvas de vulnerabilidad se superponen la una sobre la otra, para ambos países. Esto significa que la estrategia de crear una red más robusta no implica una mayor protección frente a los ataques deliberados contra las infraestructuras.

Por otro lado, la comparación entre el caso 1 y el caso 3 (planes de expansión de red), evidencia que la red expandida es más vulnerable frente a los ataques deliberados. Dado que al expandir la red se construye una red menos compacta. La retirada de los nodos de mayor conectividad tiene el efecto de aumentar dramáticamente la distancia geodésica entre los nodos de la red que quedan conectados.

6.4.3.2 Resultados

En la Tabla 6.11 se muestran algunos datos puntuales de las consecuencias asociadas a la eliminación de una cantidad de nodos con alto grado de conexión, y su impacto sobre la desconexión de cargas del sistema (vulnerabilidad $\bar{v}$).

Tabla 6.11: Impacto en la desconexión de usuarios frente ataques deliberados ($\bar{v}$)

RED	f = 0.5%	f = 1%	f = 2%	f = 5%	f = 10%
España (Caso 1)	0.36	0.45	0.62	0.84	0.95
España (Caso 2)	0.36	0.45	0.62	0.84	0.95
España (Caso 3)	0.40	0.50	0.69	0.92	0.97
Colombia (Caso 1)	0.36	0.45	0.70	0.87	0.97
Colombia (Caso 2)	0.36	0.43	0.70	0.87	0.97
Colombia (Caso 3)	0.49	0.60	0.79	0.92	0.97

Al comparar en ambos países el caso 1 y el caso 2, no se evidencian mejoras significativas en la tolerancia contra ataques deliberados. Prácticamente los valores de vulnerabilidad de ambos casos se superponen, lo que significa que la estrategia de efectuar un mayor mallado sobre la infraestructura no es efectiva para el caso de los ataques deliberados.

De manera particular, en ambos países la red ampliada del caso 3 es incluso más vulnerable a los ataques deliberados que el caso 1. Esto se explica porque tanto en España como en Colombia, en la planificación de las inversiones en expansión del sistema, surgen buses que concentran altos grados de conectividad, por ejemplo Madrid (España) y Esmeralda (Colombia), ambos con k = 10. Adicionalmente, algunos buses con k > 7 tienen el efecto de impactar casi toda la red cuando son aislados.

6.4.4 TOLERANCIA ANTE ERRORES ALEATORIOS Y ATAQUES DELIBERADOS: COMPARATIVA

Los resultados presentados en la Figura 6.8 y en la Figura 6.9 muestran que las redes son mucho más resistentes a aquellos escenarios que involucran riesgos de tipo aleatorio (fenómenos naturales, fallos técnicos, fallos humanos, etc) que a las amenazas de personas malintencionadas (vandalismo, terrorismo, cyber-ataques). Como caso particular, en el caso de la red española una amenaza que comprometa una pequeña cantidad de nodos, por ejemplo, $f \approx 5\%$, el impacto de aislamiento de usuarios es de $\bar{v} \approx 30\%$ (Figura 6.8) cuando se trata de un simple riesgo aleatorio, pero puede llegar a ser $\bar{v} \approx 85\%$ en caso que se trate de un ataque deliberado (Figura 6.9).

En consecuencia, los planes de expansión del sistema mediante la construcción de nuevas líneas de transporte dejando la misma cantidad de subestaciones reconocida como *estrategia de robustez*, es efectiva sólo como protección contra escenarios de riesgos aleatorios. Los ataques deliberados requerirán otras estrategias de protección, como por ejemplo brindar una mejor *resiliencia*, que incluya estrategias para la reconfiguración de la red, mejora de los tiempos de reparación y puesta en operación cuando se presente algún ataque deliberado.

En las dos infraestructuras analizadas, los planes de expansión correspondientes al caso 3 evidencian mayor vulnerabilidad del sistema. Esto se explica porque la expansión del sistema implica la construcción de una infraestructura menos compacta. Adicionalmente, como se indicó en la Tabla 6.8 el grado medio de conexión aumenta levemente en relación con la cantidad de activos (buses y enlaces) que se construyen en la nueva red.

Una comparación de los resultados presentados en la Tabla 6.10 y en la Tabla 6.11 permite reafirmar la conclusión de que la estrategia de mejora en la robustez de la red con la construcción de nuevos enlaces entre los actuales buses de la red (caso 2) es muy efectiva ante aquellos riesgos relacionados con fenómenos aleatorios. Sin embargo, para el caso de las amenazas de ataques deliberados no se evidencia el mejor funcionamiento del sistema. Por su parte, la adición de nuevos buses a las redes (caso 3) se relaciona con una mayor vulnerabilidad. Lo anterior se explica porque el grado medio de conexión (calculado en la Tabla 6.8) no aumenta en la misma proporción, es decir, no existen planes de mallado adicionales.

6.5 COMENTARIOS AL CAPÍTULO

Con el propósito de darle una aplicación práctica a las propuestas metodológicas que se han desarrollado en los capítulos previos, se ha realizado una aplicación práctica de la metodología de evaluación fundamentada en teoría de grafos, a partir de los conceptos formulados y resultados obtenidos en los capítulos 4 y 5. La aplicación de la metodología se ha realizado de manera sistemática con la finalidad de obtener una valoración cuantitativa de la vulnerabilidad en redes de transporte de alta tensión.

En la aplicación se han comparado las estructuras de las redes de transporte en alta y media tensión en dos países con características diferentes. El principal objetivo es la cuantificación de la vulnerabilidad en función de los usuarios afectados por una determinada componente de riesgo (nodos aislados *f*).

A partir de la aplicación de la metodología, se obtiene una evaluación cuantitativa del impacto que generan algunos de los escenarios de riesgo sobre la red de transporte. Dada la correlación existente entre la vulnerabilidad geodésica y la desconexión de cargas, este impacto refleja el porcentaje de usuarios desconectados. Obsérvese que aquellos riesgos relacionados con acontecimientos aleatorios, como los fenómenos naturales, los fallos técnicos en equipos, fallos humanos, etc. pueden ocasionar el aislamiento de una pequeña cantidad de nodos. En el caso que $f \approx 5\%$ se ocasiona un impacto sobre el 30% de la red en España y el 40% en Colombia. Sin embargo, aquellos ataques deliberados sobre los buses con mayor grado nodal para el mismo porcentaje de nodos aislados ($f \approx 5\%$) ocasionan un impacto sobre más del 85% de los usuarios conectados en ambas redes.

Además, ha sido posible obtener conclusiones sobre la efectividad de las inversiones en la topología de las infraestructuras, según la aplicación de los planes indicativos de expansión de las redes (casos 2 y 3). Se observa que una estrategia de mejora del mallado de la red (robustez) solamente permite disminuir la vulnerabilidad frente a los errores aleatorios, pero no frente a los ataques deliberados. Por otra parte, la planificación en la expansión de las redes del caso 3 se asocia con una mayor vulnerabilidad de las redes, dado que se hacen menos compactas y más extensas.

Finalmente, se ha validado la utilidad de los modelos de teoría de grafos que proporcionan una visión conceptual de una red eléctrica y facilitan su implementación computacional mediante algoritmos más rápidos y eficientes. Es un método sustitutivo de los flujos de carga para el análisis de la vulnerabilidad relativa de redes eléctricas.

Con la propuesta aquí desarrollada sólo es necesario conocer la distribución topológica de la infraestructura para desarrollar el caso de estudio.

La metodología presentada en el caso de estudio de este capítulo puede aplicarse en otras áreas, como las redes de información, internet, y redes sociales, lo cual podrá constituir una futura línea de investigación a partir de los conceptos expuestos en esta sección.

7 CONCLUSIONES

Se presentan las conclusiones del trabajo de investigación, así como el resumen de los resultados más relevantes y las contribuciones originales de la tesis doctoral. El esfuerzo investigador en el desarrollo de una metodología que integre estrategias de gestión de riesgo y herramientas de análisis en redes de transporte en alta y media tensión culminan aquí con una breve discusión de las principales aportaciones y de los resultados obtenidos en las diferentes secciones de la tesis.

7.1 CONSIDERACIONES FINALES

La seguridad, la prosperidad económica y el bienestar social en cualquier país dependen de la infraestructura eléctrica, transversal a todos los sectores de la economía. Esta investigación contribuye al desarrollo de estrategias de gestión de riesgos que permitan identificar y evaluar eficazmente las amenazas asociadas a las actividades relacionadas con el suministro eléctrico.

En esta tesis se ha comenzado por realizar una revisión en el contexto de las políticas y de los planes de protección de infraestructura crítica, destacando especialmente su relación con los programas de gestión de riesgos. Dentro de esta revisión, se ha incorporado la descripción de aquellas plataformas, técnicas y metodologías que permiten describir el estado actual de la infraestructura, así como su comportamiento dinámico a través de ciertas técnicas de simulación. El análisis del estado del arte en el tema de protección de infraestructura crítica se ha fundamentado en literatura especializada y fuentes públicas de información, las cuales están relacionadas en el capítulo 2 y que se complementan con la síntesis presentada en el anexo A.

Para la identificación de amenazas en el sistema eléctrico se ha formulado la técnica de *mapas interconectados de riesgos* descritos en el capítulo 3, los cuales permiten identificar de manera integral y versátil los riesgos que impactan al sistema de infraestructura crítica. Un mayor nivel de detalle en esta actividad ha requerido la determinación de componentes de riesgo, definiendo su categorización (riesgos operacionales, de entorno, financieros e indicadores de calidad y cumplimiento), así como su impacto en la cadena de valor del sistema de infraestructura eléctrica.

En el capítulo 4 se ha formulado la técnica de *cartas de riesgos* que permite realizar una evaluación semicuantitativa de los riesgos que afectan la cadena de valor en las infraestructuras. Esta calificación depende directamente de las evaluaciones subjetivas, de las opiniones de analistas, de las circunstancias y de los lugares en los que se lleva a cabo el procedimiento de evaluación. De esta manera, se ha realizado un caso de estudio teniendo en cuenta la experiencia de las compañías eléctricas colombianas. Esta calificación se complementa con la priorización de las acciones de mitigación de riesgos, especialmente aquellos calificados como “críticos” e “importantes”. Las recomendaciones surgidas en esta etapa se pueden extender a otras infraestructuras.

En el capítulo 5 se ha desarrollado un modelo matemático fundamentado en teoría de grafos para evaluar la vulnerabilidad estructural de los sistemas de potencia. Se ha validado la utilidad de modelar los sistemas eléctricos de potencia como un grafo de libre escala, y también se ha demostrado la correlación existente entre los indicadores geodésicos de las redes complejas y las técnicas tradicionales de flujos de carga en ingeniería eléctrica.

Se ha formulado una metodología de análisis estructural de vulnerabilidad en la red de transporte de alta y media tensión, ocasionada por errores aleatorios, o por ataques deliberados a las infraestructuras. En este punto, las técnicas de teoría de grafos se han convertido en una herramienta útil para analizar el funcionamiento físico de las redes de energía, especialmente cuando se analizan los fallos que determinan los eventos en cascada. Se ha definido un indicador de vulnerabilidad geodésica en los grafos de libre escala, que tiene correlación con los parámetros de carga conectada al sistema. Los estudios de validación se han ejecutado con diferentes redes de prueba IEEE, lo que ha permitido comprobar la efectividad de los resultados al aplicar la teoría de grafos. De esta manera ha sido posible integrar el análisis de contingencias en sistemas de potencia, con la evaluación de riesgos.

Mediante el caso aplicativo desarrollado en el capítulo 6 (redes de Colombia y de España) se ha comparado la vulnerabilidad relativa existente entre dos infraestructuras, así como el impacto de los planes de expansión enunciados en diferentes documentos gubernamentales. El efecto de invertir en estrategias de mayor robustez, aumentando el grado medio de conectividad de cada bus, representan mejoras leves en la vulnerabilidad de la red. Sin embargo, al aumentar el tamaño mediante expansión de la misma, ésta se hace menos compacta y el mallado no crece en la misma proporción, por cuya razón se presentan valores más elevados en los indicadores de vulnerabilidad estructural del sistema.

7.2 PRINCIPALES CONTRIBUCIONES DE LA TESIS

El trabajo de investigación desarrollado permite concluir los siguientes resultados relevantes de esta tesis doctoral:

- Se ha desarrollado una propuesta metodológica de identificación de riesgos en la cadena de valor del sistema eléctrico, contribuyendo con una estrategia de clasificación, que a su vez considera la subdivisión en componentes de riesgo. La metodología puede ser aplicable a las organizaciones propietarias y operadoras de los sistemas de infraestructura crítica.

- Se ha comprobado la versatilidad de la metodología de mapas de riesgos mediante la asociación de las amenazas identificadas a los diferentes subsistemas del sistema eléctrico.
- Se ha definido una propuesta metodológica para evaluación semicuantitativa de los recursos técnicos, financieros, humanos y materiales dentro de las organizaciones, asignando una calificación a cada riesgo en términos de su probabilidad y según el impacto de sus consecuencias, cuyos resultados se representan en las *cartas de riesgos*.
- La aplicación de esta metodología de evaluación semicuantitativa en un caso de estudio, ha permitido concluir cuáles son los riesgos más críticos, en un escenario de país.
- Se ha validado una propuesta de modelización de la red eléctrica de transporte en alta y media tensión, cuya representación corresponde a un grafo de libre escala, considerando como nodos todos los elementos que conforman el sistema: torres de transporte, transformadores, condensadores, plantas de generación, subestaciones, centros de carga, etc.
- Se ha desarrollado una metodología de evaluación de la vulnerabilidad estructural para cualquier red eléctrica, mediante la definición de un indicador fundamentado en la distancia media geodésica del sistema eléctrico de potencia.
- Se ha demostrado la correlación existente entre los modelos de flujos de carga con las mediciones obtenidas a partir de la teoría de grafos, haciendo posible la sustitución de herramientas que requieren mayores recursos computacionales (como son las rutinas de flujos de carga) por técnicas más eficientes (como los parámetros de redes complejas), para valorar la vulnerabilidad del sistema de infraestructura eléctrico.
- Una aplicación de la metodología desarrollada para evaluar la vulnerabilidad estructural en redes eléctricas de transporte ha proporcionado conclusiones sobre la efectividad de las inversiones en la topología de las infraestructuras, según la aplicación de los planes gubernamentales de expansión.

- La estrategia de brindar mayor robustez a las redes, es decir, mejorar el mallado y el grado de conectividad de los buses, proporciona leves mejoras en la vulnerabilidad de la red frente a errores aleatorios; sin embargo, no se evidencian mejoras en el caso de ataques deliberados a la infraestructura.

7.3 RECOMENDACIONES PARA FUTUROS TRABAJOS

Teniendo en cuenta las propuestas realizadas en esta tesis, quedan abiertas posibilidades para nuevas aplicaciones, desarrollos e investigaciones, en el campo de la toma de decisiones, la simulación de sistemas, y la gestión de riesgos, sobre la base de los conceptos y conocimientos generados a partir de la investigación. Algunas líneas de continuación de esta investigación pueden añadir valor a las aportaciones principales de esta tesis doctoral y permitir nuevos trabajos de investigación en el tema de protección de infraestructura crítica:

- Desarrollo de nuevas metodologías para identificar los activos más vulnerables en el sistema. El anexo C proporciona elementos básicos que pueden ser utilizados en esta futura línea.
- Desarrollo de metodologías para evaluar la efectividad de estrategias de mejora continua y acciones de mitigación del riesgo en el sistema de infraestructura.
- Evaluación cuantitativa de probabilidad e impacto de cada componente de riesgo, mediante indicadores de *Energía no Suministrada*, que tenga en cuenta el tiempo de restauración del servicio (t en horas), así como el porcentaje de nodos que se desconectan (f) por la manifestación de un riesgo.
- Aplicación de la metodología desarrollada a otros sistemas de infraestructura crítica, por ejemplo, sistemas de transporte y distribución de gas natural, petróleo, agua, así como los sistemas de transporte por carreteras y vías férreas. Todos estos sistemas pueden ser modelarse como una red compleja de libre escala, sometida a fallos sucesivos aleatorios o deliberados.

8 REFERENCIAS BIBLIOGRÁFICAS

[1] **ABDUR RAHMAN, H. M.** (2009). "*Modelling and Simulation of Interdependencies between the Communication and Information Technology Infrastructure and other Critical Infrastructures.*" Electrical and Computer Engineering. Vancouver (Canadá), University of British Columbia. **Tesis Doctoral:** 163p.

[2] **AJJARAPU, V. & CHRISTY, C.** (1992). "*The continuation power flow: a tool for steady state voltage stability analysis.*" Power Systems, IEEE Transactions on: Vol:**7**: (#*1*): 416-423, (0885-8950

[3] **ALBERT, R. & BARABÁSI, L.** (2002). "*Statistical mechanics of complex networks*." Review Modern Physics: Vol:**74**: 47-97) http://arxiv.org/abs/cond-mat/0106096

[4] **ALBERTS, C., DOROFEE, A., KILLCRECE, G.*, et al.*** (2004) "*CERT/CSIRT: Computer Security Incident Response Team*." **CMU/SEI-2004-TR-015**, Pittsburgh, PA (EEUU), (Consultado: Junio 2004), http://www.cert.org/csirts/.

[5] **ANDERSON, D. R. & SWEENEY, D. J.** (2008). "*Estadística para administración y economía.*" México, DF, Cengage Learning Latin America. (Isbn: 9789706868251). 10 ed., México, DF

[6] **AON, R. S.** (2010) "*Global Risk Managemente Survey*." (Consultado: Diciembre 2010), www.aon.com.

[7] **ARGONNE LABS, N. L. & CONZELMANN, G.** (2008). "*EMCAS: Electricity Market Complex Adaptive System*." (consultado Octubre 2010): http://www.dis.anl.gov/pubs/61084.pdf

[8] **ARGONNE LABS, N. L. & PEERENBOOM, J.** (2010). "*CEEESA Natural Gas Systems Analysis Tools*." (consultado Octubre 2010): http://www.dis.anl.gov/projects/NaturalGasAnalysisTools.html

[9] **ARGONNE LABS, N. L., PEERENBOOM, J., GILLETE, J.*, et al.*** (2007). "*CI3: Critical Infrastructures Interdependencies Integrator.*" (consultado Octubre 2010): http://www.ipd.anl.gov/anlpubs/2002/03/42598.pdf

[10] **ARGONNE LABS, N. L., SANDIA LABS, N. L. & LOS ALAMOS LABS, N. L.** (2008a). "*CIPDSS: Critical Infrastructure Protection Decision Support System.*" (consultado Octubre 2010): http://www.dis.anl.gov/pubs/63060.pdf

[11] **ARGONNE LABS, N. L., SANDIA LABS, N. L. & SYDELKO, P.** (2008b). "*TEVA: Threat Ensemble Vulnerability Assessment.*" U.S. Environmental Protection Agency's National Homeland Security Research Center. (consultado Octubre 2010): http://www.dis.anl.gov/projects/teva.html

[12] **ARROYO, J. M.** (2010). "*Análisis de Vulnerabilidad en Sistemas de Potencia.*" (consultado Noviembre 2011): http://www.dee.feis.unesp.br/lapsee/arquivos/down_materiaiscursos/2008_nataliajose/9_analisis_vulnerabilidad.pdf

[13] **AS/NZS** (1999). "*Estándar Australiano de Administración del Riesgo*. **AS/NZS 4360:1999:** 36 p.), www.netconsul.com/riesgos/ar.pdf.

[14] **AUSTRALIAN, F. G. & CSIRO, M., INFORMATICS AND STATISTICS**. (2008). "*CIPMA: Critical Infrastructure Protection Modeling and Analysis.*" (consultado Octubre 2010): http://www.csiro.au/partnerships/CIPMA.html

[15] BAGHERI, E. & GHORBANI, A. (2007) "*The State of the Art in Critical Infrastructure Protection: a Framework for Convergence*." New Brunwick University, (Consultado: Mayo 2007), http://glass.cs.unb.ca/~ebrahim/papers/CIPFramework.pdf.

[16] BAIARD, F., SALA, G. & SGANDURA, D. (2007). "*VINCI: Managing Critical Infrastructures through Virtual Network Communities.*" Second International Workshop, CRITIS 2007, Málaga (España), Universidad de Pisa (Italia). Consultado: http://www.springerlink.com/content/gj10397l44q27h18/

[17] BARABÁSI, A.-L. & ALBERT, R. (1999). "*Emergence of Scaling in Random Networks*." Science: Vol:**286**: (#*5439*): 509-512, (1095-9203) http://es.wikipedia.org/wiki/Red_libre_de_escala

[18] BATAGELJ, V. & MRVAR, A. (2002). "*Pajek - Analysis and Visualization of Large Networks*." Liubliana, Eslovenia. (Isbn, Liubliana, Eslovenia. 477

[19] BELLUCK, D., HULL, R., BENJAMIN, S.*, et al.* (2006). "*Environmental Security, Critical Infrastructure And Risk Assessment: Definitions And Current Trends*.), http://www.springerlink.com.

[20] BELLUCK, D., HULL, R., BENJAMIN, S.*, et al.* (2007). "*Environmental Security, Critical Infrastructure And Risk Assessment: Definitions And Current Trends*.**"** Environmental Security in Harbors and Coastal Areas, Linkov, I, et al. (eds.) Springerlink**:** pp. 3 - 17.), http://www.springerlink.com.

[21] BESCANSA, M. (2007). "*Operación Óptima en Sistemas de Gas y Electricidad.*" Proyecto de Fin de Carrera. Ingeniería Industrial en Eléctrica. Madrid, Universidad Pontifica de Comillas. **Ingeniería Industrial con énfasis en Eléctrica:** 166p.

[22] BEYELER, W. & BROWN, T. (2004). "*Assessing Economic Impacts of Infrastructure Disruptions : Comparison of Input/Output and System Dynamics Approaches*." Proceedings of the 22nd International Conference of the System Dynamics Society, Oxford, England, The System Dynamics Society.

[23] BEYELER, W., BROWN, T. & CONRAD, S. H. (2002). "*A Modular Dynamic Simulation Model of Infrastructure Interdependencies*." Proceedings of the 20th International Conference of the System Dynamics Society, Palermo, Italy, The System Dynamics Society.

[24] BOE (2011a). "*Ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas.* Madrid (Spain)**:** 11p), http://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf.

[25] BOE (2011b). "*Real Decreto 704/2011, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.* Madrid (España)**:** 18p), http://www.cnpic-es.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf.

[26] BOMPARD, E., CIWEI, G., NAPOLI, R.*, et al.* (2009). "*Risk Assessment of Malicious Attacks Against Power Systems*." IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans: Vol:**39**: (#*5*): 1074-1085, (1083-4427

[27] BRANCUCCI, C., BOLADO, R., DE VRIES, L.*, et al.* (2012). "*European power grid reliability indicators, what do they really tell?*" Electric Power Systems Research: Vol:**90**: (#*1*): 79-84, (0378-7796) http://www.sciencedirect.com/science/article/pii/S0378779612001071

[28] BROADWATER, R. (2006). "*DEW: Distributed Engineering Workstation*." (consultado Octubre 2010): http://www.edd-us.com/

[29] BROWN, T. (2007). "*Multiple Modeling Approaches and Insights for Critical Infrastructure Protection.*" En, IOS Press, NATO Series for Peace and Security Services. **13:** pp. 23-35.

[30] BSI. (2011). "*Bundesamt für Sicherheit in der Informationstechnik*." (consultado May, 2011): http://www.bsi.bund.de/

[31] BUITRAGO, O. & TAUTA, D. (2008). "*Análisis del sistema de transporte nacional de energía colombiano desde el punto de vista de redes complejas.*" Tesis en Ingeniería Eléctrica. Bogotá, Universidad Nacional de Colombia. **Bs Ingeniería Eléctrica:** 85p.

[32] CANADIAN. (2011). "*Public Safety Canada*." (consultado January, 2011): http://www.publicsafety.gc.ca/

[33] CCN-CERT. (2011). "*Centro de Incidentes del Centro Seguridad de la Información del Centro Criptológico Nacional* ", (consultado Enero 2011): www.ccn-cert.cni.es

[34] CCN CRIPTOLOGÍA, C. N. (2010). "*MARGERIT: METODOLOGIA DE ANALISIS Y GESTION DE RIESGOS DE LOS SISTEMAS DE INFORMACION DE LAS ADMINISTRACIONES PÚBLICAS*." (consultado Octubre 2010): http://www.csi.map.es/csi/pg5m20.htm

[35] **CE- EUROPA, C. D. L. C.** (2005). "*Libro Verde: Sobre un Programa Europeo para la Protección de Infraestructuras Críticas*." Comisión de las Comunidades Europeas. Bruselas (Bélgica)**:** 28p.

[36] **CE**. (2006). "*Síntesis de la legislación de la UE: Lucha contra el terrorismo*." (consultado Agosto 2010): http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_es.htm

[37] **CERT-CCIT**. (2011). "*Centro de Coordinación Informática Colombia*." (consultado Enero 2011): www.cert.org.co

[38] **CERT.BR**. (2011). "*Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil*." (consultado Enero 2011): www.cert.br

[39] **CNA, M. A. B.** (2009) "*Powering America's Defense: Energy and the Risks to National Security*." Washington, DC (EEUU), (Consultado), http://www.cna.org/sites/default/files/Powering%20Americas%20Defense.pdf.

[40] **CNCERT/CC**. (2011). "*Computer Emergency Response Teams within China*." (consultado May, 2011): http://www.cert.org.cn/english_web/index.htm

[41] **CNPIC**. (2010). "*Centro Nacional de Protección de Infraestructuras Críticas en España*." (consultado Agosto 2010): http://www.cnpic-es.es/cnpic/

[42] **CONSOLINI, T.** (2009). "*Regional security assessments: A strategic approach to securing federal facilities.*" Master Thesis. Naval Postgraduate School. Monterey - California (EEUU)**:** 103p.

[43] **COSO** (2004) "*Enterprise Risk Management – Integrated Framework*." (Consultado), www.coso.org.

[44] **COURSAGET, A. & (SGDSN), S. G. F. D. A. N. S.** (2010). "*SAIV: Security of Activities of Vital Importance* F. S. G. f. D. a. N. Security. Paris (Francia).

[45] **CPNI**. (2011). "*Centre for the Protection of National Infrastructure*." (consultado Enero 2011): www.cpni.gov.uk

[46] **CUE** (2008). "*Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección*." Consejo de la Unión Europea. Bruselas. **Directiva 114/CE:** 24p.

[47] **CURTIS, P.** (2007). "*Maintaining Mission Critical Systems in a 24/7 Environment.*" Rosenwood, MA (EEUU), IEEE Press. (Isbn: 9780771683742, Rosenwood, MA (EEUU). 484p

[48] **CHEN, G., DONG, Z. Y., HILL, D. J., *et al.*** (2009). "*An improved model for structural vulnerability analysis of power networks*." Physica A: Statistical Mechanics and its Applications: Vol:**388**: (#*19*): 4259-4266, (0378-4371) http://www.sciencedirect.com/science/article/pii/S0378437109004804

[49] **CHEN, G., DONG, Z. Y., HILL, D. J., *et al.*** (2010). "*Attack structural vulnerability of power grids: A hybrid approach based on complex networks*." Physica A: Statistical Mechanics and its Applications: Vol:**389**: (#*3*): 595-603, (0378-4371) http://www.sciencedirect.com/science/article/pii/S0378437109008164

[50] **CHEN, G., ZHAO, D., HILL, D. J., *et al.*** (2011). "*Exploring Reliable Strategies for Defending Power Systems Against Targeted Attacks*." Power Systems, IEEE Transactions on: Vol:**26**: (#*3*): 1000-1009, (0885-8950

[51] **DODRILL, K., GARRETT, J. H., MATTHEWS, S., *et al.*** (2007). "*Knowledge Management and Visualization in Support of Vulnerability Assessment of Electricity Production.*" Transportation Research Board 86th Annual Meeting, Washington DC, Transportation Research Board 86th Annual Meeting. Consultado: http://pubsindex.trb.org/view.aspx?id=802270

[52] **DONZELLI, P. & SETOLA, R.** (2007). "*Identifying and evaluating risks related to enterprise dependencies: a practical goal-driven risk analysis framework*." International Journal of Risk Assessment and Management: Vol:**7**: (#*8*): pp. 1120 - 1137, (1741-5241) http://inderscience.metapress.com/openurl.asp?genre=article&eissn=1741-5241&volume=7&issue=8&spage=1120

[53] **DRABBLE, B., BLACK, T., KINZIG, C., *et al.*** (2009). "*Ontology Based Dependency Analysis: Understanding the Impacts of Decisions in a Collaborative Environment.*" IEEE Collaborative Technologies and Systems, 2009., New Brunswick (Canadá), University of New Brunswick

[54] **EC** (2011a) "*A Reference Security Management Plan for Energy Infrastructure*." Prepared by the Harnser Group for the European Commission, Norwich (Inglaterra), (Consultado), www.prismworld.com.

[55] **EC**. (2011b). "*Thematic Network on Critical Energy Infrastructure Protection (TNCEIP)*." (consultado February, 2011): http://ec.europa.eu/energy/infrastructure/critical_en.htm

[56] **ENEA, EUROPA, C. D. L. C. & BOLOGNA, S.** (2010). "*MIA: Methodology for Interdependencies Assessment*." (consultado Octubre 2010): http://www.progettoreti.enea.it/mia/

[57] ERA, S. S. (2010). "*ERA: Enterprise Risk Administration (GAMS Software)*." (consultado Octubre 2010): http://www.gams.org/home/

[58] ERM INITIATIVE, N. C. U. (2010). "*Strengthening Enterprise Risk Management for Strategic Advantage*." Committee of Sponsoring Organizations of the Treadway Commission (COSO), (consultado Noviembre 2010): http://mgt.ncsu.edu/erm/

[59] ERNST & YOUNG, A. (2009) "*The top 10 risks for business: A sector-wide view of the risks facing businesses across the globe*." 48p, (Consultado: Diciembre 2010), www.ey.com/businessrisk2010.

[60] EZELL, B. C., V., F. J. & WIESE, I. (2000). "*Infrastructure Risk Analysis of Municipal Water Distribution System*." Journal of Infrastructure Systems: Vol:**6**: (#*3*): 118-122) http://link.aip.org/link/?QIS/6/118/1

[61] FERIGATO, C. & MASERA, M. (2007). "*Design of a Platform for Information Exchange on Protection of Critical Infrastructures.*" Second International Workshop, CRITIS 2007, Málaga (España), JCR (Joint Research Centre of European Commission). Consultado: http://www.springerlink.com/content/978-3-540-89095-9#section=698877&page=1&locus=0

[62] GHORBANI, A. & MARSH, S. (2004). "*AIMS: Agent-Based Infrastructure Modeling and Simulation*." (consultado Octubre 2010): http://iit-iti.nrc-cnrc.gc.ca/colloq/0405/04-11-04_e.html

[63] GIROUX, J. A. (2010). "*A Modern Twist: The Evolution of Energy Infrastructure Attacks*." Energy Security and Critical Infrastructures: Threats, Risks and Interdependencies, Davos (Suiza), Organization for Security and Co-operation in Europe (OSCE). 7p.

[64] GLEICH, D. (2008). "*MATLAB_BGL: Graph Theory Toolbox*."): http://www.mathworks.com/matlabcentral/fileexchange/10922

[65] GÓMEZ-EXPÓSITO, A. (2002). "*Análisis y operación de sistemas de energía eléctrica.*" Madrid, McGraw-Hill. (Isbn: 9788448135928, Madrid

[66] GROSS, J. L. & YELLEN, J. (2004). "*Handbook of graph theory*, CRC Press. (Isbn: 9781584880905. 1167p

[67] HAIDAR, A. M. A., MOHAMED, A. & HUSSAIN, A. (2007). "*Vulnerability Assessment of a Large Sized Power System Using Radial Basis Function Neural Network.*" 5th Student Conference on Research and Development, 2007. (SCOReD 2007).

[68] HAIDAR, A. M. A., MOHAMED, A., HUSSAIN, A.*, et al.* (2008). "*Vulnerability assessment and control of large scale interconnected power systems using neural networks and neuro-fuzzy techniques.*" Power Engineering Conference, 2008. AUPEC '08. Australasian Universities

[69] HAMILTON, C. (1999). "*Risk Management and Security*." Information Security Journal: A Global Perspective: Vol:**8**: (#*2*): pp 69 - 78) http://www.informaworld.com/smpp/content~content=a768426563&db=all

[70] HOLMGREN, A. (2007a). "*A framework for Vulnerability Assesment of Electric Power Systems.*" En: Critical infrastructure: reliability and vulnerability. A. T. MURRAY & T. H. GRUBESIC. Berlin (Alemania), Springer Verlag.

[71] HOLMGREN, A. (2007b). "*Quantitative Vulnerability Analysis of Electric Power Networks.*" Department of Measurement Technology and Industrial Electrical Engineering. Estocolmo (Suecia), Royal Institute of Technology. **Doctoral Thesis in Safety Analysis:** 47p.

[72] HOLMGREN, Å. J. (2006). "*Using Graph Models to Analyze the Vulnerability of Electric Power Networks*." Risk Analysis: Vol:**26**: (#*4*): 955-969, (1539-6924) http://dx.doi.org/10.1111/j.1539-6924.2006.00791.x

[73] HOLMGREN, A. J., JENELIUS, E. & WESTIN, J. (2007). "*Evaluating Strategies for Defending Electric Power Networks Against Antagonistic Attacks*." Power Systems, IEEE Transactions on: Vol:**22**: (#*1*): 76-84, (0885-8950

[74] HULL, R., BELLUCK, D. & LIPCHIN, C. (2006) "*A framework for multi-criteria decisionmaking with special reference to critical infrastructure: policy and risk management working group summary and recommendations*." (Consultado), http://www.springerlink.com.

[75] ICONTEC (2004). "*Norma Técnica Colombiana para 5254 la Gestión de Riesgos*.**"** Norma Técnica Colombiana NTC 5254**:** 44p.

[76] IDAHO, N. L. & DUDENHOEFFER, D. (2006). "*CIMS: Critical Infrastructure Modeling System*." (consultado Octubre 2010): http://www.inl.gov/research/critical-infrastructure-modeling/

[77] **IEA** (2002) "*Security of supply in electricity markets*." IEA INFORMATION PAPER, 177p, (Consultado: Agosto 2010), http://www.iea.org/.

[78] **IEEE-GROUP**. (1973). "*Common Format For Exchange of Solved Load Flow Data*." Power Apparatus and Systems, IEEE Transactions on, (consultado 6): http://www.ee.washington.edu/research/pstca/

[79] **INTEPOINT, T. L. & ARMSTRONG, M.** (2010). "*IntePoint Vu: Critical Infrastructure Integration Modeling and Simulation*." (consultado Octubre 2010): http://intepoint.com/products/index.html

[80] **ISA**. (2009). "*Política para la gestión integral de riesgos grupo empresarial ISA*." Documentos ISA, (consultado Agosto 2010): http://www1.isa.com.co/irj/go/km/docs/documents/ContenidoInternetISA/ISA

[81] **ISAGEN**. (2009). "*Mapa de Riesgos ISAGEN*." Documentos ISAGEN, (consultado Agosto 2010): www.isagen.com.co

[82] **ISO**. (2010). "*Norma ISO 31000, para la Gestión de Riesgos*." (consultado Octubre 2010): http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170

[83] **ISOGRAPH INC**. (2008). "*Hazop+: Hazard and Operability Study*." (consultado Octubre 2010): http://www.isograph-software.com/index.htm

[84] **ISOGRAPH INC**. (2010). "*FaultTree+: Fault Tree Analysis*." (consultado Octubre 2010): http://www.faulttree.org/

[85] **JEBARAJ, S. & INIYAN, S.** (2006). "*Review of Energy Models*." Renewable and Sustainable Energy Reviews: Vol:**10**: (#*4*): pp 281-311

[86] **JELENIUS, E.** (2004). "*Graph Models of Infrastructures and the Robustness of Power Grids.*" Master Thesis. Center for Safety Research. Stockholm (Sweden), Royal Institute of Technology (KTH). **Master of Science in Physics Engineering:** 89p.

[87] **JOHANSSON, J.** (2010). "*Risk and Vulnerability Analysis of Interdependent Technical Infrastructures.*" Department of Measurement Technology and Industrial Electrical Engineering. Lund (Suecia), Universidad de Lund. **Doctorado en Automatización Industrial:** 189p.

[88] **JP-MORGAN** (1999) "*Corporate Metrics*." Technical Document, New York (EE.UU), (Consultado: Abril, 1999), http://www.riskmetrics.com.

[89] **KNIGHT, U. G.** (2001). "*Power Systems in Emergencies.*" Chichester (Inglaterra), John Wiley & Sons. (Isbn: 0471-490164, Chichester (Inglaterra). 378p.

[90] **KRCERT/CC**. (2011). "*Korea Internet Security Center*." (consultado May, 2011): http://www.krcert.or.kr/index.jsp

[91] **LATORA, V. & MARCHIORI, M.** (2001). "*Efficient Behavior of Small-World Networks*." Physical Review Letters: Vol:**87**: (#*19*): 198701) http://link.aps.org/doi/10.1103/PhysRevLett.87.198701

[92] **LE COQ, C. & PALTSEVA, E.** (2009). "*Measuring the security of external energy supply in the European Union*." Energy Policy: (#*37*): pp 4474-4481

[93] **LEE, M.** (2001). "*A Dynamic Systems Simulation Approach to Risk Mitigation for Critical Infrastructure at the United States Military Academy*." Proceedings of the 19th International Conference of the System Dynamics Society, Atlanta, Georgia, System Dynamics Society.

[94] **LEWIS, T.** (2006). "*Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.*" New Jersey, Wiley-Interscience. (Isbn: 0471786284, New Jersey. 474p.

[95] **LI, J., ZLATANOVA, S., FABBRI, A. G.*, et al.*** (2007). "*Challenges for the Application of GIS Interoperability in Emergency Management.*" En: Geomatics Solutions for Disaster Management. W. Cartwright, G. Gartner, L. Meng & M. P. Peterson, Springer Berlin Heidelberg**:** 389-405.

[96] **LÓPEZ, B. & ARBOLEDA, D.** (2010) "*Integración del manejo de riesgo e incertidumbre en la planeación financiera de empresas de transporte de energía.*" Revista CIER **54**, pp. 80-88, (Consultado: 2010), http://sg.cier.org.uy/Publicaciones/revista.nsf/0a293b20eacdf8a903257133003ea67d/a8a631cacd395ea5832576ef00650443/$FILE/IntegraciondelManejo_10.pdf.

[97] **LOS ALAMOS LABS, N. L. & FLAIM, S.** (2006). "*FinSim: Financial System Infrastructure*." (consultado Octubre 2010): http://cnls.lanl.gov/annual26/abstracts.html

[98] **LOS ALAMOS LABS, N. L. & HOLLAND, J.** (2008). "*WISE: Water Infrastructure Simulation Environment*." (consultado Octubre 2010): http://www.lanl.gov/programs/nisac/wise.shtml

[99] LOS ALAMOS LABS, N. L. & MICHELSEN, R. (2008). "*UIS: Urban Infrastructure Suite*." (consultado Octubre 2010): http://www.nemaweb.org/default.aspx?3435

[100] LOS ALAMOS LABS, N. L., SANDIA LABS, N. L. & HOLLAND, J. (2006). "*IEISS: Interdependent Energy Infrastructure Simulation System*." (consultado Octubre 2010): http://www.sandia.gov/nisac/ieiss.html

[101] LOS ALAMOS LABS, N. L. & SMITH, J. (1999). "*TRANSIMS: TRansportation ANalysis SIMulation System*." (consultado Octubre 2010): http://transims-opensource.net/

[102] LÖSCHEL, A., MOSLENER, U. & RÜBBELKE, D. (2010). "*Energy security-concepts and indicators*." Energy Policy: (#*38*): pp 1607-1608

[103] MACAULAY, T. (2008). "*Critical infrastructure: understanding its component parts, vulnerabilities, operating risks, and interdependencies.*" Boca Ratón (FL), EEUU, CRC Press. (Isbn: 9781420068351, Boca Ratón (FL), EEUU. 320p

[104] MAÑAS, A. L. H. (2007). "*PILAR: PROCEDIMIENTO INFORMATICO Y LOGICO DE ANALISIS DE RIESGOS*." (consultado Octubre 2010): http://www.ar-tools.com/index.html?tools/pilar/index.html

[105] MCMANUS, J., BAKER, G., REDWINE, S.*, et al.* (2004). "*NSRAM: Network Security Risk Assessment Model*." (consultado Octubre 2010): http://www.jmu.edu/iiia/webdocs/Reports/NSRAM%20IIIA%20TP%2004-01.pdf

[106] MILANO, F. (2003). "*Pricing System Security in Electricity Market Models with Inclusion of Voltage Stability Constraints.*" Department of Electrical Engineering. Génova (Italia), University of Genova. **Doctorado en Ingeniería Eléctrica:** 218p.

[107] MILANO, F. (2005). "*An Open Source Power System Analysis Toolbox*." Power Systems, IEEE Transactions: Vol:**20**: (#*3*): 1199-1206, (0885-8950

[108] MILANO, F. (2009). "*Continuous Newton's Method for Power Flow Analysis*." Power Systems, IEEE Transactions on: Vol:**24**: (#*1*): 50-57, (0885-8950

[109] MILANO, F. (2012). "*PSAT: Power System Analysis Toolbox.*"): http://www.uclm.es/area/gsee/web/Federico/psat.htm

[110] MILULAK, R. (2004). "*The Basics of FMEA*." (consultado Octubre 2010): http://www.fmea-fmeca.com/

[111] MINETUR, M. I. (2008). "*Planificación de los sectores de Electricidad y Gas: Desarrollo de las redes de transporte 2008-2016 en España*." Ministerio de Industria, Turismo y Comercio de España. Madrid), http://www.minetur.gob.es/energia/planificacion/Planificacionelectricidadygas/Desarrollo2008/DocTransportes/planificacion2008_2016.pdf.

[112] MOTTER, A. & LAI, Y. (2002). "*Cascade-based attacks on complex networks*." Physical Review E: Vol:**66**: (#*6*): 065102) http://dx.doi.org/10.1103/PhysRevE.66.065102

[113] MURRAY, A., MATISZIW, T. & GRUBESIC, T. (2007). "*Critical network infrastructure analysis: interdiction and system flow*." Journal of Geographical Systems: Vol:**9**: (#*2*): 103-117, (1435-5930) http://dx.doi.org/10.1007/s10109-006-0039-4

[114] NATIONAL INFRASTRUCTURE INSTITUTE, C. I. E. & PEIMER, R. (2010). "*CARVER2: Critical Infrastructure Risk Assessment Tool*." (consultado Octubre 2010): http://www.ni2cie.org/CARVER2.asp

[115] NAVI. (2011). "*Nationaal Adviescentrum Vitale Infrastructuur*." (consultado Enero 2011): http://www.navi-online.nl

[116] NESS, L. (2006). "*Securing Utility and Energy Infrastrucures.*" Washington DC (EEUU). (Isbn, Washington DC (EEUU). 340p

[117] NEWMAN, D. E., NKEI, B., CARRERAS, B. A.*, et al.* (2005). "*CASCADE: Risk Assessment in Complex Interacting Infrastructure Systems.*" IEEE 38th Conference on System Sciences, Big Island Hawaii, (EEUU), University of New Brunswick. Consultado: http://eceserv0.ece.wisc.edu/~dobson/PAPERS/newmanHICSS05.pdf

[118] NEWMAN, M. E. J. (2003). "*The Structure and Function of Complex Networks*." SIAM Review: Vol:**45**: (#*2*): 167-256) http://www-personal.umich.edu/~mejn/courses/2004/cscs535/review.pdf

[119] NIPP (2009). "*National Infraestructure Protection Plan. US Department of Homeland Security*." U.S. Department of Home Security. Washington DC (EEUU)**:** 175 p), www.dhs.gov/nipp.

[120] OAK RIDGE, N. L., JOHNSON, P. & MICHELHAUGH, R. (2003). "*TRAGIS: Transportation Routing Analysis Geographic Information System*." (consultado Octubre 2010): https://tragis.ornl.gov/TRAGISmanual.pdf

[121] **OGC**. (2002). "*Critical Infrastructure Protection Initiative, Phase 2*." (consultado Octubre 2010): http://www.opengeospatial.org/projects/initiatives/cipi2

[122] **ONTI**. (2011). "*Oficina Nacional de Tecnologías de Información*." (consultado May, 2011): http://www.sgp.gov.ar/contenidos/onti/onti.html

[123] **PANZIERI, S., SETOLA, R. & ULIVI, G.** (2005) "*CISIA: Critical Infrastructure Simulation by Interdependent Agents*." (Consultado: Noviembre 2005), http://www.dia.uniroma3.it/~panzieri/Articoli/WorldIFAC05-CIIP.pdf.

[124] **PEGGION, M., BERNARDINI, A. & MASERA, M.** (2008) "*ECI-GIS: GEOGRAPHIC INFORMATION SYSTEMS AND RISK ASSESSMENT*." 53p, (Consultado: Enero 2008), http://publications.jrc.ec.europa.eu/repository/handle/111111111/4934.

[125] **PENGCHENG, Z., SRINIVAS, P. & TERRY, F.** (2005). "*MIN: Dynamic Game Theoretic Model of Multi-Layer Infrastructure Networks*." Networks and Spatial Economics, : Vol:**5**: pp. 147-178) citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.133.5260

[126] **PMI** (2004). "*Guía de los Fundamentos de la Dirección de Proyectos*.**"** PMBOK 3. P. M. INSTITUTE. Pensilvania (EEUU)**:** 409p.), www.pmi.org.

[127] **PORTANTE, E. C., CRAIG, B. A. & FOLGA, S. M.** (2007). "*NGfast: a simulation model for rapid assessment of impacts of natural gas pipeline breaks and flow reductions at u.s. state borders and import points* " IEEE Simulation Conference, 2007 Winter, Washington DC (EEUU), Argonne National, Laboratory.

[128] **PRAGMA, L.** (2010). "*CERO: Control Estratégico del Riesgo*." (consultado Octubre 2010): http://www.riesgoscero.com/

[129] **PRUYT, E. & WIJNMALEN, D.** (2010). "*National Risk Assessment in The Netherlands*." Multiple Criteria Decision Making for Sustainable Energy and Transportation Systems: Vol:**634**: pp. 133-143, (978-3-642-04045-0) www.springerlink.com/index/l60t423960560140.pdf

[130] **QIMING, C. & MCCALLEY, J. D.** (2005). "*Identifying high risk N-k contingencies for online security assessment*." Power Systems, IEEE Transactions on: Vol:**20**: (#*2*): 823-834, (0885-8950

[131] **QUARLES, L. R. & HAIMES, Y. Y.** (2007). "*IIM: Inoperability Input-Output Model*." (consultado Octubre 2010): http://www.thei3p.org/docs/publications/IIM-factsheet-Feb2007.pdf

[132] **RADVANOVSKY, R. & MC-DOUGALL, A.** (2010). "*Critical infrastructure: homeland security and emergency preparedness.*" Boca Ratón (FL) - EEUU, Taylor and Francis. (Isbn: 9781420095272, Boca Ratón (FL) - EEUU. 318p

[133] **REE** (2009). "*Mapas de la red eléctrica de transporte."* Red Eléctrica de España S.A http://www.ree.es/transporte/mapa_red_transporte.asp

[134] **REE**. (2012a). "*El sistema de transporte eléctrico español*." Avance del informe 2011. - Red Eléctrica de España S.A 2009.): http://www.ree.es/transporte/transporte.asp

[135] **REE** (2012b). "*Mapas de la red eléctrica de transporte."* Red Eléctrica de España S.A, Madrid http://www.ree.es/transporte/mapa_red_transporte.asp

[136] **ROSAS I CASALS, M.** (2009). "*Topological Complexity of the Electricity Transmission Network. Implications in the Sustainability Paradigm.*" Departmento de Ingeniería Eléctrica. Barcelona (España), Universitat Politècnica de Catalunya. **Cátedra UNESCO de Sostenibilidad:** 134p.

[137] **SAATY, T. L.** (2008). "*Decision making with the analytic hierarchy process*." International Journal of Services Sciences: Vol:**1**: (#*1*): 83-98, (1753-1446) http://inderscience.metapress.com/link.asp?id=02t637305v6g65n8

[138] **SALMERON, J., WOOD, K. & BALDICK, R.** (2004). "*Analysis of electric grid security under terrorist threat*." Power Systems, IEEE Transactions on: Vol:**19**: (#*2*): 905-912, (0885-8950

[139] **SANDIA LABS, N. L., BARTON, D. C., EIDSON, E. D.,** ***et al.*** (2004). "*COMM-ASPEN: Simulating Economic Effects of Disruptions in the Telecommunications Infrastructure*." (consultado Octubre 2010): http://cfwebprod.sandia.gov/cfdocs/CCIM/docs/

[140] **SANDIA LABS, N. L. & BROWN, T.** (2005a). "*FAIT: Fast Analysis Infrastructure Tool*." (consultado Octubre 2010): http://www.sandia.gov/nisac/fait.html

[141] SANDIA LABS, N. L. & BROWN, T. (2005b). "*N-ABLE: Agent-Based Laboratory for Economics*." (consultado Octubre 2010): http://www.sandia.gov/mission/homeland/factsheets/nisac/NISAC_N-ABLE_factsheet.pdf

[142] SCHNEIDER, K. P. (2005). "*Analysis of Critical Infrastructure Interactions.*" Tesis de Doctorado en Ingeniería Eléctrica. Washington DC (EEUU), University of Washington. **Doctor in Philosophy:** 174.

[143] SGDSN. (2011). "*Secrétariat General de la Défense Nationale*." (consultado Enero 2011): www.sgdn.gouv.fr

[144] SOLÉ, R., CASALS, M., MURTRA, B.*, et al.* (2008). "*Robustness of the European power grids under intentional attack*." Physical Review E: Vol:**77**: (#2): 026102) http://dx.doi.org/10.1103/PhysRevE.77.026102

[145] SPARTA INC, GOODWIN, B. L. & LEE, L. (2005). "*NEMO: Net-Centric Effects-based operations MOdel.*" 2005 International Command and Control Research and Technology Symposium: The Future of Command and Control, San Diego, CA (EEUU), SPARTA. Consultado: http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/128.pdf

[146] SULLIVANT, J. & NEAVE, E. H. (2007). "*Strategies for protecting national critical infrastructure assets: a focus on problem-solving.*" New Jersey, Wiley. (Isbn: 9780471799269, New Jersey. 607p

[147] UPME (2012). "*Plan de Expansión de referencia Generación - Transporte 2010-2024*." Ministerio de Minas y Energía de Colombia. Bogotá), http://www1.upme.gov.co/index.php/servicios-de-informacion/publicaciones/category/1-energia.html#.

[148] US DEPT ENERGY OFFICE (2002). "*Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities*." U.S. Department of Energy, Office of Energy Assurance. Washington DC. EEUU. **1:** 26p.), http://www.esisac.com/publicdocs/assessment_methods/Risk_Management_Checklist_Small_Facilities.pdf .

[149] US DEPT HOME SECURITY (2003). "*Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*.**"** U.S. Department of Homeland Security.), http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.

[150] US DEPT HOME SECURITY (2009a). "*Critical infrastructure and key resources sectors*." U.S. Department of Homeland Security. Washington DC (EEUU)), http://www.dhs.gov/xprevprot/programs/gc_1189168948944.shtm.

[151] US DEPT HOME SECURITY (2009b). "*Interim integrated risk management framework*." U.S. Department of Homeland Security. Washington DC (EEUU).

[152] US DEPT HOME SECURITY & OFFICE, U. D. E. (2007). "*Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan (Redacted)*." (U.S. Department of Homeland Security & U.S. Department Energy Office). Washington DC (EEUU)), http://www.dhs.gov/files/programs/gc_1179866197607.shtm.

[153] USACE, ERDC & CERL (2010). "*Fort Future.*" En. M. Applications, US Army Corps of Engineers, Engineer Research and Development Center, Construction Engineering Research Laboratory. **October, 2010**.

[154] VALERO, A. (2008). "*Estudio de la evolución exergética del capital mineral de la tierra*." Tesis Doctoral. . Zaragoza, Universidad de Zaragoza**:** 260p.

[155] WANG, K., ZHANG, B.-H., ZHANG, Z.*, et al.* (2011). "*An electrical betweenness approach for vulnerability assessment of power grids considering the capacity of generators and load*." Physica A: Statistical Mechanics and its Applications: Vol:**390**: (#23): 4692-4701, (0378-4371) http://www.sciencedirect.com/science/article/pii/S0378437111005784

[156] WATTS, D. J. & STROGATZ, S. H. (1998). "*Collective dynamics of 'small-world' networks*." Nature: Vol:**393**: (#6684): 440-442, (0028-0836) http://dx.doi.org/10.1038/30918

[157] WEFORUM (2010) "*Global Risks 2010: A Global Risk Network Report*." World Economic Forum, (Consultado: Enero 2010), www.weforum.org.

[158] XM. (2009). "*Mapa de Riesgos XM*." (consultado Mayo 2010): http://www.xm.com.co/Pages/MapadeRiesgos.aspx

[159] XM. (2012). "*Descripción del Sistema Eléctrico Colombiano*." (consultado Abril 2012): http://www.xm.com.co/Pages/DescripciondelSistemaElectricoColombiano.aspx

[160**] YUSTA, J. M.** (2008). "*Amenazas a la seguridad del suministro energético español*." Inteligencia y seguridad. Revista de análisis y prospectiva: (#*6*)

[161**] YUSTA, J. M.** (2009). "*Amenazas a la seguridad del suministro energético español*." Inteligencia y seguridad. Revista de análisis y prospectiva: (#*6*): pp 223-248, (1887-293X-n6) http://www.plazayvaldes.es/libro/inteligencia-y-seguridad-revista-de-analisis-y-prospectiva-no-6/1329/

[162**] YUSTA, J. M., CORREA, G. J. & LACAL-ARÁNTEGUI, R.** (2011). "*Methodologies and applications for critical infrastructure protection: State-of-the-art*." Energy Policy: Vol:**39**: (#*10*): pp. 6100-6119, (0301-4215) http://www.sciencedirect.com/science/article/pii/S0301421511005337

[163**] ZIELSTRA, A.** (2010). "*GOVCERT: Cybercrime Information Exchange.*" Cybersecurity and Critical Infrastructure Protection, Madrid (España). Consultado: http://www.govcert.nl/render.html?it=35

A. ANEXO A: PLATAFORMAS Y MODELOS PARA ESTUDIO DE VULNERABILIDADES EN INFRAESTRUCTURAS CRÍTICAS

Tabla A.1: Descripción de modelos y plataformas computacionales para estudio de vulnerabilidades en infraestructuras críticas

PLATAFORMA	ACRÓNIMO	DESCRIPCIÓN	DESARROLLO
AIMS	Agent-Based Infrastructure Modeling and Simulation	Herramienta de Software. Se proyectan las interdependencias de las infraestructuras críticas de un país. Inicialmente se ha concebido para evaluar la vulnerabilidad de acueductos en ciudades.	Universidad New Brunswick (Canadá). Patrocinado por National Research Council
ATHENA		Herramienta de software. Análisis de redes de infraestructuras interdependientes, incluyendo aspectos políticos, militares, económicos y sociales. Athena incorpora varios algoritmos sofisticados de razonamiento que permiten estudiar la dependencia entre los nodos.	On Target Technologies, Inc. Patrocinado por Laboratorios Nacionales de la Fuerza Aérea de EEUU.
CASCADE		Herramienta de Software. Fundamentado en probabilidad estadística para modelar fallos en cascada dentro de infraestructuras de transporte de electricidad.	
CARVER2	Criticality, Accessibility, Recoverability, Vulnerability, Espyability (Notoriety), Redundancy	Herramienta de software. Priorización de posibles objetivos terroristas en un sistema de infraestructuras, mediante la comparación de los activos clave en jurisdicciones.	National Infrastructure Institute Center for Infrastructure Expertise. Patrocinado por Departamento de Comercio de EEUU.
CEEESA	Center for Energy, Environmental, and Economic Systems Analysis	Herramientas de software. Análisis del mercado e infraestructura de Gas Natural, proyección del mercado de gas, flujos, pérdidas de nodos de redes de gas, Aislamiento de regiones y Vulnerabilidad de red	Centro de Aseguramiento de la Infraestructura. Patrocinado por Departamento de Defensa de los EEUU

PLATAFORMA	ACRÓNIMO	DESCRIPCIÓN	DESARROLLO
CERT/ CSIRT	Computer (Emergency) Security Incident Response Team	Metodología. Prevención, detección, asesoramiento, seguimiento y coordinación necesarios para hacer frente a incidentes de seguridad informática. (Detección de virus, gusanos y troyanos, aparición de intrusiones, actos malintencionados, terrorismo o ataques coordinados a infraestructuras desde Internet).	Universidad Carneggie Mellon y gobiernos en la Unión Europea, América Latina y Norteamérica
CI3	Critical Infrastructures Interdependencies Integrator	Herramienta de software. Estimación del tiempo y/o el costo de restaurar un componente o al conjunto completo de infraestructuras interdependientes para que vuelvan a funcionar con normalidad.	Argonne National Laboratories
CIMS	Critical Infrastructure Modeling System	Herramienta de software. Simulación de escenarios georeferenciados, para efectuar análisis de sensibilidad en la toma de decisiones. Se pueden evaluar las vulnerabilidades de la infraestructura, incluyendo políticas y planes de respuesta.	Idaho National Laboratories. Patrocinado por Laboratorios de la Fuerza Aérea de EEUU.
CIP/DSS	Critical Infrastructure Protection Decision Support System	Herramienta de software. Comparación de la eficacia de estrategias de reducción en la probabilidad que se manifieste un riesgo, a partir de la construcción de escenarios en los que se plasman los impactos, teniendo en cuenta los posibles afectados, las medidas de impacto y la probabilidad de un incidente.	Argonne National Laboratories
CIPMA	Critical Infrastructure Protection Modeling and Analysis	Herramienta de software. Evaluación de las relaciones y dependencias, mediante relaciones entre fallo específico en un sector y la afectación a las operaciones de infraestructuras críticas en otros sectores, para fijar direcciones en la política gubernamental de seguridad nacional.	Gobierno de Australia
CISIA	Critical Infrastructure Simulation by Interdependent Agents	Herramienta de software. Simulación a través de un conjunto de agentes interdependientes con relaciones no lineales, para analizar los efectos a corto plazo de los fallos en las infraestructuras, en términos de propagación de anomalías y degradación del funcionamiento del sistema. Muy útil en el análisis de origen y reacción ante emergencias.	Universidad New Brunswick (Canadá)
COMM-ASPEN	Agent-Based Simulation Model of the U.S. Economy	Herramienta de software. Simulación basada en agentes, sobre los efectos de las decisiones del mercado y de las interrupciones en la infraestructura de telecomunicaciones en la economía.	Sandia National Laboratories
DEW	Distributed Engineering Workstation.	Identificación y análisis de las interdependencias en grandes sistemas de energía eléctrica. También existen aplicaciones en sistemas de hidráulicos de barcos. (Gestión de activos, procedimientos de operación, eventos, planificación a corto y largo plazo).	Electrical Distribution Design, Inc. Patrocinado por Departamento de Energía y el Departamento de Defensa de los EEUU
DUTCH APPROACH		Metodología. Fundamentado en un sistema de Toma de Decisiones Multicriterio y se ha aplicado con éxito en un número limitado de eventos catastróficos. Se maximiza la reducción del riesgo y se relaciona con las preferencias políticas o preocupaciones de la sociedad.	Gobierno de Holanda
EAR-PILAR	Procedimiento Informático-Lógico para el Análisis de Riesgos	Herramienta de software. Caracterización de los activos (identificación, clasificación, dependencias y valoración), Caracterización de las riesgos, Evaluación de las salvaguardas. La herramienta evalúa el impacto y el riesgo, acumulado y repercutido, potencial y residual, presentándolo de forma que permita el análisis de por qué se da cierto impacto o cierto riesgo.	Centro Nacional de Criptología de España

PLATAFORMA	ACRÓNIMO	DESCRIPCIÓN	DESARROLLO
ECI-GIS	Geographic Information Systems and Risk Assessment	Herramienta de Software. Generación de modelos que predicen los efectos del daño o la pérdida de una infraestructura crítica para la continuidad de diversas operaciones. Proporciona una funcionalidad de precisión, para determinar la ubicación física de los activos críticos, la identificación y modelos de los riesgos potenciales y las vulnerabilidades asociadas a los desastres naturales o provocados por el hombre.	Joint Research Centre. Patrocinado por la Comisión Europea
EMCAS	Electricity Market Complex Adaptive System	Herramienta de software. Simulación mediante agentes, para investigar posibles impactos operativos y económicos en el sistema eléctrico, cuando es afectado por varios eventos externos.	Argonne National Laboratories. Patrocinado por ADICA Consulting
FAIT	Fast Analysis Infrastructure Tool	Herramienta de software. Contiene una base de conocimientos que incluye los datos actualizados del sistema (Censos, red de emergencias, georreferenciación, etc), así como el conocimiento de expertos sobre el funcionamiento y sobre las interacciones de la infraestructura.	Sandia National Laboratories. Patrocinado por Departamento de Seguridad Nacional de EEUU
FINSIM	Financial System Infrastructure	Herramienta de software. Representación del sector de los servicios financieros de EE.UU. como si fuera un sistema complejo descentralizado, con autonomía de la interacción de múltiples nodos de decisión, o agentes. Se aplica a escenarios de crisis que afectan el sistema de pago bancario y el uso del dinero plástico, así como el mercado de fondos federales y de las interacciones entre esas entidades.	Los Alamos National Laboratories. Patrocinado por Departamento de Seguridad Nacional de EEUU.
FMEA-FMECA	Failure Modes and Effects Analysis	Metodología. Procedimientos de análisis de fallos potenciales en un sistema de clasificación determinado por la gravedad o por el efecto de los fallos en el sistema. Ampliamente utilizada por empresas manufactureras en varias fases del ciclo de vida del producto, y también se usa en la industria de servicios. FMECA es una variante del FMEA.	
FORT-FUTURE		Herramienta de software. Ejecución de múltiples simulaciones dinámicas, evaluando un conjunto de alternativas. Adicionalmente, se soporta en sistema de información geográfica, para sistemas de transporte, energía eléctrica, sistemas de agua, etc.	Cuerpo de Ingenieros del Ejército de los EEUU, y actualmente su uso se limita a la estrategia militar
FTA	Fault Tree Analysis	Metodología. Técnica deductiva que se centra en un suceso accidental particular (riesgo) y proporciona un método para determinar las causas que desembocan en la manifestación de un riesgo dentro de un sistema. Proporciona resultados tanto cualitativos mediante la búsqueda de caminos críticos, como cuantitativos, en términos de probabilidad de fallos de componentes en un sistema.	
GAMS-CERO-ERA	Enterprise Risk Administration	Metodología. Estrategias de manejo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferencia del riesgo a otra parte, evasión del riesgo, reducción de los efectos negativos del riesgo, aceptación de algunas o todas las consecuencias de un riesgo particular, etc.	
GIS INTEROPERATIBILITY		Metodología. Utilización de los Sistemas de Información Geográfica, en la coordinación de emergencias y en el apoyo a la toma de decisiones.	Universidad de Waterloo (Canadá).

PLATAFORMA	ACRÓNIMO	DESCRIPCIÓN	DESARROLLO
GORAF		Herramienta de software. Identificación de los recursos más críticos dentro de una infraestructura. Se presentan métricas que representan las pérdidas económicas y métricas estratégicas que presentan el resultado del mal funcionamiento de un recurso. (Se suele combinar con la herramienta CISIA)	Universidad New Brunswick (Canadá)
INICIATIVAS GUBERNAMENTALES CERT		Metodología. Los equipos de trabajo en estas iniciativas están directamente ligadas a los ministerios de defensa en los países donde se implementan. Algunos casos de éxito en la implementación de estos programas se pueden consultar en el GOVCERT.nl (Holanda), COLCERT (Colombia), VENCERT (Venezuela), CERT.br (Brasil), Es-CERT (España), etc.	
HAZOP	Hazardous Operations	Metodología. Técnica de identificación de riesgos inductiva basada en la premisa de que los riesgos, los accidentes o los problemas de operabilidad, se producen como consecuencia de una desviación de las variables de proceso con respecto a los parámetros normales de operación en un sistema dado y en una etapa determinada.	
IEISS	Interdependent Energy Infrastructure Simulation System	Herramienta de software. Orientada especialmente a los infraestructuras de transporte de energía eléctrica y de gas natural, y simula el comportamiento dinámico, incluyendo las interdependencias entre los sistemas, permitiendo analizar las interacciones complejas, no lineales entre los sistemas de infraestructuras en áreas metropolitanas. El modelamiento se apoya en los sistemas multiagente.	Universidad de Virginia (EEUU)
IIM	Inoperability Input-Output Model	Herramientas de software. Modelos analíticos, para determinar el impacto de un ataque contra una infraestructura y los efectos en cascada en todas las demás infraestructuras interconectadas (en términos económicos y de operación). La herramienta permite representar la recuperación del sistema después de un ataque o de un evento y también permite realizar un análisis temporal del modo de recuperación.	Sandia National Laboratories y Los Alamos National Laboratories. Patrocinado por Departamento de Seguridad Nacional de EEUU .
INFRASTRUCTURE DISRUPTIONS		Herramienta de software. Modelo con dinámica de sistemas para comprender los sistemas de infraestructura bajo condiciones inusuales, así como la evaluación de las potenciales consecuencias económicas.	
IRAM	Infrastructure Risk Analysis Model	Herramienta de software. Simulación de la asignación de recursos para mejorar la confiabilidad en un sistema de infraestructura interconectada. La metodología se basa en la identificación, clasificación y gestión de los riesgos extremos que amenazan a un sistema de infraestructura.	
INTEPOINT VU		Herramienta de software. Planeación de las respuestas ante eventos intencionales y no intencionales en infraestructuras, teniendo en cuenta el impacto social y los modelos de comportamiento de la población. (sistema multiagente, combinado con un sistema de información geográfica del área que se analiza).	Intepoint LLC. Patrocinado por Departamento de Defensa de EEUU
KNOWLEDGE MANAGEMENT & VISUALIZATION		Herramienta de Software. Análisis de vulnerabilidades asociadas con la entrega de combustible en las plantas de generación eléctrica, específicamente las entregas de carbón a las centrales eléctricas de EEUU.	Universidad Carneggie Mellon. Patrocinado por el Departamento de Energía de EEUU.
Teoría Grafos		Metodología. Permite establecer las relaciones entre cada uno de los nodos que componen un sistema de infraestructura de transporte terrestre o ferroviaria interconectada. (Fundamentada en la teoría de grafos)	Universidad de Lund (Suecia). Patrocinado por Agencia Internacional de la Energía

PLATAFORMA	ACRÓNIMO	DESCRIPCIÓN	DESARROLLO
MARGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información	Metodología. Protección de información digital, redes de datos y sistemas informáticos, con la finalidad de determinar cuánto valor está en juego y la importancia de proteger la información.	Consejo Superior de Administración Electrónica de España
MIA	Methodology for Interdependencies Assessment	Metodología. Identificación de interdependencias críticas de los sistemas que están sometidos a vulnerabilidades.	Comisión Europea
MIN	Multi-Layer Infrastructure Networks	Herramienta de Software. Combinación de la Teoría de Juegos con la simulación basada en agentes, aplicada a la Infraestructura de Transporte Terrestre, en un modelo de 3 capas	
MODULAR DYNAMIC MODEL		Herramienta de Software. Simulación de la interacción del sistema de infraestructura eléctrico en California, incluyendo la operación de los generadores, la transporte, la distribución, la comercialización de energía, y la entrega de combustible para los generadores de energía.	Sandia National Laboratories
MUNICIPAL	MUlti-Network Interdependent Critical Infrastructure Program for Analysis of Lifelines	Herramienta de software. Entendimiento de eventos perjudiciales que afectan la interdependencia de las infraestructuras civiles, y la respuesta ante eventos de interrupción de la prestación de servicios de salud, seguridad y bienestar económico de sus ciudadanos. (Bases de datos con información de conexión de la infraestructura crítica, y sistema de información geográfica).	Rensselaer Polytechnic Institute (EEUU)
N-ABLE	National Agent-Based Laboratory for Economics	Herramienta de software. Simulación distribuida con agentes, en tiempo real en áreas de infraestructura de transporte por carreteras, energía eléctrica.	Sandia National Laboratories y Los Alamos National Laboratories
NEMO	Net-Centric Effects-based operations Model	Herramienta de software. Realización de análisis de sensibilidad para tomar decisiones adecuadas, en casos de emergencias, y para facilitar el proceso de planeación de un sistema de infraestructuras, permitiendo otorgarle mayor cubrimiento al sistema. (Fundamentada en bases de datos con información de conexión de la infraestructura crítica, así como un sistema de información geográfica).	Sparta, Inc
NSRAM	Network Security Risk Assessment Model	Herramienta de software. Simulación de grandes redes y análisis en condiciones de fallos o averías estructurales. Se simula con precisión la gravedad de los fallos de la red, y se consideran las variables de reparación (tiempo, costo, prioridades de reparación).	Universidad James Madison
NGFAST		Herramienta de software. Permite realizar evaluaciones en el caso que falle un gasoducto, y las simulaciones dentro de la infraestructura crítica del sistema de gas.	Argonne National Laboratories
OGC CIPI	Critical Infrastructure Protection Initiative	Metodología. Manejo de emergencias a través de intercambio de datos a diferentes niveles en las entidades del gobierno, y notificación de alertas de emergencias.	Open Geospatial Consortium
PCI INFORMATION		Metodología. Iniciativa para estandarizar el sistema de comunicaciones entre las partes interesadas europeas y los organismos reguladores, contribuyendo a la creación de confianza mutua entre los actores involucrados.	Joint Research Centre. Patrocinado por la Comisión Europea
SAIV	Security of Activities of Vital Importance	Metodología. Iniciativa francesa de protección de infraestructura crítica, que se ha centrado en el diálogo entre el Estado y los operadores, la coherencia intersectorial y el Refuerzo de la seguridad como resultado de enfoque de prioridades.	Gobierno de Francia

PLATAFORMA	ACRÓNIMO	DESCRIPCIÓN	DESARROLLO
TEVA	Threat Ensemble Vulnerability Assessment	Herramienta de software. Análisis de vulnerabilidades en sistemas de distribución de agua potable, su impacto en la salud pública y las consecuencias económicas. La construcción de la herramienta incluye la evaluación de estrategias de mitigación de amenazas estos sistemas de infraestructura.	Argonne National Laboratories. Patrocinado por Agencia de Protección Ambiental de los EEUU.
TRAGIS	Transportation Routing Analysis Geographic Information System	Herramienta de software. Cálculo de rutas óptimas de transporte, incluso en caso de fallo dentro del sistema de carreteras y autopistas, con especial énfasis en el transporte de cargas con materiales peligrosos. (Predecesor de las aplicaciones que se encuentran en los actuales GPS para los automóviles).	Oak Ridge National Laboratories
TRANSIMS	TRansportation ANalysis SIMulation System	Herramienta de software. Simulación basada en agentes y en autómatas celulares, capaces de representar los movimientos de las personas o de los vehículos a través de las calles dentro de las zonas urbanas, lo cual permite analizar el sistema regional de transporte.	Los Alamos National Laboratories
UIS	Urban Infrastructure Suite	Herramientas de software. Simulación tanto del comportamiento de las infraestructuras urbanas, como el de sus habitantes, los efectos de las interdependencias, y la dinámica de sus interconexiones.	Los Alamos National Laboratories. Patrocinado por Departamento de Seguridad Nacional de EEUU.
UML.CI		Metodología. Modelo de configuración de arquitectura en red, inspirado en metamodelos de alto nivel para crear un perfil de un sistema de infraestructura, de manera que se documenten las mejores prácticas en la planeación y mantenimiento del sistema de infraestructura.	
USARMY RISK MITIGATION		Herramienta de software. Simulación de la gestión de la red infraestructura de agua dulce para el consumo en bases militares del ejército de EEUU, especialmente en los meses de verano.	Los Alamos National Laboratories
WISE	Water Infrastructure Simulation Environment	Herramienta de software. Apoyo en la evaluación de la infraestructura de acueductos, riego y alcantarillados, para predecir los daños que se infringen en el sistema de infraestructura a consecuencia de emergencias como incendios, atentados, desastres naturales y falta de agua, con especial utilidad en las áreas urbanas.	
VINCI	Virtual Interacting Network Community	Metodología. Arquitectura de gestión de redes de información de infraestructura crítica, en la que se asignan redes de máquinas virtuales, sistema de almacenamiento virtual y políticas.	Universidad de Pisa (Italia)

B. ANEXO B: PRIORIZACIÓN DE ACCIONES Y SALVAGUARDIAS PARA MITIGACIÓN DE RIESGOS EN PROTECCIÓN DE INFRAESTRUCTURAS DE TRANSPORTE EN ALTA Y MEDIA TENSIÓN

Tabla A.2: Priorización de acciones para la gestión de riesgos en sistemas de infraestructura de media y alta tensión

N°	RIESGO	PRIORIZACIÓN DE ACCIONES
1	Aumento de las cuentas por cobrar (Cobranzas)	Gestiones de cobro: Actuaciones judiciales y extrajudiciales, facturación de intereses de mora, negociación y firma de acuerdos de pago se busca disminuir el impacto financiero de los retrasos en los pagos por parte de los clientes. Cláusula de incumplimiento en contratos de conexión, buscando que se dé una atención adecuada y por tanto se disminuya el impacto de eventos de materialización del riesgo. Considera la suspensión del servicio. Cláusula de cargo por retiro incluida en los contratos de conexión con grandes consumidores (Privados) Análisis de estados financieros a los clientes nuevos de conexión Aplicación guía de provisión de cartera para cubrir pérdidas probables por impagos y cuentas atrasadas.
2	Financiación insuficiente	Agilización y aprobación de autorizaciones a niveles internos y externos, para la adquisición de los recursos financieros. Seguimiento a indicadores financieros de bancos prestamistas, alertas de crisis y noticias de impacto en el sector financiero. Gestión proactiva en la negociación de financiación, lo cual facilita el acceso oportuno a los recursos. Aplicación de metodologías de cuantificación de riesgos: Análisis de sensibilidad (EaR, CFaR, VaR) que permite cuantificar el riesgo puro y residual al que se encuentran expuestos los estados financieros. Seguimiento a los indicadores financieros de la empresa. Análisis permanente de las variables macroeconómicas, que contribuye a mejorar la planeación financiera, permite tomar decisiones oportunas en cuanto a Financiación y coberturas, hacer estimaciones de pagos. Definición de la divisa para adquisición de deuda o del esquema de aportes para nuevos negocios.

N°	RIESGO	PRIORIZACIÓN DE ACCIONES
		Estructuración de operaciones de cobertura para estabilizar estados de resultados y caja. Implementación de esquemas de Financiación y garantías que no afecten el nivel de endeudamiento. Proyección de los flujos de caja de los proyectos según las necesidades de inversión. Operaciones de manejo de deuda (identificar mejores condiciones de la deuda en cuanto a perfil y riesgo).
3	Cambios en la regulación, políticas y jurisdicción en el sistema de Infraestructura	Sistema de Gestión Ambiental, (e.g. ISO 14000) para asegurar que sus procesos estén alineados con la búsqueda del desarrollo ambientalmente sostenible. Modelo de Gestión Socioambiental, para evitar conflictos con las comunidades. Atención oportuna a notificaciones de infracciones ambientales emitidas por corporaciones de vigilancia ambiental. Exigencia de pólizas, seguros o garantías en los contratos requeridos para la operación, gestión y mantenimiento del sistema de infraestructura, seguro de responsabilidad civil extracontractual. Análisis, seguimiento y gestión a proyectos de Ley en materia fiscal, aduanera, cambiaria, contable, ambiental. Gestión ante el ente regulador para soportar técnicamente adecuaciones regulatorias Seguimiento permanente a los planes de uso del suelo. Definición de planes de acción regulatorios convenidos con diferentes áreas de la empresa Actuaciones judiciales y extrajudiciales para desestimular demandas o parar gestionar indemnizaciones, cuando sea el caso. Adecuada identificación y gestión de los riesgos asociados a los procesos de contratación. Exploración, análisis e implementación de contratos de estabilidad tributaria. Interacción con gremios y autoridades competentes (administrativas, regulatorias, contables, tributarias, jurídicas). Revisión financiera y jurídica como parte del proceso de contratación. Seguimiento y análisis permanente a los cambios regulatorios y normativos que impactan el negocio de generación, transporte, distribución de energía eléctrica. Validación jurídica de la interpretación técnica de la regulación. Mercadeo relacional, estableciendo diferentes medios de contacto como página web, realización de eventos, etc, de manera que se facilite el flujo de información
4	Cambios en las políticas Públicas Nacionales en torno al sistema de Infraestructura	Gestión directa con entidades del Estado Análisis permanente de la situación política y económica de los paises donde existe el sistema de infraestructura eléctrica Incorporación de cláusulas en el contrato de financiación, mediante las cuales se otorguen períodos de gracia en caso de un evento de nacionalización
5	Condiciones Meteorológicas adversas	Esquema de disponibilidad de personas especialistas para atender contingencias. Implementar y actualizar los planes de contingencia, considerando eventos de alta lluvia, temperaturas extremas de frío y calor. Sistemas contra incendio en subestaciones, plantas de generación, edificios y sedes. Sistema de apantallamiento y puesta a tierra para Torres, plantas de generación, edificios, sedes y subestaciones. Diseño de líneas de transporte y distribución, con adecuado cálculo de cadenas de aisladores y uso de conductores de cobre en zonas de alta salinidad y polución.
6	Fenómenos naturales adversos	Adopción de planes de emergencia y la aplicación de planes de comunicaciones para la gestión de crisis. Implementación y certificación en sistemas de gestión de seguridad industrial (e.g. OSHAS 18000) y Gestión Medioambiental (e.g. ISO 14000). Seguridad por medio de equipos electrónicos (vigilancia, monitoreo, etc), integradas en el perímetro de seguridad física de las instalaciones. Requisito en las políticas, en los seguros o en las garantías de los contratos necesarios para el funcionamiento, gestión y mantenimiento de la infraestructura. Seguros de vida para los trabajadores de las empresas que poseen u operan infraestructuras críticas. Seguros contra los daños y contra sus posibles consecuencias.

N°	RIESGO	PRIORIZACIÓN DE ACCIONES
		Realizar rutinas de mantenimiento correctivo de los equipos. Implementar planes de continuidad del negocio. Criterios de diseño que incluyan estudios geológicos y capacidades del suelo, con inspecciones periódicas de los suelos que sostienen la red de infraestructura. Ajustes y adaptaciones de las instalaciones existentes y establecer normas para resistir a terremotos.
7	Incomprensión y oposición de la población	Sistema de Gestión Ambiental, (e.g. ISO 14000) para asegurar que sus procesos estén alineados con la búsqueda del desarrollo ambientalmente sostenible. Modelo de Gestión Socioambiental, para evitar conflictos con las comunidades. Definición, comunicación y aplicación de los protocolos para gestión de riesgos derivados del conflicto social Gestión predial con familias asentadas en las zonas de servidumbre de las líneas de transporte y en los embalses hidroeléctricos Aplicación de la Política Social, comprometiendo el respeto a los derechos humanos, la prestación de servicios con calidad y eficiencia, el suministro oportuno de información de interés público. Actuaciones judiciales y extrajudiciales para desestimular demandas o parar gestionar indemnizaciones, cuando sea el caso. Monitoreo y análisis de la dinámica del conflicto social Inspección periódica de servidumbres para las líneas de transporte en áreas rurales y urbanas, y para los embalses Establecer opciones de mitigación en las zonas y terrenos por donde pasan las líneas de transporte.
8	Terrorismo y vandalismo	Creación de planes de contingencia y de emergencia, entre ellos el Comité de gestión de crisis. Aplicación del plan de comunicaciones para la gestión de crisis. Definición e implantación de protocolos de comunicación para la gestión de los riesgos derivados de los conflictos sociales. Seguridad por medio de equipos electrónicos (vigilancia, monitoreo, etc), integradas en el perímetro de seguridad física de las instalaciones. Requisito de las políticas, los seguros o las garantías en los contratos necesarios para el funcionamiento, gestión y mantenimiento de la infraestructura. Disponibilidad de presupuesto para la reparación a las centrales eléctricas, torres de transporte y subestaciones. Desarrollo de habilidades personales y competencias en la gestión institucional de los riesgos asociados a los conflictos armados. Seguimiento y análisis de la dinámica de los conflictos armados en países o regiones donde se encuentra la infraestructura crítica. Esto requiere una coordinación constante con las fuerzas policiales. Coordinación interinstitucional para la evacuación de las personas que invaden áreas de infraestructura (presas, servidumbres, etc), incluyendo la inspección periódica de las servidumbres en embalses y líneas de transporte (zonas rurales y urbanas). Colaboración interinstitucional entre comités de infraestructuras críticas, empresas eléctricas, organismos gubernamentales. Investigaciones internas y vigilancia sobre comportamientos sospechosos.
9	Volatilidad de Variables Macroeconómicas	Análisis permanente de las variables macroeconómicas y evaluación de los efectos de la volatilidad de las variables económicas sobre la estructuración de los procesos de contratación (inflación, tasa de cambio de divisas, crecimiento económico, salarios, impuestos, etc). Aplicación de metodologías de cuantificación de riesgos: Análisis de sensibilidad (EaR, CFaR, VaR) que permite cuantificar el riesgo puro y residual al que se encuentran expuestos los estados financieros. Evaluación de los efectos de la volatilidad de las variables sobre la situación financiera de las empresas propietarias y operadoras del sistema de infraestructura Definición de la divisa para adquisición de deuda o del esquema de aportes para nuevos negocios Operaciones de manejo de deuda Estudio y aplicación de fórmulas de reajuste de precios de insumos o materias primas
10	Corrupción, fraude, mala	Definición de un Código de Buen Gobierno.

N°	RIESGO	PRIORIZACIÓN DE ACCIONES
	administración	Definición, proceso, aplicación y verificación de los procesos de control interno en las contrataciones. Sistema de gestión para la seguridad de la información y política de control de aplicaciones, que incluye la trazabilidad en las operaciones en el sistema informático. Definición de los compromisos y de las prohibiciones sobre el manejo de información por parte de los empleados. Implementación de mecanismos que permitan a la empresa de infraestructura, asegurar que todas las partes interesadas comprendan y la acepten el marco institucional. Implementación, en el marco de inducción corporativa: valores, políticas, códigos de ética Rigurosidad en el proceso de selección de personal en las organizaciones operadoras/propietarias de infraestructuras eléctricas. Aplicación de políticas de talento humano y de beneficios para los empleados y demás partes interesadas. Cumplimiento de los requisitos relacionados con los procesos disciplinarios a los empleados en investigación. Doble control en transacciones y en cantidades máximas de transferencia. Acuerdos con los bancos, para la gestión de tesorería (autorizaciones). Auditorías externas sobre la vulnerabilidad de la red, y procesos de auditorías internas en la contabilidad general.
11	Deficiente gestión del conocimiento	Implementación de programa de fortalecimiento de la competencia en manejo y seguridad de la información Gestión sobre la plataforma tecnológica, Permite identificar elementos de riesgo para la seguridad sobre la plataforma tecnológica y tomar medidas oportunamente. Aplicación de la Política de información y del conocimiento. Se declaran los criterios para generar, administrar, conservar y proteger la información y el conocimiento como activos estratégicos de la organización y se define el marco de actuación para la gestión de éstos, de manera que contribuya a la mejora y el crecimiento organizacional, la realización de las estrategias y la continuidad óptima de la operación de las empresas del Grupo. Incluye guías y procedimientos. Definición de responsables y de protocolos para asignación de autorizaciones de acceso a información confidencial y estratégica Conservación y administración de la información física de carácter confidencial y estratégico. Se garantiza la correcta administración de la información física, de acuerdo con la normatividad vigente para el efecto. Definición de compromisos y prohibiciones respecto al manejo de la información por parte de los trabajadores Capacitación sobre riesgos en contratación
12	Retos del Crecimiento del Sistema de Infraestructura	Gestión de oportunidades de inversión, priorización de las oportunidades que son de interés de la empresa, de acuerdo con la estrategia negocios. Seguimiento y evaluación al cumplimiento del plan de negocio y a la gestión de las empresas Aplicación de Política de Inversión, buscando el crecimiento con rentabilidad que permita la generación de valor agregado. Incorporación de acuerdos y cláusulas de confidencialidad en los contratos Análisis del entorno en los países donde se gestiona el sistema de infraestructura, o donde proyecta desarrollar su estrategia de crecimiento. Análisis interdisciplinario de nuevos negocios, incluyendo la factibilidad del negocio (modelo financiero, análisis de sensibilidad, optimizaciones, rentabilidades). Estructuración del caso de negocios (capacidad financiera, inversión, financiación, socios). Análisis y evaluación de impacto de los proyectos en los estados financieros y en los indicadores Implementación de esquemas alternativos de Financiación y garantías, disminuyendo la probabilidad de ocurrencia de eventos de incumplimiento por incapacidad financiera. Evaluación ex-post de los negocios (identificar lecciones aprendidas). Evaluación ex-post de las ofertas en las licitaciones contractuales (identificar lecciones aprendidas). Validación y aprobación de propuestas de nuevos negocios en diferentes instancias

N°	RIESGO	PRIORIZACIÓN DE ACCIONES
		Participación de directivos en Juntas Directivas, Directorios y Consejos de Administración de las empresas propietarias y operadoras del sistema de infraestructura Provisión adecuada y oportuna del talento humano, y en caso necesario, recurrir a consultorías externas.
13	Fallos humanas y de procedimiento	Mantener la disponibilidad de turnos para personas especialistas en caso de contingencias. Creación de planes de contingencia y de emergencia, entre ellos el Comité de gestión de crisis. Prevención mediante un Sistema de Gestión para la Seguridad Industrial, por ejemplo, la norma OSHAS 18000, incluyendo la implementación de políticas de seguridad industrial y salud ocupacional, así como los procedimientos para las tareas que implican la cultura de seguridad industrial. Sistema de gestión medioambiental y certificación de calidad a través de normas ISO 9000 e ISO 14000. Requisito de políticas, seguros o garantías en los contratos necesarios para el funcionamiento, operación y mantenimiento de la infraestructura. Formación, capacitación y certificación en procesos críticos, así como la evaluación periódica de los conocimientos técnicos del personal de mantenimiento. Programas de mejora con respecto a la eficacia en la planificación del mantenimiento. Evaluación psicofísica del personal crítico, tanto en los procesos de operación como de mantenimiento. Actualización tecnológica en los centros de control. Contratación adecuada del talento humano, de acuerdo a las necesidades actuales y la estrategia de crecimiento de la compañía de infraestructura. Las operaciones de tesorería se deben permitir sólo para personas autorizadas. Definición de los protocolos de prueba y configuración de las protecciones de la red.
14	Fallos en Equipos, Materiales y hardware	Esquema de disponibilidad de personas especialistas para atender contingencias y esquema de operación en respaldo con personal especializado (Ingenieros, Personal experto) Planes de contingencia, Planes de emergencia, Sistema de gestión para la seguridad industrial, por ejemplo, Norma OSHAS 18000, Aplicación de la Política de seguridad industrial y Salud Ocupacional Sistema de Gestión Ambiental, por ejemplo, Norma ISO 14000 Exigencia de pólizas, seguros o garantías en los contratos requeridos para la operación, gestión y mantenimiento del sistema de infraestructura Seguro de daños materiales combinados y pérdidas consecuenciales Sistema de Gestión para la Seguridad de la Información Manejo de incidentes de seguridad, con el fin de identificarlos (infraestructura, seguridad de la información, intrusiones, etc) y tomar correctivos. Programas de mejora de procesos para disminuir las anomalías en mantenimiento y en supervisión y maniobras Programas de mejora de procesos para optimizar la planeación de los activos Programas de mejora de procesos para aumentar la eficiencia en la logística de inventario Programas de mejora de procesos referentes a la efectividad en la planeación del mantenimiento Sistemas contra incendio en subestaciones, plantas de generación, edificios y sedes Sistema preventivo de mantenimiento y mantenimiento correctivo de equipos Actualización tecnológica para las empresas propietarias de la red de infraestructura y optimización de activos de la infraestructura. Evaluación técnica de equipos operativos en el sistema de infraestructura. Operaciones con subestaciones aledañas, para eventos de pérdida de supervisión de una subestación. Implementar estrategias de seguridad para los equipos de respaldo eléctrico.
15	Inadecuado entrenamiento, formación y capacitación del capital humano	Aplicación de la Política de seguridad industrial y Salud Ocupacional Entrenamiento, habilitación y certificación en procesos críticos Evaluación psicofísica de personal de procesos críticos de operación y mantenimiento

N°	RIESGO	PRIORIZACIÓN DE ACCIONES
		Documentación de procesos y procedimientos Medición periódica de competencias técnicas de personal de operación y mantenimiento Aplicación del sistema de gestión de desempeño, tutorías y seguimiento Evaluación, seguimiento y gestión del clima organizacional Aplicación de la Política de información y del conocimiento Planeación del talento humano (necesidades de personas, en términos de la cantidad y los perfiles humanos y técnicos requeridos) y selección del personal que se ajusta a los requisitos de los perfiles (formación, experiencia, y competencias humanas y técnicas). Identificación de talento directivo y técnico y estructura de cuadros de reemplazo Evaluación y desarrollo de competencias técnicas y humanas, dentro de un sistema de formación y certificación. Análisis y cierre de brechas para el desarrollo del talento humano Análisis de cargas y turnos de trabajo, con el fin de evitar cansancio y agotamiento.
16	Perturbaciones técnicas en la red eléctrica y en plantas de generación	Mantener la disponibilidad de turnos para personas especialistas en caso de contingencias. Adoptar planes de contingencia y planes de emergencia, así como planes de comunicaciones para la gestión de crisis, incluida la aplicación de un plan de continuidad del negocio. Mantener una comunicación fluida entre los centros de control de infraestructuras eléctricas. Analizar los incidentes de seguridad reportados por los usuarios con el fin de identificar, clasificar la causa (infraestructura, seguridad de la información, intrusión, etc) y tomar decisiones y medidas correctivas. Asegurar los servicios complementarios (Regulación de frecuencia, control de tensión, sustitución del servicio) proporcionados por el operador del sistema eléctrico, para garantizar la calidad y la seguridad del suministro mediante la gestión de las desviaciones y los servicios adicionales. Realizar el mantenimiento preventivo en el sistema, incluida la inspección de cada tecnología de componentes y equipos. Realizar el mantenimiento correctivo de los equipos, incluyendo revisiones de programación para equipos críticos y de mayor duración. Implementar la plataforma de gestión de la tecnología. Mecanismos de activación de servicios auxiliares para compensar los aumentos imprevistos en la demanda. Realización de actualizaciones de hardware y software para la operación de la infraestructura. Acuerdos de cooperación con escuelas y universidades para promover la investigación, desarrollo e innovación en torno al problema de la estabilidad del sistema eléctrico. Suscripción garantías de potencia entre los agentes del mercado eléctrico.
17	Vulnerabilidad de los sistemas TIC	Información de respaldo: almacenamiento de los respaldos y de los *back-ups* en lugares seguros. Centralizar el sistema de control de la red de infraestructura crítica. Implementar plataformas de gestión de la tecnología. Implementar políticas para el acceso a los sistemas de información. Definición de las metodologías documentales para garantizar la disponibilidad de información. Definición de procedimientos para garantizar la calidad en el funcionamiento de los sistemas de información Actualizaciones de hardware y de software para la operación de la infraestructura. Duplicar los centros de control de las infraestructuras eléctricas. Implementar métodos de cyber-protección y de defensa como CERT / CSIRT [ALBERTS, DOROFEE *et al.*, 2004]
18	Cumplimiento y calidad en el suministro eléctrico	Sistema de Gestión Ambiental, por ejemplo, Norma ISO 14000 y Sistema de Gestión de Calidad, por ejemplo, Norma ISO 9000, Sistema de gestión para la seguridad industrial, por ejemplo, Norma OSHAS 18000. Sistema de mantenimiento preventivo, mantenimiento correctivo de equipos. Planes de trabajo para garantizar la continuidad del servicio de los centros de control.

N°	RIESGO	PRIORIZACIÓN DE ACCIONES
		Planes de trabajo para la diversificación de las habilidades del talento humano. Inspección tecnológica de cada componente y equipo. Programación de overhaults a equipos críticos y con mayor vida útil. Suministro de Servicios Auxiliares. Interconexiones internacionales con redes de transporte.
19	Riesgo Reputacional y de Imagen Pública	Implementación del plan de comunicaciones para manejo de crisis Diseño e implementación de estrategias de comunicación corporativa (credibilidad, confianza y una buena percepción de imagen). Aplicación de la política de Comunicación para el grupo empresarial, el cual está orientado a afianzar la identidad corporativa, formar opinión pública favorable, facilitar la interacción entre la organización y gestionar las relaciones con el entorno. Definición, divulgación y aplicación de lineamientos de comunicaciones por negocios, y aplicación de protocolos de comunicación. (Gestión de la reputación) Modelo de Gestión Integral, direccionamiento estratégico, gerencia de corto plazo y transformación cultural. Seguimiento y evaluación al cumplimiento del plan de negocio y a la gestión de las empresas Implantación y actualización de los modelos de negocio, operativo y de gobierno Código de buen gobierno (políticas, normas, sistemas y principios éticos que orientan la actuación empresarial respecto de su gobierno, su conducta y su información.) Participación de directivos en Juntas Directivas, Directorios y Consejos de Administración de las empresas propietarias y operadoras del sistema de infraestructura Homologación de mejores prácticas - transferencia de conocimiento
20	Deficiencias de proveedores y subcontratistas del sistema	Sistema de Gestión Ambiental, por ejemplo, Norma ISO 14000 y Sistema de Gestión de Calidad, por ejemplo, Norma ISO 9000, Sistema de gestión para la seguridad industrial, por ejemplo, Norma OSHAS 18000. Exigencia de pólizas, seguros o garantías en los contratos requeridos para la operación, gestión y mantenimiento del sistema de infraestructura Sistema de Gestión para la Seguridad de la Información Reunión de inicio de los procesos de contratación Aplicación de la política de adquisición de bienes y servicios, definiendo el marco general para los procesos de adquisición de bienes y servicios, orientado a satisfacer las necesidades y asegurar el mejor resultado técnico y económico. Actuaciones judiciales y extrajudiciales para desestimular demandas o parar gestionar indemnizaciones, cuando sea el caso. Segregación de información sobre estructuración de licitaciones Capacitación sobre riesgos en contratación, definición y aplicación de la normatividad relacionada con el proceso de contratación, revisión financiera y jurídica como parte del proceso de contratación Incorporación de acuerdos y cláusulas de confidencialidad en los contratos, cláusulas de propiedad intelectual Definición de criterios para evaluación de empresas contratistas. Proyecto de automatización de documentos para el proceso de contratación Evaluación de proveedores de bienes y servicios Seguimiento y monitoreo al funcionamiento y al cumplimiento de los compromisos pactados Cláusulas contractuales que dan el marco de actuación para hacer exigible el cumplimiento de lo pactado en los contratos Definición e implementación de acciones contra los contratistas por incumplimientos
21	Vulnerabilidad de la cadena de suministro	Inversiones de capital para garantizar suministro de gas, carbón, *fuel oil*, según el caso. Diversidad de costos variables de producción en función a su fuente primaria de energía (Agua, gas, carbón, bunker, etc.). Producción de energía en el momento que se consume, implicando la necesidad de tener capacidad siempre disponible para atender las demandas instantáneas de los usuarios. Despacho coordinado de mínimo costo.

N°	RIESGO	PRIORIZACIÓN DE ACCIONES
		Comercialización de transacciones se generalmente por unidades vendidas de Energía, Potencia o capacidad, Energía firme, reserva de capacidad, regulación de frecuencia, etc. Estrategias y políticas de seguridad nacional para aseguramiento energético.

C. ANEXO C: CONTINGENCIAS N–1 EN REDES DE PRUEBA IEEE

El estudio de los eventos que ocurren cuando un elemento de la red es retirado o sale de servicio por causas imprevistas o programadas, se conoce como **Contingencia N-1**. Cada vez que se presenta la salida de un elemento en el sistema, las corrientes en las líneas se redistribuyen a través de la red y las tensiones de las barras cambian. Como consecuencia de esto, pueden aparecer sobrecargas en líneas o transformadores [GÓMEZ-EXPÓSITO, 2002]. Algunas de esas estrategias para el estudio de estas contingencias consisten en: supervisión y control del sistema en tiempo real, control predictivo, estimación de la demanda y planificación de la generación, control dinámico del sistema, evaluación del flujo por cada una de las líneas y transformadores del sistema y las tensiones en los nodos de la red. Dichas estrategias se conocen como **estudio de contingencias.**

A. DEFINICIONES

Los **análisis en estado estable para contingencias N-1** se realizan generalmente resolviendo muchos flujos de carga sobre la red de potencia. Según

esos resultados, se pueden conocer las condiciones de estado que el sistema adquiere después de la salida de cada elemento del sistema.

En la literatura se pueden encontrar diversidad de índices que permiten evaluar las condiciones de redes de transporte de media y alta tensión, ante una contingencia N-1. Algunos índices útiles para el análisis de contingencias simples y en estado estacionario son calculados resolviendo flujos de carga AC.

En todos los casos, los resultados obtenidos durante una contingencia se comparan con el **caso base**, es decir, la red operando bajo condiciones normales. El caso de mayor impacto en una contingencia N-1 permite identificar los nodos que mayor vulnerabilidad propagan en el sistema de potencia. Esta identificación y evaluación de los nodos más vulnerables constituyen la primera etapa para la toma de decisiones en la protección de dichos activos.

Para la realización del cálculo de contingencias N-1 se tiene en cuenta la existencia de un *generador de slack*, que igualmente está conectado al respectivo *bus de slack*. Ambos elementos deben estar siempre conectados al sistema de transporte, dado que constituyen la referencia para efectuar los flujos de carga. A priori, estos elementos también merecen particular atención y se identifican como de alta criticidad. Su eliminación, ante fallo o ataque, tiene consecuencias en un evento de *blackout* de toda la red de transporte o distribución.

En la literatura se aplican una serie de indicadores que miden las consecuencias de contingencias N−1 sobre una red. Entre ellos se encuentran: Condiciones de Carga Máxima [MILANO, 2003], Información comprensiva del sistema [HAIDAR, MOHAMED *et al.*, 2007], Pérdida de Carga del Sistema [HAIDAR, MOHAMED *et al.*, 2008], etc.

B. DESCONEXIÓN DE CARGAS - PLS

En la Figura A.2 se puede apreciar el *índice de desconexión de cargas* (PLS) (ecuación [5.34]) para contingencias N−1, asociadas a cada nodo de las redes de prueba IEEE. Los resultados presentados se obtienen mediante la ejecución sucesiva de *flujos de carga estándar* (SPF, Standard Power Flow), con algoritmo Newton-Raphson (sección 5.2.4.1). En el eje de las abscisas se muestra el nombre del nodo fallado en la contingencia, aunque desafortunadamente no es posible mostrar la totalidad de esos nombres.

Se obtiene una curva de demanda no suministrada por cada red. Los nodos más críticos, que merecen particular atención, son aquellos cuya eliminación constituye la mayor desconexión de carga en el sistema.

En este ejemplo, obsérvese que en la red de 14 buses, compuesto por 50 nodos, el aislamiento de su único generador implica la desconexión total de las cargas del sistema, configurándose un evento de *blackout*.

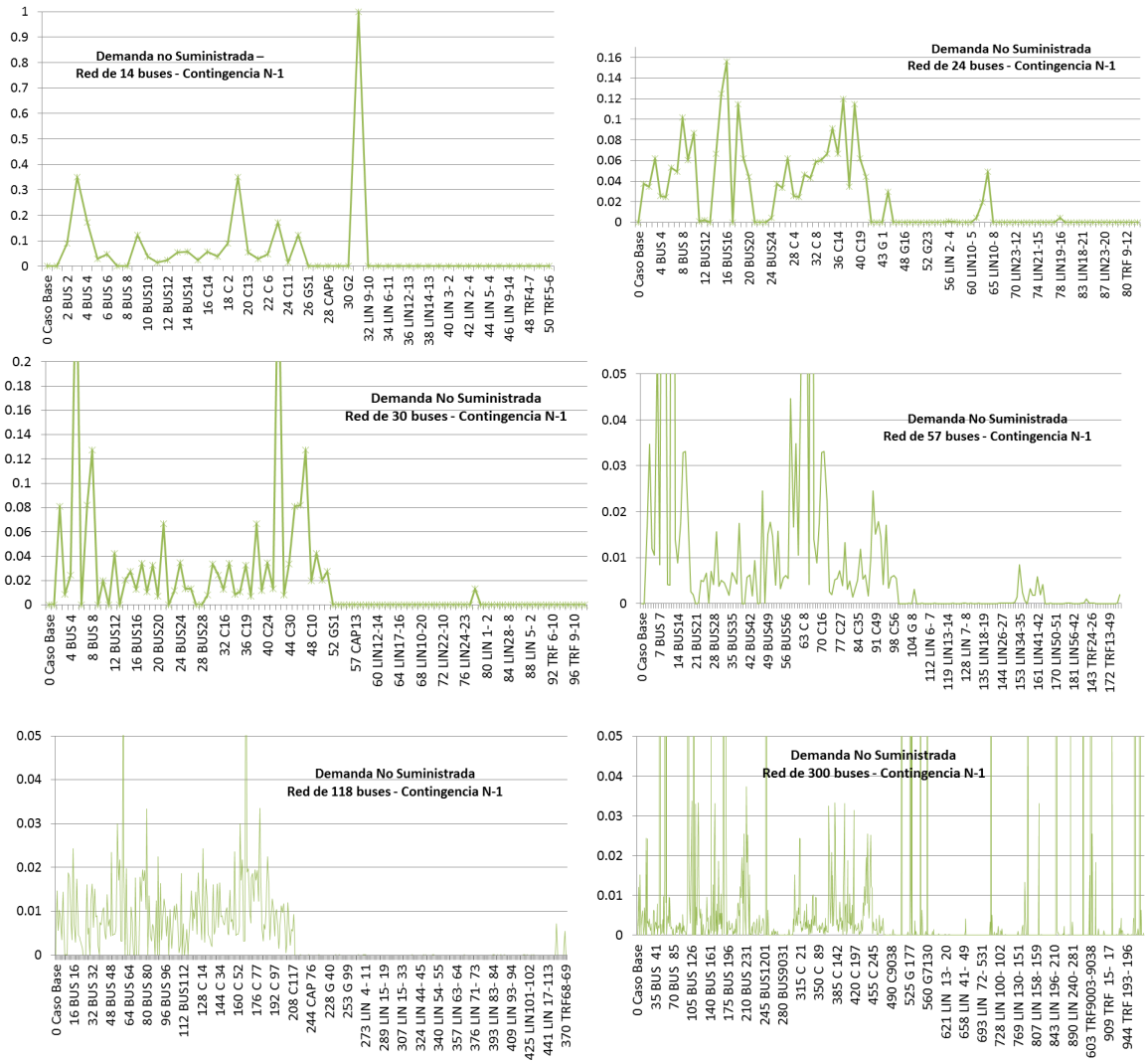


Figura A.1: Contingencias N-1: *Índice de Desconexión de Cargas (PLS)*

Igualmente, la red de distribución de 300 buses, compuesta por 966 nodos, contiene un total de 18 nodos que impacta la capacidad de todo el sistema. Un ataque a cualquiera de ellos produce el colapso total del sistema (*PLS* = 100%). Se identifican como los nodos más vulnerables: 7 buses o barras, 4 transformadores, 3 líneas de distribución, y 4 generadores de potencia activa.

La priorización de acciones de protección para estos sistemas debe concentrar especial atención en esos nodos críticos. Cualquier manifestación del riesgo sobre esos activos particulares tendrá serias consecuencias en la operación de todo el sistema de infraestructura crítica.

En las demás redes (24, 30, 57 y 118 buses), aunque no existen nodos que conlleven a un colapso total en la operación del sistema, sí tienen un impacto significativo en el indicador de demanda no suministrada; en algunos casos puede significar un impacto hasta el 20% sobre toda la carga del sistema.

Dado que estas redes tienen un modelo topológico de libre escala, los nodos menos conectados tienen un menor impacto sobre todo el sistema. Sin embargo, es evidente el impacto que genera el ataque a un bus con muchas conexiones sobre los flujos de la red. Esto causa problemas para el sistema, ya que sin los nodos muy conectados el sistema se rompe en varias áreas desconectadas que no pueden comunicarse entre sí.

C. ÍNDICES DE SEVERIDAD

Uno de los métodos más utilizados para el análisis de contingencias N-1 es el índice de severidad ***IS***, que refleja el nivel de carga de líneas y transformadores tras un determinado evento [GÓMEZ-EXPÓSITO, 2002].

$$IS_i = \frac{1}{N}\sum_{i=1}^{N}\frac{\left|P_f(i)\right|}{P_f^{máx}} \qquad \text{[A.1]}$$

En [A.1], P_f es la potencia en el elemento *i*, de un total de ***N*** nodos que representan las líneas y transformadores. $P_f^{máx}$ es el flujo de potencia en el elemento, generalmente asociada al flujo del caso caso base. La potencia indicada puede ser *activa* o *aparente*. En consecuencia, el índice de severidad corresponde a la **carga media de los elementos del sistema**. En todos los casos, estos resultados se obtienen mediante los flujos de carga de cada uno de los casos en las contingencias N−1.

Es posible normalizar el índice de severidad de la ecuación [A.1] y determinar cuánto cambia la carga media de los elementos del sistema, respecto del caso base.

$$\left(IS_{norm}\right)_i = \frac{IS_i}{IS_{CB}} \qquad \text{[A.2]}$$

En la Figura A.1 se puede apreciar el *Índice de Severidad Normalizado* para contingencias N−1, **calculado con potencia aparente** en diferentes redes de prueba

IEEE. Los resultados presentados se obtienen mediante la ejecución sucesiva de *flujos de carga estándar* (SPF, Standard Power Flow), con algoritmo Newton-Raphson (sección 5.2.4.1). En el eje de las abscisas se muestra el nombre del nodo fallado en la contingencia, aunque desafortunadamente no es posible mostrar la totalidad de esos nombres.

Los nodos más críticos, que merecen particular atención, son aquellos cuya eliminación constituye la mayor desviación de la carga media en los elementos del sistema, respecto del caso base. Una desviación de más del 25% se considera problemática, porque sobrepasa los parámetros de diseño del sistema eléctrico, aumentando las pérdidas y eventuales desconexiones por sobrecarga de la red [GÓMEZ-EXPÓSITO, 2002].

El **índice de severidad** permite detectar contingencias muy graves asociadas a la pérdida de ciertos activos que impactan gravemente el funcionamiento de la red, especialmente la pérdida de generadores, líneas de transporte y transformadores. La sobrecarga de la red se puede relacionar con un posterior evento de *blackout*, porque podrá operar en condiciones que superan los parámetros de diseño. A diferencia del indicador de *demanda no suministrada* (el cual realiza una medición específicamente sobre la cantidad de carga que se aísla del sistema), el índice de severidad plantea una visión más global sobre el funcionamiento de toda la red, detectando desviaciones respecto a su funcionamiento bajo condiciones normales (caso base).

Puede deducirse que las redes de transporte de alta tensión están más interconectadas que aquellos sistemas radiales de distribución de media tensión. Obsérvese que en el caso de la red IEEE-14, las contingencias de mayor impacto son aquellas asociadas al fallo del único generador, o del bus al cual éste se conecta (en cuyo caso, $IS_{norm} \approx 2$).

En la red IEEE-24 destaca el impacto del bus #16, que soporta alta conectividad, incluyendo un generador (en cuyo caso $IS_{norm} \approx 1.2$), pero en general el sistema puede soportar las demás contingencias. En el caso de la red IEEE-30, la alta criticidad de la contingencia asociada al fallo de tres buses (2, 6 y 27) se explica dado el fallo del único generador de la red, o porque constituyen nodos con alta conectividad (dado que $IS_{norm} > 1.5$). La misma situación ocurre para la red IEEE-57, por la contingencia de 2 generadores de gran capacidad, o por la contingencia de la línea eléctrica que une sus respectivos buses (en esos casos $IS_{norm} > 1.4$).

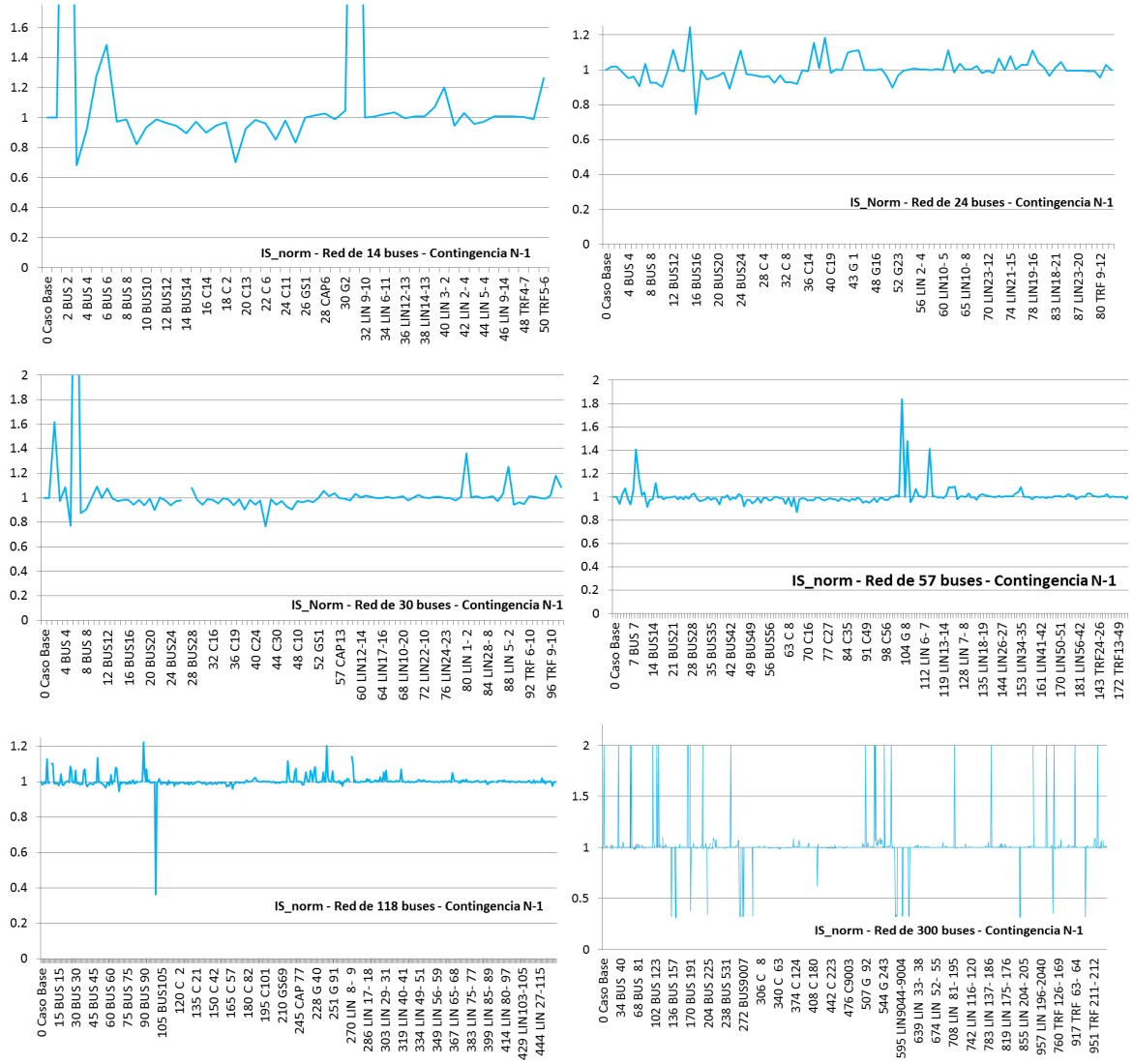


Figura A.2: Contingencias N-1: *Índice de Severidad Normalizado* (IS_{norm}) para potencia aparente

No obstante, en la red IEEE-300 se evidencia que la contingencia de unos cuantos nodos genera grandes sobrecargas en el sistema (IS_{norm} >> 1.4). Se identifican como los nodos más vulnerables: 9 buses o barras, 4 transformadores, 2 líneas de distribución, y 6 generadores de potencia activa.

D. IMPACTO EN LA CONECTIVIDAD DEL GRAFO DE LIBRE ESCALA

En la Figura A.3 se puede apreciar *impacto sobre la conectividad* (S) del grafo resultante por el fallo de cada nodo en contingencias N-1 (ecuación [5.19]). En el eje

de las abscisas se muestra el nombre del nodo fallado en la contingencia, aunque desafortunadamente no es posible mostrar la totalidad de esos nombres.

Estos resultados muestran una fuerte correlación entre la robustez del sistema y la topología de la red. En particular, estas redes de libre escala son más robustas ante contingencias de componentes con menor grado nodal, pero son más vulnerables ante las contingencias de los nodos con mayor grado nodal.

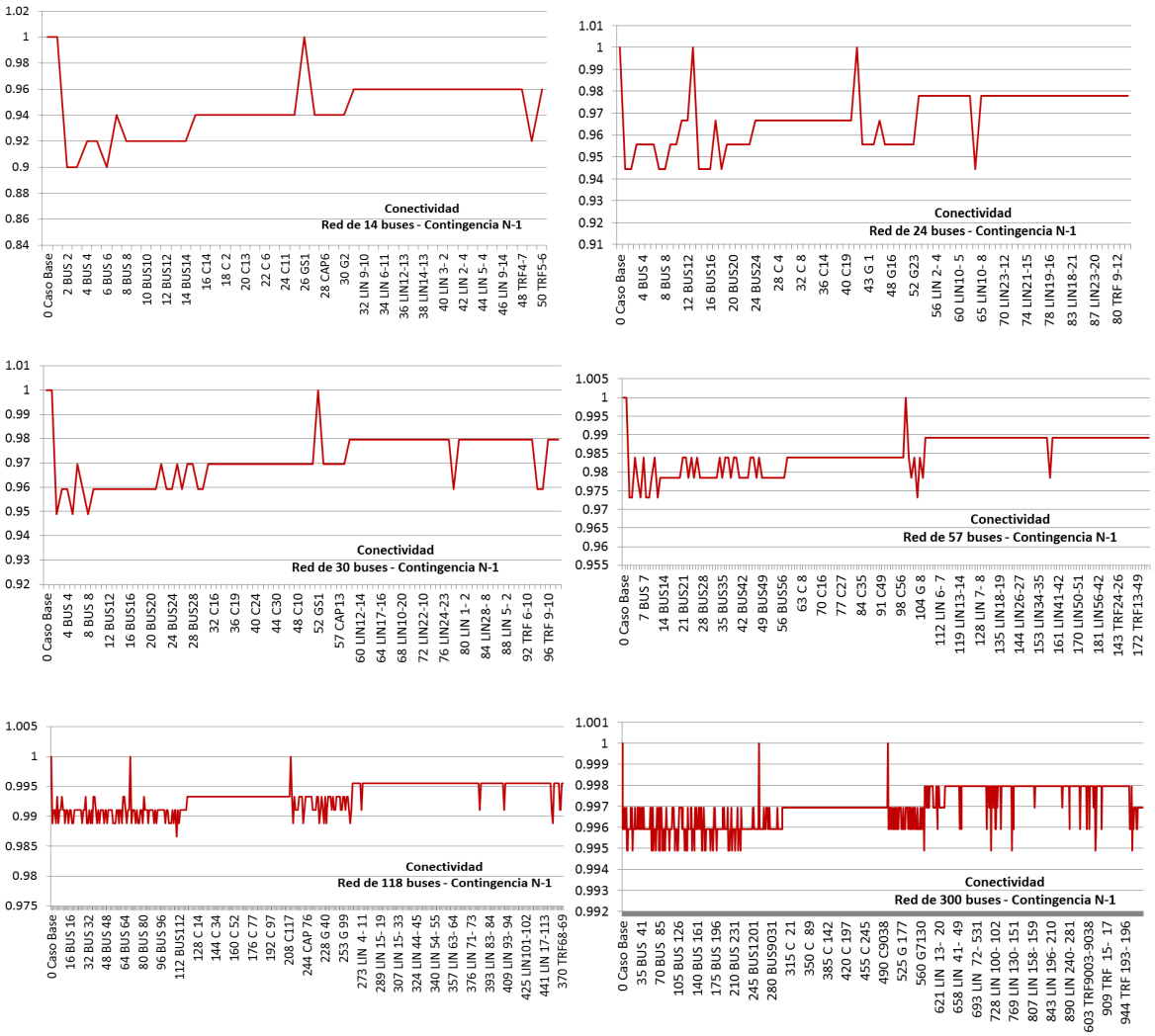


Figura A.3: Contingencias N-1: *Índice de Impacto en la Conectividad (S)*

Según este indicador, se puede observar que en todos los casos el mayor impacto sobre las redes ocurre por la eliminación o aislamiento de los nodos con mayor grado de conectividad, especialmente los buses, en tanto los nodos con menor grado (como los generadores, los condensadores y las cargas) tienen un impacto mínimo sobre el índice de conectividad. Para las redes más grandes, que tienen un mayor número de nodos, la eliminación de cualquier nodo repercute en menor medida

sobre el indicador, dado que el numerador siempre tiene valor similar al del denominador.

Cualquiera de los indicadores previamente estudiados son de utilidad en el proceso de identificación y de activos más críticos dentro del sistema, según se especifica en las primeras etapas (identificación y evaluación) de los programas de protección de infraestructuras críticas. Como se ha sugerido previamente, la aplicación de medidas de protección y priorización de acciones de mitigación de riesgos pueden enfocarse inicialmente en los nodos que ocasionan mayor vulnerabilidad al sistema.

Hay que tener en cuenta que las vulnerabilidades y sus consecuencias no son obvias por completo. La identificación de las amenazas debidas a personas malintencionadas son distintas a las amenazas debidas a fenómenos naturales (huracanes, terremotos, incendios y otros desastres). Desde el punto de vista de la infraestructura crítica, la red interdependiente cuenta con algunos nodos críticos, en los cuales el sistema energético simplemente requiere ser suficientemente seguro como para permitir una interrupción ordenada. En otros casos, los nodos críticos tienen que ser tan robustos como para garantizar el funcionamiento autónomo durante horas, días, semanas o incluso más tiempo (en caso que se requiera). En consecuencia, el reforzamiento del sistema de infraestructura eléctrica implica la realización de actividades que se extiendan más allá y con mayor profundidad que las acciones tradicionales.