Lámpsakos
E-ISSN: 2145-4086
lampsakos@amigo.edu.co
Fundación Universitaria Luis Amigó
Colombia

Correa-Henao, Gabriel Jaime; Yusta-Loyo, José María
SEGURIDAD ENERGÉTICA Y PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS
Lámpsakos, núm. 10, julio-diciembre, 2013, pp. 92-108
Fundación Universitaria Luis Amigó
Medellín, Colombia

Lámpsakos | Nº 10 | pp. 92-108 | julio-diciembre | 2013 | ISSN: 2145-4086 | Medellín - Colombia

SEGURIDAD ENERGÉTICA Y PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

ENERGY SECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

Gabriel Jaime Correa-Henao, PhD
Facultad de Ingenierías
Fundación Universitaria Luis Amigó
Medellín, Colombia
gabriel.correahe@amigo.edu.co

José María Yusta-Loyo, PhD
Departamento de Ingeniería Eléctrica
Universidad de Zaragoza
Zaragoza, España
jmyusta@unizar.es

(Recibido el 20-05-2013 Aprobado el 21-06-2013)

Resumen. En los últimos años se ha intensificado la preocupación de todos los países y gobiernos por la seguridad del abastecimiento energético, y particularmente por la protección de las infraestructuras críticas para el suministro de energía. A los marcos de referencia internacionales de la Directiva 2008/114/CE de la UE y el Plan Nacional de Protección de Infraestructuras de EEUU de 2009, se suma en España la reciente aprobación de la Ley 8/2011 y del Real Decreto 704/2011 sobre identificación y protección de infraestructuras críticas.

En este artículo se muestran, en el marco de estas referencias, distintas estrategias internacionales de organización de la protección de infraestructuras. También se propone un marco conceptual para la identificación de amenazas en infraestructuras eléctricas mediante mapas de riesgos interconectados.

Palabras Clave: Seguridad, riesgos, energía, infraestructuras.

Abstract. In recent years, concerns on energy supply security have raised up for many countries and governments, and particularly on energy critical infrastructure protection. The international frameworks of the EU Directive 2008/114/EC and the U.S. National Infrastructure Protection Plan since 2009, is now accompanied by the recent approval in Spain of Act 8/2011 and Royal Decree 704/2011 on the identification and protection of critical infrastructures.

In this article, on behalf of such references, different international strategies for infrastructure protection management are shown. A conceptual framework for risks identification in electric infrastructure through interconnected risk maps is also proposed.

Keywords: Security, risk, energy, infrastructure.

Citación de artículo, estilo IEEE:
G.J. Correa-Henao, J.M. Yusta-Loyo, "Seguridad Energética y Protección de Infraestructuras Críticas", Lámpsakos, N° 10, pp. 92-108, 2013.

1. INTRODUCCIÓN

Los gobiernos consideran la seguridad del abastecimiento como uno de los principales objetivos de su política energética. No es difícil encontrar en los últimos años esfuerzos institucionales en muchos países del mundo enfocados en el análisis de su seguridad energética desde diferentes puntos de vista, así como en la necesidad de mejorar su protección, con el ánimo de garantizar la seguridad nacional, la actividad económica, la salud pública, entre otros asuntos.

En el marco de esta definición, se hace evidente la estrecha relación entre la seguridad global de la infraestructura energética con los otros sectores de infraestructuras críticas de la economía y de estos con la sociedad. La infraestructura crítica constituye el sistema nervioso central de la economía en una nación. No es posible alcanzar las metas de sostenibilidad energética, los objetivos económicos, ni el desarrollo social, si se manifiestan vulnerabilidades y riesgos en redes de infraestructura como las del transporte, comunicaciones y energía.

Tanto la Comisión Europea como el Departamento de Seguridad Nacional de los Estados Unidos de América y otros, han desarrollado una preocupación creciente en los últimos años sobre la seguridad de sus infraestructuras, a consecuencia de las nuevas amenazas internacionales. Como resultado, en el año 2005 se publicó en Bruselas el Libro Verde "Programa Europeo para la Protección de Infraestructuras Críticas" [1]. Posteriormente, la Comisión Europea aprobó la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, mediante la cual se puso en marcha el Programa Europeo para la Protección de Infraestructura (PEPIC) [2]. Por su parte, en 2009 se publicó y se puso en marcha el Plan Nacional de Protección de Infraestructuras de Estados Unidos (NIPP) [3]. En el caso particular de España, mediante la Ley 8/2011 [4] 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.

Entre las infraestructuras objeto de análisis y protección, las redes energéticas ocupan un papel principal en todos los instrumentos de seguridad citados, dado que la energía es el motor económico que sustenta la actual sociedad moderna. Para lograr el objetivo de proteger la infraestructura energética crítica en cualquier país es preciso involucrar todos los componentes de esta en un programa completo de gestión de riesgos, que se inicia con un análisis de vulnerabilidades y evaluación de riesgos, y se completa con la aplicación de medidas de mitigación de amenazas.

Precisamente el interés estratégico asociado a la seguridad energética de las naciones constituye la motivación de este artículo, en el que se presenta una metodología cualitativa para la identificación de amenazas a la seguridad de la infraestructura eléctrica. Además, se contribuye a la discusión sobre las diferentes definiciones y enfoques sobre los conceptos de seguridad energética, infraestructura crítica y recursos clave. Se presenta también una revisión exhaustiva sobre experiencias internacionales, entre las que se destacan los programas europeos de protección de infraestructura (PEPIC) y el programa implementado actualmente por el gobierno de los EEUU (NIPP), que constituyen la referencia internacional en la protección de infraestructuras críticas. Se realiza además la presentación del nuevo marco legal en España, incluyendo una breve descripción de la Ley 8/2011, del Real Decreto 704/2011 y del organismo encargado de coordinar los planes españoles, el CNPIC.

2. SEGURIDAD ENERGÉTICA Y PROTECCIÓN DE INFRAESTRUCTURA CRÍTICA

La literatura relacionada con el aseguramiento energético es extensa y basada en gran parte en fuentes abiertas. Una revisión de las publicaciones especializadas proporciona información que relaciona la definición de "seguridad del abastecimiento energético" con áreas como: indicadores y estado del arte sobre el suministro energético, diversificación de fuentes energéticas, técnicas para toma de decisiones, infraestructura crítica y recursos clave, geopolítica y pensamiento militar, entre otras.

El concepto de suministro energético abarca diferentes enfoques, que además pueden ser analizados en diversos escenarios. Así, la definición clásica de "seguridad del suministro energético" basada en la provisión de suficiente cantidad de energía a precio asequible, necesita de la incorporación en los tiempos actuales de un nuevo mapa conceptual, que incluya

estabilidad de los precios, diversificación de fuentes energéticas, economía de las inversiones, seguridad física de las infraestructuras, reservas y almacenamiento, equilibrio político y poder militar, eficiencia energética, mercados, sostenibilidad, entre otros [5].

Tradicionalmente el enfoque de la seguridad energética se ha concentrado sobre todo en los accidentes y en los desastres naturales. A partir del 11 de septiembre 2001, las autoridades y también la industria han tenido que considerar la amenaza de un daño intencional en un grado mucho mayor que antes [6]. Como consecuencia de las nuevas amenazas, la visión sobre la seguridad energética en el actual contexto geopolítico internacional se relaciona directamente con las estrategias de defensa nacional y de estabilidad económica, vinculadas al funcionamiento de determinadas infraestructuras.

Entre los enfoques más recientes de la "seguridad del suministro energético" se encuentran aquellos relacionados con la vulnerabilidad de infraestructuras críticas [7], un término que está recibiendo cada vez más atención, y que concuerda con las definiciones establecidas tanto por la Comisión Europea en el Libro Verde [1] y en la Directiva 2008/114/CE [2], como por el gobierno de Estados Unidos en su programa de seguridad de infraestructuras [3], [8]. El término de infraestructura crítica es definido como aquel elemento, sistema o parte de este, situado en un Estado, y que es esencial 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 al no poder mantener esas funciones.

La literatura en general 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 [9].

La Figura 1 esquematiza, a modo de ejemplo, cuán entrelazados con la infraestructura energética de una nación se encuentran los recursos clave y los servicios de distribución de gas o telecomunicaciones [10], indispensables para mantener el desarrollo y funcionamiento de los sistemas que mueven la actividad de un país.

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, ante ataques intencionales, accidentes o desastres naturales [11]. La identificación de las amenazas debidas a la acción de personas malintencionadas requiere procedimientos distintos a las de fenómenos naturales (huracanes, terremotos, olas de frío, incendios y otros desastres).

Evidentemente el tema de la seguridad energética se contempla como uno de los asuntos de mayor importancia en las políticas nacionales. Los gobiernos tienen un papel esencial en la protección de las infraestructuras, así como en la prevención y gestión de crisis relacionadas con el suministro energético, tanto si se trata de infraestructuras gestionadas directamente por el Estado, bien si están en manos de empresas privadas [7].

En los países de la OCDE, la gran mayoría de los activos relacionados con los sistemas de infraestructura crítica son propiedad de organizaciones privadas. Cerca del 80% de estas son operadas directamente por empresas privadas, en el caso del suministro de energía eléctrica [12]. Algunas excepciones las constituyen el suministro de agua, las instalaciones gubernamentales o los servicios de emergencias, propiedad habitualmente de los estados o de entidades mixtas.

3. PLANES DE PROTECCIÓN DE INFRAESTRUCTURA

El concepto de infraestructura crítica abarca a todos aquellos activos que son tan vitales para cualquier Estado, que su destrucción o degradación tendría un efecto debilitante sobre las funciones esenciales del gobierno, la seguridad nacional, la economía nacional, o la salud pública [13]. La interrupción de un solo sector de la infraestructura crítica, a causa de ataques terroristas, desastres naturales o daños provocados por el hombre, es probable que tuviera efectos en cascada sobre otros sectores [14].

Los enfoques que los gobiernos y las organizaciones internacionales realizan sobre la protección de infraestructuras no son siempre coincidentes. Las abundantes fuentes de información disponibles demuestran que los países en Norteamérica, en América Latina, la Unión Europea y Australia/Nueva Zelanda son aquellos donde se han realizado mayores avances en la planificación de la protección de las infraestructuras críticas.

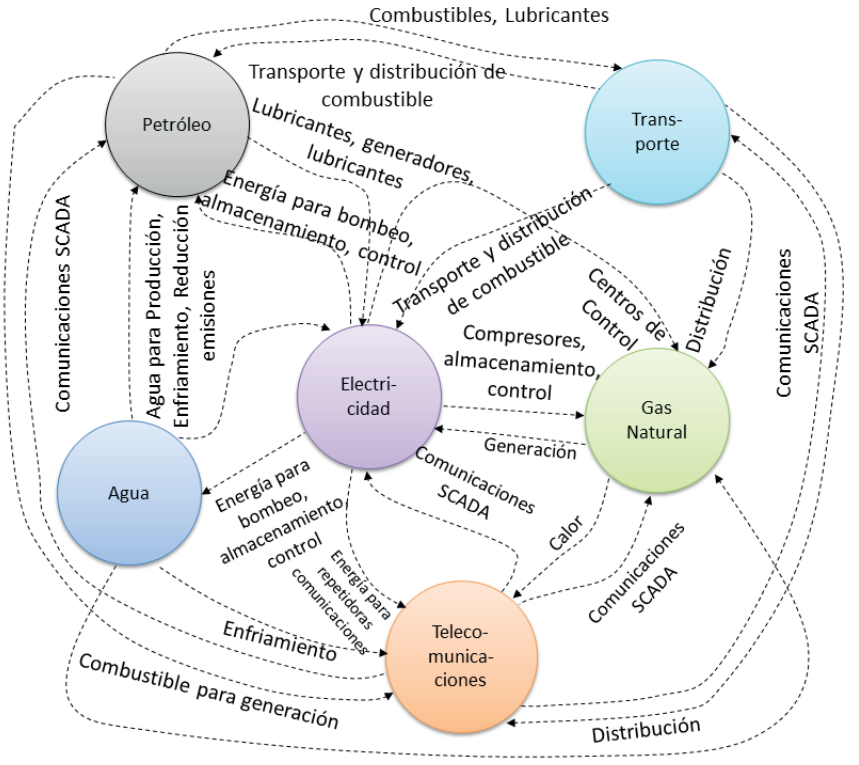

Figura 1: Ejemplo de interdependencia entre el sistema energético y otras infraestructuras críticas

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 en cualquier combinación de estas cuestiones [15].

Según la Directiva 2008/114/CE de la Unión Europea: las infraestructuras críticas se definen como todo elemento, sistema o parte de este situado en los Estados miembros que es esencial 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 [2].

De acuerdo con la Ley Española 8/2011 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 la operación 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 [4, 16].

A pesar de que a finales de los años 90 se identificó la posibilidad de un ataque cibernético a infraestructuras clave, solo a partir del 11-S se encontró la necesidad urgente de definir estrategias e iniciativas concretas de seguridad. Los acontecimientos de principios del siglo XXI, que afectaron notablemente a la opinión pública, en EEUU y en la Unión Europea, con motivo de los atentados terroristas en Nueva York (11 de septiembre de 2001), en Madrid (11 de marzo de 2004) y Londres (7 de julio de 2005), pusieron de manifiesto el riesgo de atentado terrorista contra las infraestructuras. En todos los casos, los gobiernos de EEUU y de la UE coinciden en que la respuesta debe ser rápida, coordinada y eficaz ante las nuevas amenazas [17].

Tanto los países que conforman la Unión Europea, como los Estados Unidos de América, constituyeron comités y mesas de trabajo sobre prevención, preparación y respuesta a los ataques terroristas, y como resultado, en el año 2005 se publicó en Bruselas el Libro Verde "Sobre un Programa Europeo para la Protección de Infraestructuras Críticas" [1]. Posteriormente, en diciembre de 2008 la Comisión Europea aprobó la directiva 2008/114 [2]. Por su parte, en los EEUU se aprobó en 2009 el Plan Nacional de Protección de Infraestructuras [3].

Estos programas proporcionan tanto a los gobiernos como al sector privado la oportunidad de aprovechar la experiencia colectiva para definir más claramente los sistemas de alertas en infraestructuras críticas, su protección, la planificación, así como las actividades de continuidad y fiabilidad de estas infraestructuras. Dichos programas de protección de infraestructura se concentran en los sectores de energía, transportes, tecnologías de la información y comunicaciones.

3.1 NIPP: PROGRAMA DE PROTECCION DE INFRAESTRUCTURAS DE ESTADOS UNIDOS

El NIPP (National Infrastructure Protection Plan) es un plan para las infraestructuras esenciales en Estados Unidos que proporciona un marco global y unificado para la protección de Infraestructuras Críticas y Recursos Claves (IC/RC), a través de entidades federales, estatales, locales y el sector privado [18], 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 [9].

El marco de gestión de riesgos, el NIPP define seis etapas bien diferenciadas: 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 efectividad. Adicionalmente, se proporciona un marco de retroalimentación y de mejora continua, flexible y adaptable a las situaciones de riesgo de cada sector. El esquema de este plan se presenta en la Figura 2.

Desde la perspectiva de cada sector de actividad, y dentro de la gestión de riesgos, en la etapa del **establecimiento de los objetivos de seguridad** se define la posición que se desea alcanzar en materia de seguridad. La pérdida de vidas, el impacto económico o en la seguridad nacional deben considerarse en el momento de formular los objetivos de seguridad.

La **identificación de recursos, sistemas, redes y funciones** consiste en la elaboración de un inventario completo que contenga información básica sobre estos asuntos en el país, y que pueda utilizarse para determinar los recursos, sistemas o redes que se clasifiquen como "críticos" 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 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 mediante la 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 de los servicios afectados.

Finalmente, la etapa de **medición de la efectividad** se establece a partir de un sistema de indicadores para aportar información sobre el logro de objetivos específicos de seguridad, definidos en [3].

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.

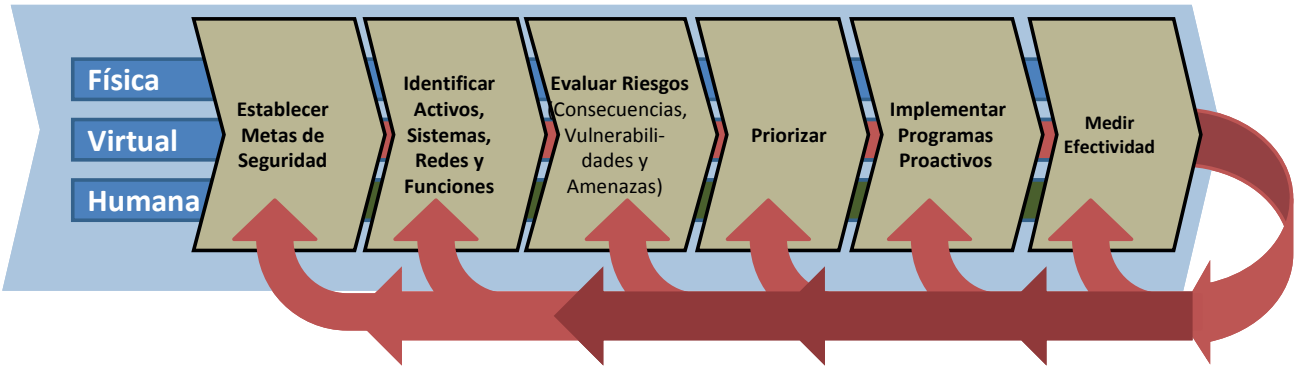

Figura 2: Marco de mejora continua para la protección de Infraestructuras Críticas y Recursos Clave [3].

3.2 PEPIC: PROGRAMA EUROPEO PARA LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

El objetivo general del PEPIC es mejorar la protección de las infraestructuras críticas de la Unión Europea. Este objetivo se alcanzará mediante la aplicación de la legislación europea presentada en las directivas y recomendaciones de la Comisión Europea [19]. El marco legislativo del PEPIC consta de los siguientes elementos [20]:

- 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.

Tanto el programa de Estados Unidos (NIPP) como el de la Unión Europea (PEPIC) definen las áreas críticas en las que deben centrarse los esfuerzos para la prevención y la protección de las infraestructuras. La Tabla 1 resume el listado de infraestructuras críticas definidas por cada uno de ambos programas.

La visión presentada por el NIPP es más amplia, dado que abarca una mayor cifra de sectores en los que se identifican infraestructuras críticas. Aunque la aproximación inicial realizada por la Comisión Europea en el Libro Verde [1] apuntaba inicialmente a cubrir un buen número de infraestructuras distintas, finalmente la Directiva 2008/114 [2] se enfocó básicamente en los sectores de energía y transporte.

3.3 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 [21].

Australia: la *Estrategia Nacional de Protección de Infraestructura Crítica* provee los principios generales para tal fin, describe las principales tareas y asigna las responsabilidades para su aplicación. La estrategia define, en el caso de este país, a la infraestructura crítica nacional como “aquellas instala-

Tabla 1: Listado de los Sectores de Infraestructuras Críticas, según los programas del NIPP (EEUU) y de la Directiva 2008/114 de la Unión Europea

IDENTIFICACIÓN MACROSECTORES (EEUU)	IDENTIFICACIÓN MACROSECTORES (UNIÓN EUROPEA)	
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		

ciones físicas, cadenas de proveedores, tecnologías de la información y redes de telecomunicaciones que si fueran destruidas, degradadas o no estuvieran disponibles por un período extenso de tiempo, podrían provocar un impacto significativo en el bienestar social y económico de la nación, o afectar la capacidad de Australia para conducir la defensa nacional y seguridad de la nación" [22].

La Estrategia se diseña a partir de la metodología contenida en el Estándar Australiano AS/NZS 4360:1999, una guía genérica para la implementación del proceso de gestión del riesgo, que comprende el contexto, la identificación, el análisis, la evaluación, el tratamiento, la comunicación y la monitorización de los riesgos en empresas y corporaciones [23]. La estrategia se aplica no solo a todos los niveles del gobierno, sino también a los propietarios y operadores de las infraestructuras.

El principal mecanismo empleado en Australia para el intercambio de información relevante relacionada con la protección de las infraestructuras críticas entre el gobierno y el sector privado es la *Trusted Information Sharing Network for Critical Infraestructure Protection*, establecida en el año 2004 y compuesta por un grupo de analistas de nueve sectores específicos que cubren las áreas de banca y finanzas, comunicaciones, energía, servicios de emergencia, cadenas de alimentos, salud, transporte y lugares de alta concentración de personas.

El Gobierno de Australia juega un papel importante en la protección de las infraestructuras críticas por medio de su agencia *National Infraestructure Information,* en la que están representados los propietarios y operadores de infraestructuras críticas australianas, a quienes se responsabiliza de asegurar sus activos y aplicar técnicas de gestión de riesgos a sus procesos.

Canadá: actualmente se encuentra en desarrollo la *Estrategia de Protección a la Infraestructura Crítica Nacional*, en la que se da gran importancia a la promoción de una gestión integrada del riesgo de las infraestructuras críticas, incluyendo componentes físicos y cibernéticos, aplicados tanto en el sector público como en el privado. Dado que el intercambio de información es un elemento esencial para la protección y aseguramiento de las infraestructuras críticas, se ha propuesto el mecanismo de las Actas de Gestión de Emergencias para facilitar el intercambio de información relativo a emergencias, incluyendo avisos de amenazas, instalaciones vulnerables, planes de continuidad de actividades y demás.

La política de seguridad de Canadá está contenida en el documento *Securing an Open Society: Canada´s National Security Policy*. El objetivo de esta política es asegurar que el gobierno está preparado para enfrentar y responder a diversas amenazas de seguridad como actos terroristas, enfermedades infecciosas, desastres naturales, ataques cibernéticos a infraestructura crítica [24]. Por otro lado, la organización *North American Electric Reliability Corporation* (NERC) promueve un programa conjunto de protección de infraestructuras de la red eléctrica de América del Norte (EEUU y Canadá), en el que se establecen normas de obligado cumplimiento, evaluaciones de riesgos, difusión de información crítica mediante alertas a la industria y la sensibilización sobre cuestiones clave de seguridad.

España: en el país ibérico se ha puesto en marcha el *Plan Nacional de Protección de Infraestructuras* y se ha constituido el *Centro Nacional de Protección de Infraestructuras Críticas* [25], organismo que tiene como misión principal la coordinación de las actividades de los agentes implicados en la protección de las infraestructuras críticas, tanto en el sector público como el privado, y la elaboración de planes generales de protección, así como planes específicos de cada sector. El CNPIC es el órgano director y coordinador de cuantas actividades relacionadas con la protección de las infraestructuras críticas tiene encomendadas la Secretaría de Estado de Seguridad del Ministerio del Interior, al cual está adscrito.

En coordinación con el CNPIC se ha impulsado también la creación del CCN-CERT, que es un órgano gubernamental con capacidad de respuesta a incidentes de Seguridad de la información del *Centro Criptológico Nacional* (CCN), dependiente del *Centro Nacional de Inteligencia* (CNI). Se constituyó a principios de 2008, estando presente desde entonces en los principales foros internacionales en los que se comparten objetivos, ideas e información sobre la seguridad de forma global [26].

El CNPIC ha orientado claramente sus esfuerzos a la protección de las infraestructuras críticas desde un punto de vista holístico, de acuerdo a la tendencia de integración de la seguridad física con la seguridad cibernética.

Los planes de protección de infraestructura crítica articulan sus políticas a partir de la normativa establecida en la Ley 8/2011 [4] y el Real Decreto 704/2011 [16], que puede ser considerada una de las legislaciones más completas en el ámbito internacional referida a este tema.

Francia: la coordinación interministerial en materia de defensa y de seguridad nacional es realizada mediante la *Secretaría General de la Defensa y de la Seguridad Nacional* (Secrétariat General de la Défense Nationale –SGDSN-, [27]), servicio del Primer Ministro que trabaja en estrecha relación con la Presidencia de la República y que asiste al Jefe del Gobierno en el ejercicio de sus responsabilidades en materia de defensa y de seguridad nacionales.

En ese ámbito, la SGDSN asume la secretaría de los consejos de defensa y de las reuniones interministeriales de alto nivel celebradas bajo la presidencia del Jefe de Estado, del Primer Ministro o de sus principales colaboradores.

La SGDSN se ocupa, igualmente, de ciertas funciones permanentes o misiones puntuales, confiadas a los servicios del Primer Ministro en razón de su naturaleza interministerial o de la evolución institucional. Más allá de la permanencia de sus misiones fundamentales, la SGDSN en estos últimos años ha conocido una ampliación sensible de su campo de acción a los retos de seguridad nacional en el sentido más extenso: se sitúa hoy en el punto de convergencia del conjunto de las cuestiones relacionadas con la seguridad interior y exterior de Francia. El SGDSN ha generado el Libro Blanco sobre Defensa y Seguridad Nacional, que es una iniciativa que nace a partir de la Directiva Europea 2008/114. Adicionalmente, se han constituido algunos órganos como el *Centre opérationnel de la sécurité des systèmes d'information* (COSSI) y se ha desarrollado el Plan PIRANET para la prevención y la protección contra ataques informáticos.

Países Bajos: el gobierno de los Países Bajos ha constituido el *Centro Nacional de Asesoría sobre Infraestructuras Críticas* (*Nationaal Adviescentrum Vitale Infrastructuur,* [28]), organismo que tiene conocimiento y experiencia en la seguridad de infraestructuras esenciales y el objetivo de compartir estos con empresas privadas y entidades públicas de los sectores involucrados. En los Países Bajos, NAVI ofrece servicios de soporte para análisis de riesgo y asesoría en seguridad, buenas prácticas y contactos internacionales. Adicionalmente, se ha constituido en Holanda el grupo GOVCERT.nl que, tomando la metodología CERT, ha propuesto un conjunto de medidas para proteger la infraestructura crítica de sistemas de información [29].

En Holanda el intercambio de información se realiza en diferentes foros, entre otros en las reuniones periódicas del *National Crisis Centre*. La retroalimentación entre el gobierno y el sector privado es una parte integral de la gestión de riesgo en este país. Existe un acuerdo entre el gobierno y los grandes operadores de infraestructuras críticas, mediante el cual estos últimos se encuentran sometidos a la obligación de informar sobre las interrupciones o fallos que puedan presentar, a partir de ciertos niveles de severidad, los sistemas que administran.

Países Latinoamericanos: los gobiernos de los países latinoamericanos han encargado generalmente la protección de las infraestructuras críticas a los operadores de los sistemas y redes. Esta tarea se realiza siempre a través de una fuerte relación con

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 en los países latinoamericanos se basan en los marcos de gestión de riesgos conocidos, ya sea el estándar australiano [23] o la norma ISO 31000 [30].

Sin embargo, a partir del año 2008 ha surgido una notable preocupación, especialmente en el área de la seguridad de las redes y sistemas de tecnologías de la información, para cuya protección se opta por seguir los ejemplos y recomendaciones de organizaciones y expertos internacionales (ONU, OEA, OTAN, ITU) para luchar contra ciberataques y contra el cibercrimen [29].

Las políticas para la protección de la infraestructura de información se focalizan en dos aspectos: internet y telecomunicaciones, de conformidad con la metodología CERT/CSIRT (Computer Emergency Response Team) que es un nombre dado a los grupos de expertos que se encargan de incidentes de seguridad informática. El CERT/CSIRT es un término genérico que se refiere a una parte esencial de los centros de coordinación nacionales que involucran a las juntas de gobierno y las empresas en la seguridad cibernética. Los dos sectores no pueden ser separados ya que están íntimamente ligados, y los intereses de los proveedores de internet y telecomunicaciones para operar redes seguras están interrelacionados [31].

Entre las principales iniciativas de los países latinoamericanos se encuentra la organización de grupos de trabajo adscritos a los Ministerios de Defensa, en países como Brasil [32] y Colombia [33], pioneros en la implementación de estrategias contra ataques informáticos. Otros países como Chile, México y Venezuela, se encuentran aún en proceso de análisis y conformación de los CERT gubernamentales.

Reino Unido: el gobierno británico ha creado el *Centro de Protección de la Infraestructura Nacional* (*Centre for the Protection of National Infrastructure*, [34]). Dentro de esta iniciativa se presentan nueve sectores de infraestructura crítica –comunicaciones, servicios de emergencia, energía, finanzas, alimentos, gobierno, salud, transporte y agua –y cada uno incluye recursos y servicios que son esenciales en todos los niveles de la sociedad. CPNI es una organización interdepartamental, con recursos de la industria, la academia y una serie de departamentos y organismos oficiales. Entre estos, se incluye el Servicio de Seguridad, el CESG (autoridad técnica nacional del Reino Unido para el aseguramiento de la información) y otros departamentos ministeriales responsables de los sectores de infraestructura nacional.

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 para los que 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.

3.4 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 [4], y se da cumplimiento a la transposición a la legislación nacional de la Directiva 2008/114/CE [35]. La Ley crea el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), órgano adscrito al Ministerio del Interior por medio 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 y 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 2008/114/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 [4]:

- 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 mediante Real Decreto 704/2011 del 20 de mayo de 2011, con la finalidad de desplegar los instrumentos de planificación y ejecución de los programas de protección [16]:

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 estos, 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 que 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 la empresa Red Eléctrica de España S.A.

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 [25]:

- 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 puesta en marcha se prevee 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; deberá contar para ello con el apoyo y colaboración de los agentes del sistema y de todos aquellos otros organismos o entidades afectados [16]. 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 [36].

4. CADENA DE VALOR DE INFRAESTRUCTURAS ELÉCTRICAS

Los riesgos asociados a los sistemas eléctricos no están localizados solamente en la etapa de producción de electricidad; afectan en general a todas las etapas de la cadena de valor: generación, transporte, distribución y comercialización de la electricidad. En la Figura 3 se presenta un esquema de los subsistemas que componen la cadena de valor de los sistemas eléctricos.

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 en España el sistema de líneas y subestaciones de 220 y 400 kV, cuyo principal operador es Red Eléctrica de España S.A. [37].

Desde el punto de vista de la infraestructura, la red cuenta con algunos nodos críticos en los cuales el sistema requiere ser suficientemente seguro como para permitir una interrupción controlada en caso de un suceso no previsto. En otras circunstancias, 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.

Aunque es indudable la necesidad de proteger la red de mayor escala, es decir, la red de transporte en alta tensión, también requieren cuidado 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 [38]. Es importante tener presente que la tarea de protección de estas infraestructuras tan extensas y numerosas debe realizarse en la medida que sea viable técnica y económicamente. 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 [39]. 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.

El aumento de los requerimientos de seguridad en Europa y Norteamérica coincide también con una época de mejora continua de los servicios públicos, en el que las empresas operadoras están preocupadas por incrementar la fiabilidad de sus actividades de suministro para maximizar su beneficio. Sin embargo, teniendo en cuenta que se trata de una infraestructura tan vasta, es imposible garantizar la seguridad física de las redes eléctricas al 100% [40]. En general, se detecta una alta vulnerabilidad del sistema eléctrico en aquellos nodos de la red donde un fallo pueda propagarse en cascada y causar apagones en una región o en uno o varios países. El

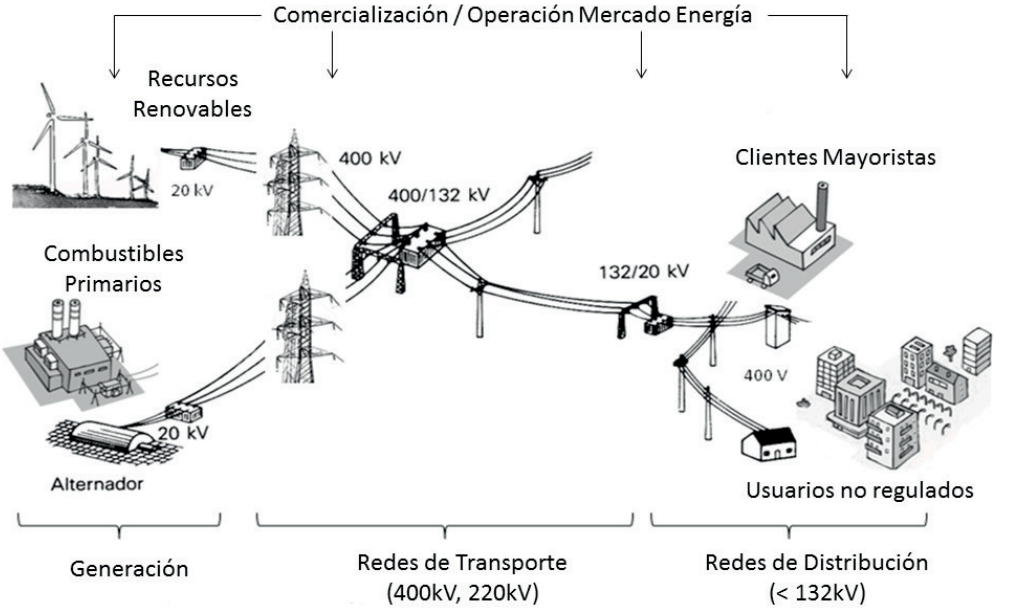

Figura 3: Subsistemas de la cadena de valor del sistema eléctrico

nivel de amenaza, sin embargo, es difícil de valorar, hasta que se alcancen grados mayores de coordinación entre los sectores público y privado involucrados en el sistema eléctrico.

5. IDENTIFICACIÓN DE RIESGOS EN INFRAESTRUCTURAS ELÉCTRICAS

La infraestructura energética alimenta la economía en cualquier nación. Sin un suministro de electricidad estable, la salud y el bienestar se ven amenazados y la economía del país no puede funcionar. Esta infraestructura se puede dividir en tres grandes segmentos interrelacionados: electricidad, petróleo y gas natural. El sector eléctrico concentra una importante cantidad de estudios y análisis, dada la alta interdependencia de todos los sectores de actividad con las infraestructuras de suministro de electricidad.

Para el caso concreto de las infraestructuras del sector eléctrico, se pueden emplear los procesos del marco de gestión del riesgo aplicables a las infraestructuras críticas: Identificación de Amenazas, Evaluación de Riesgos, Priorización de Acciones, Implementación de Programas y Medición de Efectividad.

El primer paso consiste en la identificación de riesgos y amenazas al sistema de infraestructura. Constituye la piedra angular de la actuación en la protección de infraestructuras críticas, ya que los criterios para la selección de las posibles amenazas y el análisis detallado de sus componentes de riesgo serán determinantes en la calidad del proceso de gestión de riesgos en infraestructuras. La identificación de riesgos es la etapa fundacional de cualquier proceso de gestión de riesgos, y es previa a la valoración, definición e implementación de acciones para mitigarlos.

En un marco de gestión de riesgos, el proceso de identificación se enfoca en detectar cuáles son las fuentes principales de riesgo [23, 41]. En resumen, el propósito al realizar el proceso de identificación de riesgos se limita a un ejercicio cualitativo, mediante el cual se definen los posibles riesgos en el sistema, y se obtiene un listado completo de riesgos y sus componentes aplicable a la cadena de valor y al ciclo de vida de la red de infraestructura [42].

Una revisión del estado del arte de las herramientas y metodologías para la identificación de riesgos permite concluir que la aplicación sistemática de una metodología debe seleccionar activos críticos, verificar interdependencias e impactos económicos y sociales de los riesgos, desde el punto de vista organizacional, empresarial y gubernamental [21].

La identificación de riesgos por medio de las herramientas y metodologías citadas tiene aplicación en los subsistemas de la cadena de valor de la infraestructura eléctrica, 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 definición de medidas de protección será una actividad posterior a la identificación y evaluación de las amenazas, su impacto y probabilidad. Estas medidas son elementos de defensa desplegados para que las amenazas no causen daños [36].

Una de las técnicas que permite un enfoque integral más completo del análisis de la vulnerabilidad de un sistema de infraestructura son los **mapas de riesgos** [21, 43]. 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 riesgos, asociados tanto a la red eléctrica como al entorno de la organización que la gestiona.

Pero, ¿hasta qué punto es factible aplicar la metodología de mapas de riesgos? Tanto el mapa de riesgos, como las componentes, necesitan del conocimiento íntimo de la organización. Existirán riesgos que afecten a toda la cadena de valor, y a cada nivel de la organización. A modo de ejemplo, un modelo de mapa de riesgos se puede aplicar a un activo específico de la red de infraestructura, como puede ser una subestación eléctrica (menor nivel de abstracción, en el ámbito operativo), o a la organización completa (mayor nivel de abstracción, en al ámbito estratégico) [44].

Para la construcción de un mapa de riesgos es indispensable recoger y gestionar gran cantidad de información, lo que a menudo es difícil dada la inexistencia, la inaccesibilidad y la falta de fiabilidad de muchos de los datos necesarios.

El *mapa de riesgo* permite simplificar el número de categorías que agrupan las componentes de riesgo, lo cual implica la identificación de los incidentes tanto internos como externos a un sistema de infraestructura crítica. Se distinguen las siguientes categorías de riesgos, aplicables al sistema de infraestructura crítica [44, 45]:

- **Cumplimiento e Indicadores:** están relacionados con las amenazas provenientes de la expedición de políticas, leyes y regulaciones y su impacto en el desarrollo económico y social de la región o nación en la que se implanta la infraestructura.
- **Activos y Finanzas:** se derivan de la volatilidad de los mercados y de la economía, que pueden afectar el normal funcionamiento y/o la expansión de las redes de infraestructura eléctrica. También se incluyen los riesgos relacionados con la cartera de cobros pendientes, 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 relacionados con aspectos jurídicos, políticos, sociales, fenómenos naturales, entre otros, que afectan las operaciones y el normal funcionamiento de la red de infraestructura eléctrica.
- **Operacionales:** aquellos que afectan los procesos, sistemas, personas y cadena de valor dentro del sistema de infraestructura eléctrica. Pueden corresponder a fallos en la ejecución de actividades, deficiencia o ausencia de procedimientos, y fallos en la gestión del capital humano, tecnológico y administrativo, que afectan el funcionamiento y el crecimiento de la red de infraestructura.
- Además, la conveniencia de indicar el origen técnico o no técnico de un riesgo, permitirá definir posteriores responsabilidades en su tratamiento, según se propone a continuación [5]:
- **Amenazas de tipo técnico.** Incluyen los riesgos financieros y los riesgos operacionales; también, aquellas amenazas ocasionadas como consecuencia de los sistemas, los procedimientos, las decisiones y las actuaciones de personas que puedan afectar al sistema de infraestructura.

- **Amenazas de tipo no-técnico.** Incluyen los riesgos de entorno, los riesgos estratégicos y los riesgos de asignación de recursos; además, aquellos que se materializan como consecuencia de factores ajenos a la red de infraestructura, tales como: fenómenos naturales, situaciones sociopolíticas, acciones de terceros, decisiones de autoridades administrativas, regulatorias, entre otras.

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.

La elaboración de un mapa de riesgos para infraestructura eléctrica recopila todos los requerimientos establecidos al comienzo del presente artículo. En la figura 7 se muestra un mapa de riesgos genérico, aplicado al sistema de infraestructura crítica del sector eléctrico [44].

En este mapa de riesgos interconectado, el grosor de la línea indica la fuerza de las interconexiones o relación entre los riesgos. Asimismo, la proximidad entre los componentes de los riesgos es mayor cuanto más interconectados se encuentran.

Para efectuar el estudio detallado de cada uno de los riesgos del mapa es preciso realizar la identificación de sus componentes. Aunque el propósito de este artículo 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 su sistema de gestión de riesgo, realizan el desglose en forma de componentes [46-48]. Para el caso particular de los 21 riesgos establecidos para la red de infraestructura eléctrica, se ha determinado un listado de 141 componentes de riesgos, que pueden consultarse en [44, 49].

En el marco de la gestión de riesgos, la propuesta metodológica de identificación con 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 [50].

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 seguridad.

6. CONCLUSIONES

La seguridad, la prosperidad económica y bienestar social en cualquier país dependen de un complejo sistema de infraestructuras interdependientes. Particular atención reciben aquellas relacionadas con la infraestructura eléctrica y su cadena de valor, tanto en el ámbito organizacional como de los activos físicos que componen la infraestructura.

Como respuesta a la necesidad de aplicar planes de protección de infraestructura, inspirados en las múltiples iniciativas internacionales de la última década y en la reciente legislación española aprobada en 2011, es preciso iniciar programas de gestión de riesgos que garanticen la aplicabilidad de dichos planes. Un primer paso consiste en la identificación de riesgos y amenazas al sistema de infraestructura, sobre la que se edifique el proceso de protección de infraestructuras críticas.

Para la identificación de amenazas en el sistema eléctrico se sugiere la utilización de la técnica de mapas de riesgos, que permite un análisis integral en el entorno completo de la organización que gestiona las infraestructuras. Un mayor nivel de detalle en esta actividad requiere la determinación de componentes de riesgos, preferiblemente 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.

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.

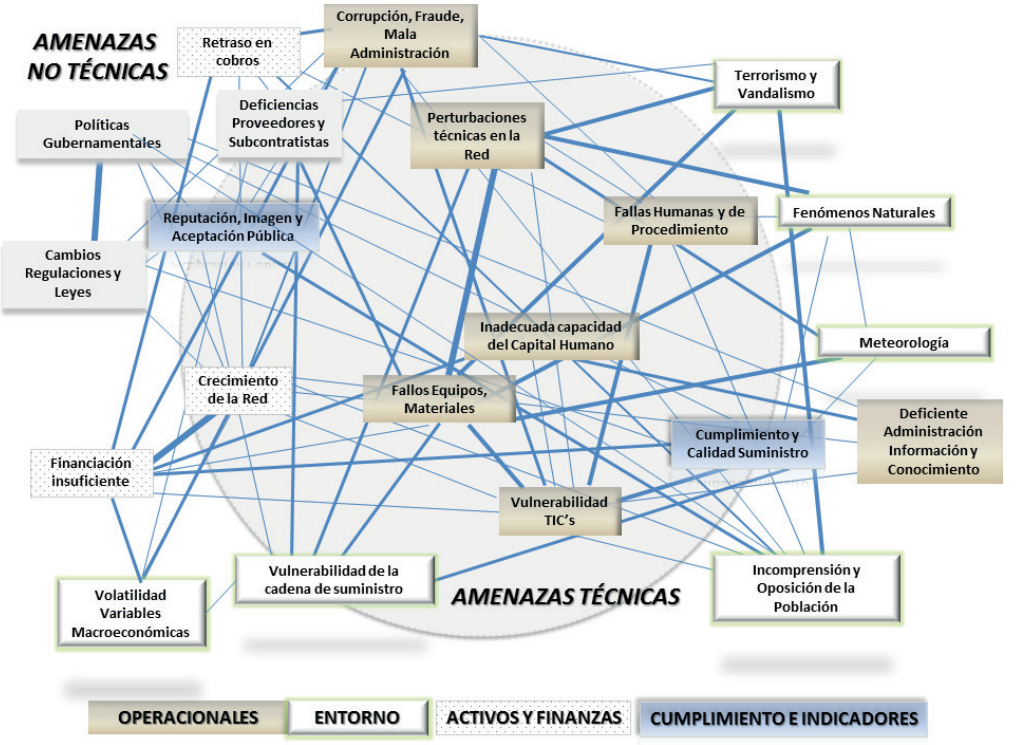

Figura 4: Propuesta de mapa de riesgos e interdependencias aplicado a la red de infraestructura crítica en el sector eléctrico

REFERENCIAS BIBLIOGRÁFICAS

[1]. Comisión Europea, "Libro Verde: Sobre un Programa Europeo para la Protección de Infraestructuras Críticas". *Comisión de las Comunidades Europeas*, Bruselas (Bélgica). 2005, 28p. Disponible en: http://www.proteccioncivil.net/Documentos%20pdf/LIBRO%20VERDE%20SOBRE%20UN%20PROGRAMA%20EUROPEO%20PARA%20LA%20PROTECCI%C3%93N%20DE%20INFRAESTRUCTURAS%20CR%C3%8DTICAS.pdf

[2]. Consejo Europeo. "Sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección", Directiva 114 CE/2008, *Diario Oficial de la Unión Europea,* Bruselas (Bélgica), 2008, 24p. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:ES:PDF

[3]. NIPP, "National Infrastructure Protection Plan", Washington DC (USA): *U.S. Department of Home Security*, 2009, 175 p.. Disponible en: http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

[4]. BOE, "Ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas.," Madrid (España), *Boletín Oficial del Estado del Reino de España*, 2011, 11p.

[5]. J.M. Yusta, "Amenazas a la seguridad del suministro energético español. Inteligencia y seguridad". *Revista Inteligencia y Seguridad,* N° 6, 2009, .pp. 223-252.

[6]. Giroux, J. "A Portrait of Complexity: New Actors and Contemporary Challenges in the Global Energy System and the Role of Energy Infrastructure Security". Capítulo Libro *Risk, Hazards & Crisis in Public Policy*, Wiley. Edición 1, pp 33–56. doi: 10.2202/1944-4079.1034

[7]. B. Morel, I. Linkov, D. A. Belluck, R. N. Hull, S. L. Benjamin, J.Alcorn, I. Linkov, "Environmental Security, Critical Infrastructure and Risk Assessment: Definitions and Current Trends," *Environmental Security and Environmental Management: The Role of Risk Assessment*. Springer Netherlands, vol. 5, pp. 1-16, 2006.

[8]. US Dept Home Security, “Critical infrastructure and key resources sectors” *U.S. Department of Homeland Security*, 2012. Disponible en: http://www.dhs.gov/critical-infrastructure-and-key-resources-support-annex

[9]. T. Consolini, “Regional security assessments: A strategic approach to securing federal facilities,” Tesis Magistral en *Safety Naval Postgraduate School*, Monterrey, CA (USA), 2009, 103p.

[10]. L. Ness, “Securing Utility and Energy Infrastructures”. Wiley Interscience. Washington DC (EEUU), 340p, 2006.

[11]. E. Michel-Kerjan “New Challenges in Critical Infrastructures: A US Perspective”. *Journal of Contingencies and Crisis Management*, Vol. 11, N° 3, p. 132-141, 2003.

[12]. J.M. Arroyo “Análisis de Vulnerabilidad en Sistemas de Potencia”, Artículo de trabajo, 2010, Disponible en: http://www.dee.feis.unesp.br/lapsee/arquivos/down_materiaiscursos/2008_nataliajose/9_analisis_vulnerabilidad.pdf

[13]. R. Hull, D. Belluck, & Lipchin, C. “A framework for multi-criteria decision making with special reference to critical infrastructure: policy and risk management working group summary and recommendations” Capítulo Libro: Ecotoxicology, Ecological Risk Assessment and Multiple Stressors. Springer, pp. 355-370, 2006,

[14]. A. Löschel, U. Moslener, D. Rübbelke, “Indicators of energy security in industrialised countries”, *Energy Policy*, pp. 1665-1672, 2010.

[15]. US Dept Energy Office, “Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities”, Washington DC (USA): U*.S. Department of Energy, Office of Energy Assurance*, 26p, 2002.

[16]. BOE, “Real Decreto 704/2011, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.,” Madrid (España), *Boletín Oficial del Estado del Reino de España*, 2011, 18p.

[17]. CIEP, “Study: EU Energy Supply Security and Geopolitics”, Clingendael International Energy Programme, La Haya (Holanda), 2004, 281p. Disponible en: http://www.clingendaelenergy.com/publications/publication/study-eu-energy-supply-security-and-geopolitics

[18]. US Dept Home Security, “Directive 7: Critical Infrastructure Identification, Prioritization, and Protection,” U.S. Department of Homeland Security, 2003.

[19]. V. Costantini, F. Graccevaa, A. Markandyaa, G. Vicini, “Security of energy supply: Comparing scenarios from a European perspective,” *Energy Policy*, pp 210-226, 2007.

[20]. Comisión Europea, “Síntesis de la legislación de la UE: Lucha contra el terrorismo”. Comisión de las Comunidades Europeas, Bruselas (Bélgica). 2006, 30p. Disponible en: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_es.htm.

[21]. J. M. Yusta, G. J. Correa, and R. Lacal-Arántegui, “Methodologies and applications for critical infrastructure protection: State-of-the-art,” *Energy Policy*, vol. 39, pp. pp. 6100-6119, 2011.

[22]. CSIRO, Informatics and Statistics, “CIPMA: Critical Infrastructure Protection Modeling and Analysis.” Clayton (Australia): CSIRO Mathematics, Informatics and Statistics, 2008. Disponible en: http://www.csiro.au/partnerships/CIPMA.html.

[23]. AS/NZS, “Estándar Australiano de Administración del Riesgo,” AS/NZS 4360, 1999, 36 p.

[24]. H. M. Abdur Rahman, “Modelling and Simulation of Interdependencies between the Communication and Information Technology Infrastructure and other Critical Infrastructures,” Tesis Doctoral en: Electrical and Computer Engineering, University of British Columbia, Vancouver (Canadá), 2009, 163p.

[25]. CNPIC, “Centro Nacional de Protección de Infraestructuras Críticas en España.”, Madrid (España), 2010. Disponible en: http://www.cnpic-es.es/cnpic

[26]. CCN-CERT, “Centro de Incidentes del Centro Seguridad de la Información del Centro Criptológico Nacional”, Madrid (España), 2011.

[27]. CCN-CERT, “Centro de Incidentes del Centro Seguridad de la Información del Centro Criptológico Nacional”, Madrid (Spain), 2011. Disponible en: www.sgdn.gouv.fr

[28]. NAVI, “Nationaal Adviescentrum Vitale Infrastructuur.”, Amsterdam (Holanda), 2011: Disponible en: http://www.navi-online.nl

[29]. A. Zielstra, “GOVCERT: Cybercrime Information Exchange. in Cybersecurity and Critical Infrastructure Protection”. 2010. Madrid (España). Disponible en: http://www.cipre-expo.com/speakers/annemarie-zielstra

[30]. ISO, “Norma ISO 31000, para la Gestión de Riesgos.”, International Standard Organization, Geneve (Switzerland), 2010. Disponible en: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170

[31]. Alberts, C., et al., “CERT/CSIRT: Computer Security Incident Response Team”, *Carnegie Mellon University*: Pittsburgh, PA (EEUU), 2004. Disponible en: http://www.cert.org/resilience/publications/index.cfm

[32]. CERT.br, “Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil”, Brasilia (Brasil), 2011. Disponible en: www.cert.br

[33]. CERT-CCIT, “Centro de Coordinación Informática Colombia.”, Bogotá (Colombia), 2011. Disponible en: www.cert.org.co

[34]. CPNI, “Centre for the Protection of National Infrastructure” Londres (Reino Unido), 2011. Disponible en: www.cpni.gov.uk

[35]. European Comission, “European Network and Information Security Agency”, *Official Journal of the European Communities*, Bruselas (Bélgica), 2005, 12

[36]. CCN-CERT, “Centro de Incidentes del Centro Seguridad de la Información del Centro Criptológico Nacional”, Madrid (España), 2011. Disponible en: http://www.cii-murcia.es/informas/abr05/articulos/Analisis_gestion_riesgos_seguridad_sistemas_informacion.php

[37]. REE. “Mapas de la red eléctrica de transporte”, *Red Eléctrica de España S.A*: Madrid (España), 2013.

[38]. G. J. Correa and J. M. Yusta, “Structural vulnerability in transmission systems: Cases of Colombia and Spain,” *Energy Conversion and Management*, vol. 77, pp. 408-418, 2013.

[39]. P. Curtis, “Maintaining Mission Critical Systems in a 24/7 Environment”. IEEE Press Series on Power Engineering, ed. J.W. Sons. Rosenwood, MA (EEUU), 2007, 484p.

[40]. C. Martenson, “The Crash Course”, 2009. Disponible en: http://www.chrismartenson.com

[41]. ICONTEC, “Norma Técnica Colombiana para 5254 la Gestión de Riesgos,” Instituto Colombiano de Normas Técnicas, 2004, 44p

[42]. J. Johansson, “Risk and Vulnerability Analysis of Interdependent Technical Infrastructures” Tesis Doctoral en Industrial Electrical Engineering, University of Lund (Sweden), 189p, 2010.

[43]. AON, “Global Risk Managemente Survey,” Chicago, IL (USA): *Aon Corporation*, 2010

[44]. G.J., Correa, J.M. Yusta, & R. Lacal-Arántegui, “Using interconnected risk maps to assess the threats faced by electricity infrastructures*”. International Journal of Critical Infrastructure Protection*, Vol. 6, N° 4, 2013, pp. 197-216.

[45]. B. López, D. Arboleda, “Integración del manejo de riesgo e incertidumbre en la planeación financiera de empresas de transmisión de energía.,” *Revista CIER*, Montevideo (Uruguay), Vol. 54, 2010, pp. 80-88,

[46]. JP-Morgan, “Corporate Metrics,” *J.P. Morgan & Co Technical Document*, New York, NY (USA), 1999.

[47]. ISAGEN “Mapa de Riesgos ISAGEN”. *Documentos ISAGEN*, 2013. Disponible en: www.isagen.com.co

[48]. ISA. “Política para la gestión integral de riesgos grupo empresarial ISA”. Documentos ISA, 2013. Disponible en: http://www1.isa.com.co/irj/go/km/docs/documents/ContenidoInternetISA/ISA

[49]. G. Correa, “Identificación y Evaluación de Amenazas a la Seguridad de Infraestructuras de Transporte y Distribución de Electricidad,” Tesis Doctoral en Energías Renovables y Eficiencia Energética, Universidad de Zaragoza, Zaragoza (España), 238p, 2012

[50]. CNA, “Powering America’s Defense: Energy and the Risks to National Security”. *Bipartisan Policy Center, the Energy Foundation, and the Grayce B. Kerr Foundation:* Washington, DC (EEUU), 2013. Disponible en: https://www.cna.org/reports/energy