CEDS. CENTRO DE ENERGIA Y DESARROLLO SUSTENTABLE udp
FACULTAD DE INGENIERÍA

Antecedentes para el Análisis de Seguridad del Suministro Eléctrico en Chile ante Eventos Catastróficos de Origen Natural

Claudio Huepe Minoletti

Marzo, 2013

Documento de Trabajo Nº: 05

Antecedentes para el Análisis de Seguridad del Suministro Eléctrico en Chile ante Eventos Catastróficos de Origen Natural

Claudio Huepe Minoletti [1]

Marzo, 2013

Documento de Trabajo nº5

[1] Claudio Huepe Minoletti. *Coordinador del Centro de Energía y Desarrollo Sustentable, Facultad de Ingeniería, Universidad Diego Portales. Ingeniero Comercial, Economista y Magister en Economía PUC. MSc en Economía de los Recursos Naturales y del Medio Ambiente (UCL, Londres).*

Citar documento como:

Huepe, C. (2013). *Antecedentes para el Análisis de Seguridad del Suministro Eléctrico en Chile ante Eventos Catastróficos de Origen Natural* (Documento de Trabajo nº5). Santiago de Chile: Centro de Energía y Desarrollo Sustentable

Centro de Energía y Desarrollo Sustentable

Facultad de Ingeniería, Universidad Diego Portales

Ejército 441, Santiago.

www.energiaydesarrollo.udp.cl

Resumen Ejecutivo

El análisis de seguridad para infraestructura cobra creciente importancia en todo el mundo. Este análisis considera típicamente tres aspectos separados de seguridad: amenaza, vulnerabilidad y resiliencia, aun cuando no siempre la separación sea nítida. En el caso de Chile no ha existido trabajo sistemático en este sentido y existen debilidades significativas en los tres ámbitos mencionados, aún cuando con posterioridad al terremoto de 2010 ha habido esfuerzos importantes.

Existen experiencias internacionales útiles para el análisis de seguridad, metodologías y buenas prácticas relevantes y útiles para el caso chileno, aun cuando no existe ***una*** fórmula establecida y única. Por lo anterior, es necesario identificar los elementos pertinentes para el caso chileno y adaptar metodologías en función de los objetivos deseados. Un elemento clave está en identificar con cierta precisión los alcances y objetivos del ejercicio así como las interdependencias que serán consideradas y la profundidad del estudio.

En consecuencia, si bien la brecha para avanzar en un análisis de seguridad de suministro eléctrico ante eventos (catastróficos) naturales en relación con países desarrollados es muy grande e incluye tanto información básica como de metodologías, existen estrategias que son aplicables en Chile una vez que se defina con precisión el alcance que se le quiere dar al análisis. Es decir, si bien puede requerirse mucho tiempo y recursos para cerrar la brecha por completo, es posible reducirla significativamente con una estrategia adecuada. En particular, se debe considerar dentro de dicha estrategia la resiliencia sistémica como un elemento muy importante del análisis global.

La importancia de los análisis de seguridad que se observa en la experiencia internacional, sugiere la urgente necesidad de desarrollar una estrategia aplicable a Chile que permita contar con un análisis de seguridad de suministro eléctrico ante catástrofes naturales útil para avanzar en medidas que reduzcan el riesgo y mejoren la resiliencia.

La magnitud de la brecha es tal que se hace imperativo avanzar en reducirla de la manera más efectiva y eficiente posible. Este trabajo se propone una estrategia viable para ello.

Índice

1. Introducción

El presente trabajo se propone identificar, en forma sintética y estructurada, los elementos relevantes para un análisis de seguridad del suministro eléctrico frente a la amenaza de eventos catastróficos naturales[1], orientado a diseñar medidas apropiadas para alcanzar un nivel de riesgo de suministro aceptable.

Los objetivos específicos del trabajo son:

1) Identificar la situación actual en Chile en materia de análisis de seguridad de suministro de los sistemas eléctricos frente a eventos naturales.
2) Identificar buenas prácticas (nacionales o internacionales) en análisis de seguridad, aplicables a suministro de sistemas eléctricos y frente a eventos naturales.
3) Identificar (en un formato sintético y estructurado) las brechas para un análisis de seguridad eléctrico en Chile que permita diseñar medidas para alcanzar un nivel de riesgo aceptable, y una metodología para cerrar dichas brechas.

Para lograr los objetivos, en primer lugar se presenta un marco conceptual que entrega una estructura ordenada para el análisis. Luego, se revisa, en términos generales, la información disponible en materia de seguridad relacionada al sector eléctrico nacional. Posteriormente, se revisan algunas metodologías estándar de análisis de riesgo (tales como análisis cuantitativo, análisis probabilístico, análisis preliminar de peligros) aplicadas o aplicables a suministro eléctrico (características, desarrollo y resultados), buscando, en particular, obtener referencias internacionales que puedan considerarse como un *benchmark* en términos de análisis de seguridad ante catástrofes naturales para Chile.

Finalmente, se presenta una identificación de ordenada y coherente de las brechas existentes en el análisis de riesgo nacional y algunas conclusiones generales para su mejoramiento.

2. Marco Conceptual

Para efectos de desarrollar y organizar el trabajo, se presenta un breve marco conceptual que permite reducir la ambigüedad que existe en el uso corriente del lenguaje en esta materia. Si bien no existe una nomenclatura completamente estándar dentro de los trabajos de análisis de seguridad y riesgo, hay un grado importante de consenso sobre el cual se ha construido definiciones claras y coherentes.

Por seguridad se entiende normalmente estar protegido de un peligro que afecta el estado "normal" de las cosas. Para efectos de este trabajo la atención está sobre el suministro eléctrico mismo, no sobre los usuarios de la electricidad, por lo que lo relevante será el funcionamiento de la infraestructura pertinente. Cabe notar, que se distingue generalmente dos focos de análisis de seguridad en función del *objeto*: el análisis al nivel de componente (en el caso del presente informe, el suministro eléctrico) y el análisis al nivel social (donde la seguridad depende de un conjunto de componentes). Buena parte de los trabajos actuales toman el segundo enfoque pues

[1] Si bien, muchos aspectos del análisis son equivalentes, no se incorpora explícitamente en este estudio los temas relacionados con disponibilidad de energía primaria, fallas o accidentes operacionales o acciones antrópicas externas.

la seguridad energética se integra dentro de la "seguridad nacional" y, por lo tanto, se considera, en el fondo, como un fenómeno social.

La seguridad es dependiente (inversamente) de los impactos (potenciales) resultantes de los peligros existentes (*amenazas*) para una infraestructura particular (los *riesgos*) y de la capacidad de reponerse de estos impactos (la *resiliencia*). Un análisis ***de seguridad*** en este marco, incluye, por lo tanto, dos aspectos: el análisis de ***riesgo*** y el análisis de ***resiliencia***.

Se puede distinguir dos enfoques para estudiar los riesgos**.** Uno de estos es probabilístico (expresando las amenazas en funciones matemáticas) y el otro es determinístico (cualquiera sea la probabilidad de las amenazas). Dada la multiplicidad de riesgos posibles, en el análisis probabilístico se trabaja normalmente en función del valor esperado de los impactos o de impactos más probables, mientras que el análisis determinístico se enfoca generalmente en el "peor escenario".

El análisis de riesgo probabilístico normalmente presta poca atención aquellos eventos de muy baja probabilidad pero de alto impacto final[2]. Cuando se aplica este enfoque a eventos catastróficos (aquellos con potencial de causar un daño "mayor"), existe la posibilidad de dejar fuera del análisis aspectos importantes[3].

Formalmente, los riesgos no son valores "primarios", sino que se derivan de dos condiciones que interactúan: las **amenazas**[4] a la cual un objeto está expuesto y la **vulnerabilidad** del objeto expuesto.

Una ***amenaza*** (o ***peligro***[5]), fue definido en la *International Strategy for Disaster Reduction* de las Naciones Unidades como un evento físico potencialmente catastrófico, de origen natural o antrópico. En términos más específicos, es un fenómeno cuya dinámica puede desbordar los umbrales más frecuentes de intensidad o magnitud, afectando a algún elemento natural o construido (Mardones y Vidal, 2001); la intensidad y magnitud, por lo tanto, son las características que hacen más (o menos) peligroso a un fenómeno (Ayala-Carcedo, 2001). Para efectos del análisis de riesgo, lo relevante no es la existencia de una amenaza, sino que algún elemento esté ***expuesto a la amenaza***. Es decir, lo relevante es que una infraestructura determinada pueda ser afectada por una amenaza al encontrarse en el área de influencia de ésta[6].

---

[2] Llamados a veces, *black swans*, por una expresión inglesa antigua que se refería a algo imposible…hasta que un explorador holandés encontró cisnes negros en Australia en 1697.

[3] El análisis de riesgo tradicionalmente era probabilístico no tomaba en cuenta aquellos eventos que se consideraba muy poco probables, dado que el "valor esperado" del impacto (la probabilidad de que el evento ocurriera multiplicada por el impacto potencial daba un número muy bajo) resultaba insignificante. Sin embargo, experiencias de los últimos años en distintos sectores (financiero, aeronáutico y climático, por ejemplo) han llevado a que actualmente se suela incorporar todos los impactos relevantes al análisis, pues aunque la probabilidad sea baja, ellos se manifiestan en algún momento y, cuando lo hacen, pueden ser devastadores..

[4] En este trabajo la amenaza se referirá normalmente a una amenaza natural (no antrópica, como el terrorismo ni operacional, como las fallas) que se diferencian de las otras al depender de fenómenos que el ser humano no puede evitar.

[5] Algunos autores diferencian ambos conceptos, pero, en general, peligro y amenaza pueden ser utilizados como sinónimos.

[6] Por ejemplo, la infraestructura localizada en la zona cordillerana no está expuesta (exceptuando un "cataclismo") a la amenaza de *maremoto* y por lo tanto no hay riesgo producto de maremotos para dicha infraestructura.

Las amenazas (naturales) son de diversos tipos. Se propone la clasificación siguiente[7]:

1. Sismo
2. Maremoto
3. Erupción volcánica
4. Remoción en masa
5. Fenómenos climáticos extremos, que incluyen

   — Crecidas y crecidas repentinas (inundaciones)
   — Avalanchas
   — Tormentas de polvo o de arena
   — Temperaturas extremas
   — Sequías
   — Rayos
   — Vientos fuertes/Huracanes
   — Marejada
   — Tornados

La ***vulnerabilidad*** se entiende, en general, "como un factor de riesgo interno que está expresado como la factibilidad que el sujeto o sistema expuesto sea afectado por el fenómeno que caracteriza al peligro" (Cardona, 2001:11); por lo tanto, la vulnerabilidad corresponde a la predisposición intrínseca de un objeto a ser afectado (sufrir impacto) en caso que se manifieste un fenómeno "peligroso" de origen natural o antrópico[8]. A la vez, la vulnerabilidad está determinada (en proporción inversa) por dos variables:

- la **preparación** para emergencias: la capacidad de reaccionar frente a la materialización de una amenaza;
- la **protección** frente a emergencias: referida a los elementos de diseño y materialidad incorporados en la infraestructura de modo de resistir a un evento catastrófico.

En consecuencia, **los riesgos** se entienden como los resultados potenciales de la interacción entre amenaza y vulnerabilidad de una infraestructura expuesta[9].

---

[7] Esta nomenclatura ha sido elaborada a partir del estudio del 2012, "Identificación de la Infraestructura Energética Nacional y sus Características para Enfrentar Eventos Catastróficos y Análisis de la Infraestructura de la Zona Norte", elaborado por EMG Consultores para el Ministerio de Energía.

[8] Cardona (2001) complementa seálando que no se puede ser vulnerable si no se está amenazado o no existe una condición de amenaza para un elemento, sujeto o sistema si no está expuesto y es vulnerable a la acción potencial que representa dicha amenaza. En otras palabras, no existe amenaza o vulnerabilidad en forma independiente, pues son situaciones mutuamente condicionantes.

[9] Formalmente, se puede expresar de la siguiente manera: *Riesgo = Amenaza x Vulnerabilidad.*

En cuanto a la ***resiliencia,*** se la ha definido de diversas maneras: como un conjunto de dimensiones relacionadas - menores probabilidades de falla, menores impactos severos si hay falla y más rápida recuperación (Bruneau et al., 2003); como la habilidad de reducir la magnitud o duración de eventos disruptivos (National Infrastructure Advisory Council, 2009); como la capacidad de anticipar, absorber, adaptarse y recuperarse rápidamente de un evento disruptivo.

Para este trabajo se considera que lo esencial de la resiliencia, es la capacidad de adaptación y recuperación posterior a la emergencia (el momento de manifestación de la amenaza) que permite volver a las condiciones "normales" una vez terminado el evento. La resiliencia se distingue entonces de los aspectos de protección y preparación para emergencias en la dimensión temporal, si bien, como el momento final de la emergencia no es claro, la distinción es compleja y existe algún grado de superposición conceptual.

En los últimos años, el análisis de seguridad ha incluido de manera más explícita el aspecto "social" asociado a una amenaza, con lo cual la distinción formal presentada entre los diferentes elementos de la seguridad se complica ya que la vulnerabilidad y resiliencia se refieren a temas sociales no "técnicos"[10]. Desde esta perspectiva, el ***impacto*** es el efecto sobre la seguridad económica, social y política de la población. Por ejemplo, las implicancias que tendría el hecho de no contar con dicha infraestructura por un período determinado, tanto para la comunidad usuaria de dicha energía, como para el sistema productivo asociado a ella. A partir de una definición de impacto y de lo que se considera aceptable socialmente, generalmente es posible establecer un nivel de ***riesgo aceptable*** y si la resiliencia es o no adecuada.

Si bien, en un nivel profundo, lo relevante de la seguridad de suministro eléctrico, es la capacidad de satisfacer la demanda por electricidad de acuerdo con ciertos criterios de aceptabilidad social, eso requiere definir el impacto final relevante (sobre las personas, la economía, etc), y "valorizar" de algún modo, la importancia de cierta falla. En el presente trabajo, el análisis se refiere estrictamente a *seguridad del suministro* eléctrico (no, seguridad de la sociedad en relación con suministro eléctrico). Es decir, la variable objetivo relevante no será el impacto social o su aceptabilidad, sino que el alcance y la duración de la interrupción del suministro.

Una última distinción conceptual relacionada en el análisis de seguridad se refiere al "nivel" desde el cuál se realiza el análisis. El primer nivel puede denominarse "estadístico", el cual identifica los niveles globales de riesgo o seguridad asociado a ciertas zonas, tipos de infraestructura o eventos (esencialmente, indicadores relativos de riesgo o de nivel de riesgo), y que es útil principalmente para políticas. El segundo nivel se puede denominar "casuístico", y en él se evalúa zonas o infraestructura específica o eventos específicos (definidos en función de magnitud, duración o impacto) y está orientado a estrategias y planes de acción sectoriales o zonales.

Para efectos de este trabajo, el énfasis estará en el segundo nivel. Cabe mencionar además que en el análisis se considerará la relación de la institucionalidad pública con la vulnerabilidad y

[10] Cuando la vulnerabilidad se visualiza al nivel social y no de los componentes físicos afectados, la resiliencia se integra a veces dentro del análisis de vulnerabilidad, en particular. En este trabajo, sin embargo, la vulnerabilidad se sitúa dentro de un análisis clásico, es decir se refiere a vulnerabilidad de la infraestructura (enfocado en causas y consecuencias inmediatas) y no a vulnerabilidad de la sociedad. La vulnerabilidad social se relaciona con las consecuencias finales para un entorno social y en la capacidad de reducir dichas consecuencias. (Lövkvist-Andersen, *et al.*, 2004) En general, un análisis de vulnerabilidad sirve para "establecer categorías de activos y gestionar los procesos de gestión de riesgo" (United States Department of Energy, 2002).

resiliencia de la infraestructura, pero sólo para las aplicaciones específicas, pues la dimensión de los temas institucionales excede por mucho los alcances de este trabajo.

De acuerdo con el marco recién presentado, el trabajo se organizará distinguiendo los siguientes componentes del análisis de seguridad de suministro (todos enfocados a la infraestructura):

- Amenazas
- Vulnerabilidad
- Resiliencia

Si bien la distinción no siempre es perfecta, se buscará mantener esta estructura para permitir una mayor claridad del análisis y para facilitar conclusiones que sean útiles. En particular, en el ámbito de la resiliencia, se incluye a menudo elementos de análisis de riesgos en general (es decir, habiendo ya integrado amenazas y vulnerabilidad). Por otra parte, en el análisis de vulnerabilidad se distingue, cuando es posible, entre preparación y protección frente a emergencias. El objetivo final de todo análisis de seguridad es identificar mecanismos y medidas posibles para mejorar la seguridad, por lo cual todo el análisis debe tener esa orientación práctica.

El enfoque general es el que se ha denominado "casuístico", pero se señalará cuando cierto tipo de información o metodología sea más bien de orden estadístico.

3. Estado actual en Chile del análisis de seguridad de suministro eléctrico ante catástrofes naturales

El análisis de seguridad de suministro eléctrico ante catástrofes naturales en Chile es relativamente débil, producto de debilidades que existen en todos los niveles relevantes de análisis. Es de ir, no se puede indicar que una etapa del análisis sea crítica en la debilidad del análisis global. Los esfuerzos han estado desintegrados y no se ha buscado un trabajo de consenso con los agentes participantes e interesados en el sector.

3.1 Amenazas

En Chile existe información sobre exposición a amenazas con variados grados de desarrollo y calidad, aunque en general no es de alta calidad, en particular en la zona norte. Eso implica que las áreas de exposición y el grado de la amenaza tienen un alto grado de incertidumbre. Adicionalmente, salvo por una publicación reciente de la Subsecretaría de Desarrollo Regional (2011) no existen metodologías homogéneas para análisis de amenazas.

En el caso de la zona norte, la única información específica que está disponible y procesada se refiere a erupciones volcánicas y para maremotos en ciertas áreas; aún en esos casos, los datos son a menudo estimaciones. De las amenazas naturales, la volcánica parece ser la que se conoce con mayor precisión, aunque en ciertas zonas específicas. De igual modo, hay algún conocimiento específico sobre sismos y maremotos en algunas zonas del país, pero bastante limitadas. La mayor parte de la información de la que se dispone para sismos y maremotos se elaboró para desarrollar criterios de resguardo (normas para no ser afectado por la amenaza), y

no para definir exposición a amenazas por lo que la extrapolación desde la información a análisis de exposición debe ser tomada con cautela.

En el caso de sismos, para poder hacer un análisis de exposición a amenaza, se requiere un cierto nivel de detalle (microzonificaciones). Estos existen en algunos casos, elaborados por el Servicio Nacional de Geología y Minería para el área urbana de la ciudad de Concepción, San Antonio-Llolleo y para el Área Metropolitana de Santiago, por ejemplo. No existen en absoluto para la zona norte. Lo que se suele usar como criterio de exposición son las zonas sísmicas determinadas en la norma de construcción, pero como se ha indicado, esa extrapolación pude no tener sentido en varios casos.

En cuanto a información de maremoto, hay cartas generales (definen una línea única para la amenaza), que no consideran particularidades topográficas de las zonas en función de un evento dado para localidades como Arica, Antofagasta, Iquique, Mejillones, Taltal, Tocopilla e Isla de Pascua. Se ha desarrollado estudios recientes en la zona de Bío Bío[11]. Sin embargo, la información sólo considera el caso mayor de impacto por maremotos generados por terremoto local (no maremotos locales ni por eventos distantes). Para aquellos lugares donde no existen estudios específicos, en Chile se considera como referencia la cota 30 msnm (que corresponde a estándares internacionales).

En cuanto a erupciones volcánicas, existen coberturas establecidas por estudios de SERNAGEOMIN (Amigo, A., *et al.*, 2011) que distinguen entre amenaza por piroclastos y amenaza de lava y lahares (estos dos últimos como una sola categoría). En este caso, cada una de las categorías establece niveles de amenaza para ciertas zonas: alto y bajo en el caso de lava y lahares, y alto, moderado y bajo por caída de piroclastos. Las áreas definidas corresponden, principalmente, a sectores afectados al menos una vez en los últimos 14.000 años; es decir, presenta solo áreas que han sido afectadas en el pasado, no se trata de escenarios modelados.

Asociado a terremotos, existe alguna información de remoción en masa. Esta información se puede derivar de la información topográfica existente. Respecto a fenómenos climáticos extremos la información en general es menos sistemática (y se encuentra menos sistematizada), aunque existe información disponible en lugares donde estas consideraciones son más significativas (puertos, aeropuertos).

El trabajo más avanzado en formalización de la exposición a amenazas es el que ha realizado el Instituto Geográfico Militar (administrado por la Oficina Nacional de Emergencia) en el Sistema Integrado de Información para Emergencias (SIIE). Se incluye en dicho sistema información fuentes como el SERNAGEOMIN, el departamento de sismología de la Universidad de Chile y estudios encargados por la SUBDERE, entre otros. Se trata de un sistema en desarrollo (actualmente entre las regiones III y XV. El sistema se presenta en un plano con proyección UTM, coordenadas geográficas y opera con sistema de georreferenciación de datos SIRGAS (WGS84).

El SIIE recoge información de infraestructura pública, de maremotos en algunas localidades, de actividad volcánica, información hidrometeorológica (secuencia de días con probabilidad de inundaciones) y recurrencia sísmica. Sin embargo, la información aún no es completa por lo que requiere más desarrollo.

[11] Ejemplo de un estudio desarrollado es "Estudio de Riesgos de Sismos y Maremoto para Comunas Costeras de la Región del Biobío" desarrollado por el Laboratorio de Estudios Urbanos, U del Bío Bío (2011)

En conclusión, la información disponible es de carácter general y permite tan sólo aproximaciones a "zonas" con características generales de riesgo, sin un grado de detalle suficiente para un conocimiento de la exposición a las diversas amenazas. La iniciativa SIIE puede ser un gran aporte, pero requiere un proceso de estandarización de metodologías y de definición de información a solicitar para que pueda ser una herramienta realmente poderosa.

3.2 Vulnerabilidad

La vulnerabilidad de la infraestructura eléctrica ha sido estudiada recientemente por dos trabajos, uno del Ministerio de energía y otro de la SEC.

El trabajo de la SEC consistió en el envío del Oficio Circular 10.013 (OC 10013) que es parte del "Plan de evaluación de la integridad de instalaciones eléctricas y de combustibles" posterior al movimiento telúrico del 27 de febrero de 2010. El Oficio solicitó a las empresas evaluar aquellas instalaciones que hubieran sufrido desperfectos por el sismo, proponiendo un plan de normalización para asegurar el suministro del servicio y medios para mitigar daños ante la ocurrencia de un evento similar. La información se solicitó en cuatro etapas:

1. Evaluación de integridad. Detectar fallas, deterioros o potenciales riesgos mediante inspecciones específicas.
2. Plan de normalización. Para aspectos que deben ser regularizados para el suministro de servicio (trabajos a realizar para dicho fin).
3. Análisis de riesgo. Dar cuenta del estado de las instalaciones en aspectos claves como: comportamiento debido al sismo, antigüedad, materiales, número de servicios existentes en la zona, densidad poblacional con el objeto de prevenir y mitigar futuras situaciones similares (es decir, aplicado esencialmente a sismo).
4. Plan de prevención y/o mitigación. Explicar aspectos que deben ser abordados, de acuerdo a lo detectado en las etapas anteriores, según criterio de empresa.

El OC1003, fue el primer proceso sistemático por conocer sobre el riesgo en las instalaciones energéticas, con una sección 3) que se refiere (aproximadamente) al aspecto de vulnerabilidad ya mencionado, si bien no con esta nomenclatura precisa. Aún cuando, el análisis estuvo limitado al referirse específicamente a sismos (y por su naturaleza no consideró los aspectos sistémicos de la infraestructura, sino que se enfocó en la "instalación") la cantidad de información recogida fue sustantiva. La contrapartida de esto es que el proceso de recepción y revisión de la información tardó cerca de dos años y el nivel de respuestas fue variable según las empresas, además de desarrollarse con diversas metodologías, lo que hace difícil su comparación. No obstante, se recogió abundante información que podría ser útil para ejercicios posteriores.

El estudio encargado por el Ministerio de Energía "Identificación de la Infraestructura Energética Nacional y sus Características para Enfrentar Eventos Catastróficos y Análisis de la Infraestructura de la Zona Norte", del año 2012, tuvo por propósito "identificar y levantar la información de infraestructura energética nacional[12], y analizar las características y exigencias de diseño de construcción de la infraestructura crítica del sector energético de la zona norte, así como, las medidas de resguardo utilizadas en dichas instalaciones, a fin de evaluar las condiciones en que se encuentran para el caso en que ocurra un evento catastrófico, e identificar los aspectos a mejorar para fortalecer la seguridad del suministro".

[12] Tanto eléctrica como de combustibles líquido y gaseosos.

Uno de los elementos centrales del trabajo fue desarrollar un análisis de vulnerabilidad para toda la infraestructura energética, por medio de encuestas a las empresas (método estadístico). Para esto, se estableció una tipología de infraestructura que buscó relevar aquellos elementos que tuvieran un papel significativo en la continuidad del servicio (no todos los elementos de la infroaestructura). Luego se diseñó y aplicó un instrumento de recolección de información que consultaba tanto sobre ***preparación*** ante amenazas como sobre ***protección*** (con distinto nivel de agregación) además de antecedentes generales y una referenciación geográfica (para poder cruzar la información con la exposición a amenazas y así realizar un análisis de riesgo).

Los conceptos desarrollados para que la recopilación de información fuera válida se basaron en una clasificación de la infraestructura en "tipos", que pudieran ser manejados estadísticamente. Estos tipos se derivaron de los segmentos de la infraestructura energética que se consideró en la solicitud de base (electricidad o hidrocarburos). Se desarrolló un índice de vulnerabilidad basado en un análisis multicriterio.

Sin embargo, el ejercicio mostró que es difícil establecer una definición precisa de los elementos de la infraestructura que determinan la vulnerabilidad en todos los casos y que sea comparable entre infraestructura y en el nivel sistémico. Como no existen patrones absolutos de referencia se debe definir un nivel de exigencias específico, lo cual requiere desarrollar normas y regulaciones específicas, o bien adoptar algunas internacionales que parezcan pertinentes para Chile. En consecuencia, la construcción de indicadores de vulnerabilidad, exige definir estándares claros de comparación así como métodos de medición, junto con desarrollar procedimientos para que la evaluación signifique incentivar mejoras continuas en la infraestructura.

3.3 Resiliencia

No existe información desarrollada sistemáticamente sobre la capacidad de recuperación de los sistemas eléctricos frente a catástrofes naturales. Como se indicó previamente, algo de esto se encontró en la solicitud del OC 10013, pero aplicado a un caso muy específico y con una metodología no definida claramente.

Los planes de recuperación de servicio que son desarrollados por los Centros de Despacho de Carga, si bien están vinculados con la resiliencia del sistema, no incorporan un análisis de los elementos que definen la capacidad de recuperación de estos sistemas. Esos planes consisten en un ordenamiento de acciones para recuperar el servicio en los diversos sectores de los sistemas eléctricos, pero no incluyen análisis temporal de las acciones o de las dificultades operacionales que pudieran existir o de procesos adicionales o en otros sectores que fuera necesario incorporar.

Por lo tanto, no se dispone en Chile de análisis de resiliencia de sistemas eléctricos como un todo, si bien puede haber antecedentes específicos frente a ciertos eventos específicos (como es el caso del OC 10013).

4. Metodologías y buenas prácticas internacionales sobre análisis de seguridad aplicables al suministro eléctrico[13]

[13] Esta sección se apoya de manera significativa en el trabajo de Giannopolous et al (2012) en lo relativo a vulnerabilidad y resiliencia.

La revisión de casos internacionales muestra que si bien los tres componentes básicos del análisis de seguridad están presentes en muchos tipos de análisis, no siempre se distingue con claridad los elementos y a menudo estos se integran en un "agregado" de análisis de riesgo. Por ello, en esta sección a veces se combinan algunos elementos y se establece ciertas distinciones sólo para fines analíticos.

4.1 Amenazas

Las amenazas naturales tienen en general definiciones conceptuales establecidas, criterios y categorías aplicables para poder definir el grado de exposición de una infraestructura a cada una de ellas. Por lo tanto, conceptualmente se dispone de todas las herramientas necesarias para definir adecuadamente exposición a amenazas con un grado de precisión importante.

La forma más utilizada es la de generar mapas de amenazas, pues eso permite cruzar las amenazas con infraestructura y poblaciones específicas. Para cada tipo de amenazas, existen ciertas buenas prácticas que han sido desarrolladas y que han sido aplicados a casos concretos. Estos mapas son, generalmente, de tipo probabilístico, pues establecen tipos de eventos con ciertos grados de recurrencia. Sin embargo, la aplicación de estas metodologías es compleja pues requiere la participación de especialistas con conocimiento profundo de los temas y situaciones para modelar formalmente las amenazas a partir de la información disponible y, por lo tanto, también se requiere un conjunto importante de información detallada.

En el caso de maremotos, por ejemplo, se necesita información detallada del nivel del mar de la topografía y de la batimetría de la zona. O en el caso de los sismos, se requiere, entre otros, un conocimiento geológico, geotectónico, topográfico además de datos de dinámica de suelos. A partir de los datos de base se genera modelos determinísticos o probabilísticos. Para hacer esto, las capacidades computacionales crecientes de los últimos años han permitido desarrollar modelos más completos y complejos.

En general, los países de la OCDE han desarrollado mapas de riesgo globales (para todo su territorio) y otros de mayor detalle para zonas específicas (de mayor interés por algunos temas). La Unión Europea tiene planos globales de amenazas para aluviones, maremotos, terremotos y fenómenos climáticos extremos, así como otros eventos secundarios como incendios[14]. Además de esto, los países individuales y las regiones tienen mapas específicos. Estado Unidos tiene mapas para las principales amenazas naturales globales, desarrollados por agencias federales[15] y mapas de mayor detalle para ciertos estados, como en los casos de Oregon y Washington para maremotos. Japón también posee detallados mapas de riesgo, con énfasis en temas como terremotos y maremotos por razones obvias.

Debe destacarse que, pese a la importancia de los mapas de riesgo, estos no son herramientas perfectas, y existen caso de eventos devastadores ocurridos en áreas definidas por los mapas como de bajo riesgo (terremotos de Tohoku, 2011, de Wenchuan 2008 y Haiti 2010, por ejemplo), mapas (maremoto de Japón 2011).

[14] Los mapas globales se encuentran disponibles en el sitio web de la *European Spatial Planning Observation Network (ESPON)*

[15] Se pueden encontrar mapas en los sitios de del US Geological Service o la Federal Emergency Management Agency (FEMA).

Debe recordarse que los mapas de riesgo se basan en información histórica, información de condiciones actuales y modelos matemáticos de proyección. Generalmente las bases de datos son relativamente limitadas, los parámetros seleccionados dependen de evaluaciones expertas y conocimiento teórico actual y, a menudo, no se cuenta siquiera con toda la información necesaria. De todos modos, la complejidad de los fenómenos naturales hace suponer que nunca será posible disponer de mapas completamente precisos, por lo que siempre las conclusiones del análisis deben ser cuidadosas.

4.2 Vulnerabilidad

Existen varios métodos relativamente estandarizados para analizar vulnerabilidad en el nivel de instalaciones específicas, o eventualmente, zonas industriales. Existen también normas ISO que orientan todo el proceso de análisis de riesgo, incluyendo el análisis de vulnerabilidad (ISO 31000). En contraste, pese a existir algunas orientaciones generales, no se ha desarrollado un marco común metodológico en el análisis "sistémico", posiblemente por la complejidad del ejercicio formal, la diversidad de situaciones, y por el hecho de que los objetivos buscados por el análisis pueden ser muy diversos.

El análisis de vulnerabilidad generalmente sigue tres simples etapas, que pueden asociarse al análisis preliminar de riesgos clásico para las instalaciones:

- Catastro de recursos (activos y capacidades) de un sistema
- Valorización u ordenamiento de importancia de los recursos
- Identificar las vulnerabilidades de cada recurso

De ese modo, el objetivo general es reducir las mayores vulnerabilidades de los recursos más importantes. El análisis de vulnerabilidad se diferencia entonces del análisis clásico de riesgo por cuanto este último se enfoca en el riesgo de una instalación (diseño y operación), mientras que el primero mira las interrelaciones y los elementos que determinan la vulnerabilidad (Lövkvist-Andersen, *et al.*, 2004) (los componentes de preparación y protección).

No todas las metodologías de análisis de riesgo de infraestructura (sistémicos) consideran la vulnerabilidad como un elemento "separado". En general, las que lo hacen se derivan de análisis de riesgo de instalaciones, tales como el Análisis Probabilísticos de Seguridad (PSA, por sus siglas en inglés) y los Análisis Cuantitativos de Riesgo (QRA, en inglés) los cuales han sido aplicados a nivel de plantas (en muchos sectores industriales, sobre todo nucleares en el sector eléctrico)[16]. Estos métodos incluyen cosas como modelos probabilísticos detallados, con árboles de eventos y modelos físicos del evento que difícilmente se pueden replicar con detalle a nivel sistémico.

En el nivel sistémico los análisis de vulnerabilidad por sí mismo no son comunes, sino que se incluyen dentro de un análisis de riesgo global que incorpora a menudo algún grado de consideración de la resiliencia. Se observa que cuando se trabaja en una escala relativamente grande (como es el caso de los análisis sistémicos) no es simple distinguir los elementos de la vulnerabilidad. Por ello, los ejemplos de buenas prácticas se agrupan en la siguiente sección.

[16] En términos muy simples, un PSA se enfoca en describir y analizar las probabilidades de eventos catastróficos siguiendo una secuencia de eventos posibles y los elementos que determinan estas, mientras que una QRA se enfoca más en cuantificar los efectos de distintos tipos de eventos para determinar su importancia, aunque a menudo considera también la probabilidad de los eventos.

Para este componente del análisis de riesgo, se puede trabajar con modelos computacionales de simulación o simplemente con métodos analíticos, pero siempre se requiere una base cuantitativa.

4.3 Riesgo y Resiliencia

Como se señaló, la experiencia internacional muestra que lo más común es un análisis de riesgo "integrado" es que los componentes de la resilencia están relativamente imbricados, por lo que no se les puede separar fácilmente. Esto se puede interpretar en función del objetivo de un análisis de riesgo: normalmente, las acciones en el nivel de las empresas deben ser realizadas por las propias empresas, por lo que lo esencial es identificar los ámbitos de vulnerabilidad, mientras que las vulnerabilidades específicas son materia de la cual deben ocuparse las empresas específicas. Desde el punto de vista de la evaluación, lo esencial es identificar las consecuencias (incluyendo impacto social) y los responsables, más que detallar su orígenes. Mientras mayor es la escala, entonces más integrado resulta el análisis pues, no se puede trabajar específicamente en aquellos elementos que hacen vulnerables a las instalaciones sino en ámbitos que se puede mejorar. "Indirectamente", se puede evaluar formas de reducir vulnerabilidad, pues lo que se busca es identificar ámbitos donde se requiere mayor atención.

En el análisis sistémico, las interdependencias entre infraestructura y entre sistemas es clave. Se ha definido cuatro tipos fundamentales de interdependencia (Giannopoulos et al., 2012):

- Física: en la cual la operación de una infraestructura depende materialmente de otra
- Informática: en la cual la operación de una infraestructura depende de información proveniente de otra
- Geográfica: porque eventos afectan simultáneamente a infraestructuras
- Lógica: otras

En términos de análisis globales, los Estados Unidos, por ejemplo, realiza análisis de riesgo estratégicos, con un alto nivel de agregación (nacional) y que buscan identificar los impactos mayores para efectos de enfocar temas que requieren mayor atención. Los análisis estadísticos de riesgo son algo más elaborados, pero no distinguen mayormente los componentes de amenazas y vulnerabilidad, sino que simplemente consideran el conjunto de resultados "indeseados" posibles, a partir de información real de eventos de diversas causas. Ese análisis estadístico, se basa en la materialización real de los eventos (apagones por tormentas, por ejemplo). Los ejercicios estadísticos miden generalmente impacto y severidad para analizar probabilidades de impactos.

Para el análisis de riesgo sistémico, Giannopoulos et al (2012) han propuesto una división en tres categorías: análisis clásico, estructural y comportamental. El primero se enfoca en aplicar métodos tradicionales a sistemas, el segundo considera explícitamente las interdependencias dentro de los sistemas y el tercero considera las implicancias de comportamiento en los resultados (efectos de agentes).

Existen múltiples ejemplos de análisis de riesgo en los países desarrollados[17], todos con aportes interesantes. Se ha seleccionado tres que pueden ser particularmente útiles para entender la propuesta final.

[17] Por ejemplo, Giannopoulos et al (2012) describen 21 casos.

El *Concepto de Protección Basal* (Alemania), del Ministerio del Interior la Oficina de Protección Civil y Desastres y la Policía Federal. Si bien no es una evaluación de riesgo, sino un plan, incluye un elemento de evaluación al presentar el conjunto de amenazas consideradas relevantes y al remarcar las interdependencias en la infraestructura e informar a las empresas sobre éstas para que puedan estar alerta y tomar acciones frente a estos temas en su ámbito de responsabilidad. La metodología se dirige esencialmente a los operadores de infraestructura crítica.

El enfoque *DECRIS* (Noruega), desarrollado por el Instituto SINTEF considera cuatro etapas básicas

- Establecer taxonomía de eventos y dimensiones de riesgos
- Evaluación de vulnerabilidad y riesgo simplificado para los eventos
- Selección de eventos para análisis en profundidad
- Análisis en profundidad de eventos seleccionados.

Se basa en el análisis clásico de riesgo, pero con un proceso de selección que permite enfocar el trabajo de acuerdo con la probabilidad de riesgo, importancia de la infraestructura y aspectos comunicacionales. No considera la resiliencia específicamente, pero podría hacerlo. Esta metodología se orienta tanto a tomadores de decisión en empresas como a *policy-makers* y tiende a fomentar la cooperación entre los actores sectoriales para el análisis de interdependencias. Se aplicó el concepto en Oslo para electricidad, agua, transporte y TIC.

El enfoque *RAMCAP plus* (Estados Unidos), desarrollado por la Sociedad Americana de Ingenieros Mecánicos, es una metodología para todo tipo de amenazas aplicable a todo tipo de infraestructura. Considera siete etapas; a saber:

- Caracterización de activos
- Caracterización de amenazas
- Análisis de consecuencias
- Análisis de vulnerabilidad
- Evaluación de amenazas
- Evaluación de riesgo y resiliencia
- Gestión de riesgos y resiliencia

La metodología se enfoca en los activos más críticos de cada instalación basándose en técnicas existentes pero adaptadas al nivel sistémico del análisis. La metodología trata en detalle la vulnerabilidad y la resiliencia y se dirige a los operadores y tomadores de decisión.

5. Brechas nacionales en el análisis de seguridad de suministro eléctrico ante catástrofes naturales

Las brechas se establecen en relación con las prácticas comunes y lo que se puede considerar como buenas prácticas identificadas en el mundo. Se genera una identificación estructurada de las brechas para un análisis de seguridad de suministro, que colabore en establecer una posible estrategia para enfrentarlas.

5.1 Amenazas

En términos generales la disponibilidad de mapas de riesgo para todas las amenazas significativas es una buena práctica internacional reconocida. Si bien se conoce casos en los que los mapas han entregado información equivocada o confusa, se reconoce que son elementos mínimos de los cuales se debe disponer para un análisis de seguridad, en particular en las zonas donde existe población importante e infraestructura crítica.

Para distintos tipos de amenazas, hay ejemplos de buenas prácticas en el nivel de las metodologías específicas. Estas metodologías no se refieren sólo a las técnicas de recolección de información física relevante sino también al proceso por el cual se recoge esta información, a la discusión sobre los modelos usados, al alcance y limitaciones de los ejercicios. Un ejemplo interesante es la actualización de mapas sísmicos para el 2014 que está llevando adelante la USGS, con un trabajo amplio de consulta a expertos desde el 2012.

En Chile, la brecha es muy significativa por cuanto no sólo no existen mapas para todos los tipos de amenazas naturales posibles, sin que además estos mapas a menudo carecen del nivel de detalle requerido para generar medidas apropiadas en ciertos sectores críticos (un nivel territorial específico)[18]. Además, a menudo se basan en información general y no en antecedentes específicos y carecen de metodologías estándar transparentes y ampliamente validadas para las modelaciones.

En consecuencia, si bien existe información para un análisis de riesgo, en genera los resultados obtenidos de estos tendrían un importante grado de imprecisión. Los déficits de calidad en información sobre amenazas requieren un proceso sistemático y científicamente válido de obtención y procesamiento de información. Disponer de la información completa para identificar con un nivel mayor de precisión amenazas por área puede ser un proceso largo y costoso, no obstante es posible avanzar parcialmente recopilando información en estudios que pueden realizarse en plazos relativamente acotados y con presupuestos abordables.

Adicionalmente, se debe disponer de metodologías que utilicen la información de manera coherente y comparable. La información es parte del proceso, pero se requiere además decisiones de expertos para decidir su aplicabilidad (y la manera de hacerlo) la cual es altamente dependiente del caso.

5.2 Vulnerabilidad

En general, no existe una metodología o práctica específica, ni siquiera a nivel de instalaciones, que se pueda usar como referencia, ya que los elementos que determinan la vulnerabilidad son muy específicos a las operaciones [19] y a los problemas potenciales que se quiere analizar. No obstante, existen algunos enfoques metodológicos que son de amplia utilización en esta escala.

[18] Por ejemplo, puede haber zonas donde el efecto de los maremotos sea mucho mayor dadas las particularidades de topografía, lo que requiere estudios específicos (batimetría en particular). Asimismo, debe considerarse los impactos de eventos lejanos o no derivados de sismos y la relación del área específica de interés con el área de inundación máxima.

[19] El Departamento de Energía de los Estadios Unidos, por ejemplo indica respecto al tema de la vulnerabilidad en el sector, aunque refiriéndose a vulnerablidad de instalaciones individuales “The purpose of this report is to provide a methodology resource for the electric power industry. No one vulnerability assessment methodology has all the answers. Companies should consider for themselves

El problema es más evidente cuando se considera el nivel sistémico del análisis. De hecho, la experiencia internacional muestra que este es un nivel en el cual el problema se ha comenzado a tratar relativamente hace poco y con una gran dispersión de metodologías según los intereses de los que realizan los esfuerzos, pero también de la disponibilidad de información. Además, se debe considerar el hecho de que muchos análisis sistémicos no se enfocan en vulnerabilidad específicamente.

En el nivel sistémico, en Chile los esfuerzos han sido bastante limitados y acotados por la complejidad del problema y porque ciertos elementos clave que permiten darle dirección a un esfuerzo de este tipo (según ha mostrado la experiencia internacional) no han existido; a saber: objetivos (usos esperados), alcances del ejercicio y profundidad esperada. Estos criterios son básicos pues sin ellos, el problema se vuelve inmanejable, pues la complejidad se vuelve "indefinida".

Adicionalmente, se ha dado el problema que estos ejercicios requieren una gran cantidad de información y no se ha generado una instancia que promueva que las instalaciones compartan este tipo de información y lo pongan a disposición de un análisis que los beneficie "colectivamente", como tampoco existe capacidad del sector público para obtener esta información de manera completa y eficiente. En cualquier caso, para avanzar en obtener la información necesaria, es esencial previamente definir los puntos mencionados.

5.3 Riesgo y Resiliencia

No existen análisis de riesgo (y menos si se incluye la resiliencia dentro de sus consideraciones) con suficiente desarrollo en Chile como para establecer un punto de comparación relevante. Los esfuerzos que se han realizado son incipientes por lo que se requiere un desarrollo completo. Como se señalará más adelante, para llevar adelante un ejercicio de esa naturaleza falta definir un marco básico que no ha sido siquiera planteado en la discusión sobre el tema. Por lo tanto, la "brecha" implica definir qué se busca en primer lugar.

6. Conclusiones

La revisión de los antecedentes previos permite establecer algunas conclusiones clave sobre el estado del análisis en materia seguridad eléctrica ante catástrofes naturales en Chile. En particular, se destaca:

1. Existen falencias en todos los ámbitos relevantes para análisis de seguridad de suministro[20]. Se identifica una brecha clara con el tipo de acciones que se realiza en países que han incorporado la seguridad de suministro (física) como elemento clave del desarrollo energético.
   a. En términos de amenazas, hay pocas zonas del territorio nacional que dispongan de mapas completos de todas las amenazas, con criterios uniformes. Tampoco existe una definición completa de las amenazas. Existe una iniciativa importante en curso (el SIIE),

the applicability of the vulnerability assessment elements to their individual situation. Each company should determine which elements are applicable (if any) along with the appropriate level of detail" (U.S. Department of Energy, Office of Energy Assurance, 2012:4).

[20] Existen además importantes falencias institucionales, no estudiadas en este informe, que se reflejan en particular en la ausencia de un organismo público a cargo de la infraestructura crítica.

pero que aún requiere integrar más información y más completa. Para el sector eléctrico, eso implica que no se tiene un conocimiento precios de las amenazas a las cuales esta expuesta gran parte de su infraestructura.

b. La vulnerabilidad se ha estudiado recientemente tanto por la SEC como por el Ministerio de Energía. La solicitud de la SEC (OC 10013, 2010) estuvo referida a una situación específica y sin metodologías estándar y no constituye un análisis sistémico, si bien recoge mucha información útil para un análisis de ese tipo. El Ministerio de Energía realizó un estudio con metodología homogénea de vulnerabilidad para todo el sector energético del SING, pero en un nivel estadístico, con información (entregada por las empresas) que aún requiere mejoras significativas.

c. No hay información sistemática disponible sobre resiliencia del sector. La experiencia práctica en el caso del terremoto del 2010 mostró la capacidad de recuperación bastante rápida del sector eléctrico y la capacidad de reaccionar para entregar electricidad de manera progresiva, pero no ha sido estudiada de manera sistemática para diferentes condiciones y, en particular, para distintos tipos de eventos catastróficos. Algunos antecedentes importantes se encuentran disponibles también como resultado de las respuestas la OC10013 de la SEC, aunque son aplicables sólo a terremotos y la calidad de lo entregado por las empresas es variable. Por otra parte, los planes de recuperación son indicaciones de procesos no un análisis de capacidad o condicionantes de recuperación.

2. Existen experiencias internacionales útiles para el análisis de seguridad, metodologías y buenas prácticas relevantes y útiles para el caso chileno, pero no existe ***una*** fórmula establecida y única para esto. Por lo anterior, es necesario identificar los elementos pertinentes para el caso chileno y adaptar metodologías en función de los objetivos deseados. Un elemento clave está en identificar con cierta precisión los alcances y objetivos del ejercicio así como las interdependencias que serán consideradas y la profundidad (en particular hasta dónde se analizar resiliencia por ejemplo[21].

   a. En el caso de las amenazas, los mapas de amenazas[22] son un formato estándar en el cual existe amplia experiencia en todo el mundo desarrollado con diversos alcances y grados de detalle en función de la disponibilidad de información. Mientras más extensa y detallada la información se dispone de más mapas de amenazas y con mayor precisión geográfica. No obstante, se debe tener presente que los mapas a veces no reflejan adecuadamente lo que ocurre en la realidad.

   b. En el caso de la vulnerabilidad sistémica de la infraestructura, existe una variedad de metodologías que la consideran pero no existe modelos universales. Las opciones dependen del objetivo (incluyendo el tipo de usuarios). A diferencia de los análisis de vulnerabilidad de instalaciones, la vulnerabilidad sistémica ante tipos diversos de eventos catastróficos ha tenido múltiples tratamientos y cada país ha seleccionado metodologías en función de sus objetivos y aplicado métodos en función de disponibilidad de tiempo, recursos e información disponible.

      La mayor parte de los análisis de vulnerabilidad están insertos en análisis globales de riesgo/resiliencia. Existen experiencias como la de los proyectos DECRIS o RAMCAP en que la vulnerabilidad aparece como un tema identificable y que se insertan en el nivel de las necesidades de Chile.

   c. La resiliencia ha sido tratada de diversas maneras en la experiencia internacional. El marco conceptual y metodológico es más difuso que en el resto del análisis de seguridad,

[21] Consultar Giannopoulos et al (2012)
[22] No confundir con los mapas de riesgo.

por lo que está menos estructurado. Así, por ejemplo, se dispone de variados trabajos en adaptación ante eventos de largo plazo (cambio climático, por ejemplo), otros sobre reacción a eventos de corto plazo y a menudo la resiliencia se relaciona sobre todo con el nivel social del análisis. No siempre la resiliencia es parte del análisis de riesgo sistémico, pero no se encuentra análisis de resiliencia que sea independiente del análisis de riesgo. Los ejemplos de metodologías ya citados incluyen análisis de resiliencia.

En consecuencia, si bien la brecha para avanzar en un análisis de seguridad de suministro eléctrico ante eventos (catastróficos) naturales en relación con países desarrollados es muy grande e incluye tanto información básica como de metodologías, existen estrategias que son aplicables en Chile una vez que se defina con precisión el alcance que se le quiere dar al análisis. Es decir, si bien puede requerirse mucho tiempo y recursos para cerrar la brecha por completo, es posible reducirla significativamente con una estrategia adecuada.

La brecha de información en las amenazas es particularmente compleja, costosa y demorosa de cubrir[23]. No obstante, ello no debería ser un impedimento para avanzar en análisis de riesgo de la infraestructura crítica: por una parte, debe recordarse que los mapas de amenazas no son "infalibles" y por otra, el resto del análisis de riesgo no está condicionado por esta información.

Adicionalmente, la importancia de los análisis de seguridad según se reconoce en la experiencia internacional, sugiere la urgente necesidad de desarrollar una estrategia aplicable a Chile que permita contar con un análisis de seguridad de suministro eléctrico ante catástrofes naturales útil para avanzar en medidas que reduzcan el riesgo y mejoren la resiliencia. La magnitud de la brecha es tal que se hace imperativo avanzar en reducirla de la manera más efectiva y eficiente posible.

6.1 Aspectos generales de una estrategia de análisis de seguridad eléctrica

Se ha señalado que un paso fundamental es definir un marco para el análisis. Sin dicho marco, no es posible avanzar en un análisis de seguridad claro. Esto implica definir:

1. Objetivos
2. Alcance (bordes del sistema, interdependencias)
3. Profundidad (consideraciones sociales, detalle, consideraciones de resiliencia)

Es esencial notar que sólo habiendo definido un marco preciso, es posible implementar una estrategia específica y definir las metodologías específicas que serán necesarias. No obstante, se puede delinear una estrategia general para el análisis de seguridad que cumpla con el objetivo de analizar la seguridad eléctrica, sin que sea necesario especificar en esta etapa todos los detalles, los cuales deberían ajustarse al contexto o marco mencionado. La razón de esto es

[23] En el caso de las amenazas, se requiere un proceso sistemático de obtención de información, partiendo por aquellas zonas que según juicio experto podrían tener mayor nivel de exposición objetiva. Disponer de la información completa para identificar áreas con un nivel mayor de precisión puede ser un proceso largo y costoso, en el cual difícilmente se puede acortar. No obstante es posible avanzar parcialmente recopilando información en estudios que pueden realizarse en plazos relativamente acotados (en torno a un año) y con presupuestos, que aunque no son menores, son abordables dada la importancia del fenómeno. Es importante, señalar que la información es parte del proceso, pero se requiere además de decisiones de expertos para decidir su aplicabilidad, lo cual es altamente dependiente del caso.

que al caracterizar el suministro como el objetivo general, el marco, aun cuando no es completamente preciso, queda delimitado. Dos aspectos clave deben considerarse.

Por una aparte, se debe definir el nivel de participación de los diversos actores relacionados con infraestructura eléctrica y la forma de articulación de estos actores en un análisis de seguridad. Este tipo de trabajo difícilmente puede realizarse de manera independiente por el sector público en un contexto en que la mayor parte de la infraestructura crítica es privada. Por ello, se requiere un trabajo coordinado de empresas que participan en el sector, pero además el liderazgo de alguna institución que pueda coordinar un proceso que requiere homologación y definiciones adecuadas y además relacionarse con otros sectores para evaluar interdependencias.

En cualquier forma de aplicación sería necesario conformar grupos de trabajo con los actores de la industria, de manera de identificar los aspectos esenciales de la infraestructura, así como los componentes clave en temas de seguridad, estableciendo formas homogéneas de medir sus condiciones técnicas (mantenciones, probabilidades de falla, sistemas de control, etc.), y de ponderar su rol dentro de la vulnerabilidad. En estos grupos, se podrá definir cuánta información es útil y pertinente recopilar de manera centralizada y cuánta debe ser gestionada por las empresas. Igualmente, será posible definir cuan detallado puede ser el ejercicio.

Por otra parte, para aplicar la metodología se puede desarrollar modelos formales (computacionales) utilizar a expertos o combinar ambas opciones. En cualquier caso, gran parte del trabajo se puede realizar utilizando conocimiento experto, evitando a la complejidad computacional (y los mayores tiempos y costos) asociados a los modelos formales.

La estrategia general propuesta debe permitir identificar ámbitos de preparación, protección adaptación y recuperación que pueden ser mejorados y, de ese modo, someter las medidas potenciales a un análisis más detallado (costo- efectividad por ejemplo).

La estrategia básica es bastante directa, inspirada en algunas buenas prácticas para análisis sistémico revisadas, considerando la complejidad (en particular las interdependencias entre componentes), las carencias de información y la comparabilidad (necesidad de usar enfoques coherentes para todos los casos).

6.2 Etapas de una Estrategia de Análisis de Seguridad Eléctrica

Se sugiere mantener la estructura de la revisión presentada para permitir diferentes niveles de análisis, separando los temas de vulnerabilidad de los de resiliencia pues pueden tener responsabilidades distintas. Si bien la separación no es explícita en todas las buenas prácticas revisadas, hacer la distinción permite separar de manera más clara ciertas responsabilidades y por lo tanto puede ser un análisis más práctico para el objetivo final de implementar mejoras a la seguridad.

En resumen, la estrategia metodológica propuesta, distingue tres etapas que se detallan a continuación:

1. Definición de amenazas relevantes
2. Análisis de vulnerabilidad
3. Análisis de resiliencia

6.2.1 Definición de amenazas relevantes

- *Identificar amenazas relevantes*

Dada la gran cantidad de amenazas, se debe identificar un conjunto de eventos que se considere como más significativos para el objetivo del trabajo. Esto no es una visión "objetiva", sino una apreciación a partir de la visión de los expertos y de las partes interesadas en el proceso, además de la información disponible. En ese sentido, si bien los mapas de amenaza son un aporte para entregar unos criterios más objetivos para esta identificación, siempre se requiere la opinión de expertos para ajustar la identificación de amenazas al problema central.

Los eventos se deben definir para la tipología de amenazas descritas y considerando opciones de magnitud y duración (es decir, se debe considerar la escala del evento: "peor" escenario, escenario más probable…etc). Los eventos críticos seleccionados pueden también ser una combinación de amenazas manifiestas (típicamente, terremoto con maremoto). Se debe buscar mantener un número relativamente acotado de amenazas relevantes para que el ejercicio posterior sea factible [24].

- *Caracterizar amenazas relevantes*

La caracterización de los eventos (impactos) seleccionados debe ser precisa en cuanto a magnitud, características particulares relevantes y alcance espacial[25]. El grado de exposición debe ser lo más preciso posible, lo cual idealmente se apoya en modelos formales; en ausencia de estos puede ser conceptual basado en juicio experto (alto, bajo, medio, por ejemplo).

6.2.2 Análisis de Vulnerabilidad

Uno de las decisiones centrales del marco que debe incorporarse específicamente en esta etapa del análisis se refiere al alcance y al nivel de detalle que se va a buscar. La decisión final está relacionada de manera sustancial con el tiempo y con los recursos disponibles, pero además con los objetivos de seguridad buscados y el usuario final de la seguridad. Mientras mayor el detalle de elementos considerados y más el nivel de análisis, aumenta la capacidad del ejercicio para apoyar la mejora de seguridad, pero es mayor el tiempo y los recursos requeridos. No existe un estándar para definir niveles de importancia de infraestructura, por lo que se deberá ajustar en función de la opinión experta de las partes interesadas. Es posible definir ámbitos en los cuales se requiere reducir la vulnerabilidad y dejar a las empresas el análisis de detalle de los aspectos que debe ajustar para lograrlo.

En este nivel, es posible desarrollar modelos formales (computacionales) o trabajar con análisis experto, pero en cualquiera de los dos caminos será necesario contar con información cuantitativa. Por otra parte, si se opta por modelación, se deberá definir si se opta por modelos de sistema o complejos (de agentes) [26].

- *Caracterización de la infraestructura comprometida por evento*

Se debe identificar la infraestructura relevante comprometida, en particular la eléctrica, obviamente, pero también aquella que puede estar relacionada, para cada uno de los escenarios (impactos). Para ello, a partir de la zonificación del evento, se debe establecer tipos

[24] Por ejemplo, el proyecto DECRIS en Noruega, identificó más de 300 escenarios de interés, pero finalmente se analizó del orden de un 10% de estos.

[25] Es clave precisar la infraestructura expuesta (si no hay exposición a amenaza, no hay vulnerabilidad y por lo tanto, el ejercicio siguiente no tiene sentido) y el grado de exposición en cada zona

[26] El uso de modelos computacionales requiere un despliegue mayor de recursos y de información más precisa (o estimaciones detalladas) sobre una cantidad muy significativa de variables. Para el agua potable de Los Ángeles (EEUU), por ejemplo, existe un modelo específico (llamado GIRAFFE).

de infraestructura afectada por grado y sus componentes y su relación con la gestión de la emergencia. Por ejemplo, una zona de almacenamiento puede no ser importante para la operación, pero es importante saber si existen, por ejemplo, residuos en esa zona que pudieran requerir atención (y recursos) en el caso de una emergencia.

Se debe considerar incluir la infraestructura principal (por ejemplo, turbinas), pero también aquella auxiliar que pueda ser relevante para el funcionamiento de la principal, como el equipo de mantenimiento, materiales, caminos de acceso, por ejemplo. La infraestructura principal o auxiliar puede ser comprometida directamente (por daño directo) o indirectamente (al generase efectos que impiden la utilización correcta de la infraestructura). No obstante, la consideración de cuanta infraestructura se incluirá finalmente en el análisis dependerá del marco definido y de las herramientas que se utilice. Es probable que si se utiliza modelos computacionales, no sea posible incorporar mayor nivel de detalle. Esto puede definirse en buena medida en función del alcance deseado.

- *Identificación de Secuencias y Consecuencias*

— Identificación de interdependencias

La infraestructura comprometida debería ser analizada en su interdependencia. En este caso, se considera que para cualquiera de los tipos de interdependencias, hay dos *formas* en términos generales: cadenas de efectos sobre infraestructura que generan resultados sobre otra (que puede o no haber estado comprometida por el evento inicial), y dependencias mutuas directas entre infraestructura que afecta el suministro. Es decir, hay secuencias que deben delimitarse para definir las consecuencias.

Una de las formas más “simples” de presentar estas interdependencias es a través de “mapas” que reflejan la infraestructura afectada y sus relaciones. La generación de estos mapas exige la participación de agentes expertos con conocimiento detallado de la operación de cada uno de los componentes dentro del análisis. La escala “ideal” de estos mapas no debería exceder de 1:5000, de manera análoga a buenos mapas de amenazas para “optimizar” el cruce de la información.

— Caracterización de Impacto Potencial y Fuentes de Vulnerabilidad

Con la caracterización de la infraestructura afectada y las interdependencias, se procede a caracterizar el impacto potencial sobre la infraestructura. Esto consiste en caracterizar los impactos principales y hacer un árbol de posibilidades de otros eventos que podrían darse si se producen ciertas situaciones (en las interdependencias).

Se buscará que los impactos se relacionen con protección y preparación para emergencias, a fin de identificar los elementos de la vulnerabilidad que pueden afectar el impacto potencial. Eso también dará orientaciones sobre aquellos aspectos que pueden ser mejorados para reducir la vulnerabilidad y eventualmente, caracterizar medidas posibles según costo efectividad u otras comparaciones formales.

Dada la gran cantidad de impactos potenciales posibles, es posible también generar indicadores para agruparlos en función de categorías y así poder priorizar ámbitos de investigación más detallada. Otra alternativa es incorporar elementos de probabilidad ya sea para definir eventos en términos probabilísticos o para ayudar a seleccionar aquellos que requieren más atención.

El ejercicio exige la interacción y discusión por parte de los diversos actores relevantes, en particular cuando no se incluye modelos computacionales. En cualquier caso, se requerirá opiniones expertas para formalizar esta parte del análisis.

6.2.3 Análisis de Resiliencia

En esta etapa, es también posible utilizar modelos computacionales, análisis experto o una mezcla de ambos. En ausencia de modelos computacionales, se requiere un mayor grado de apoyo en el trabajo con expertos y, en la medida que se disponga de información, de un análisis de probabilidades de ciertos tipos de situaciones dentro del árbol de posibilidades.

Cualquiera sea el mecanismo que se elija, se requiera simular ciertos casos de impacto potencial en los cuales hay vulnerabilidad relevante. Es decir, el análisis de resiliencia debe considerar la secuencia de "todas" las acciones involucradas al proceso post emergencia y no considerar ninguno necesariamente como "dado", incluyendo en particular los tiempos de desarrollo de cada acción/evento (considerando comunicación, coordinación, desplazamientos, etc..). Se debe considerar la inclusión en el análisis de todas las restricciones administrativas, materiales y de recursos, incluyendo lo siguiente:

— Equipamiento
— Repuestos/materiales
— Personal especializado
— Medios de comunicación y desplazamiento
— Capacidad gerencial / decisión

Evidentemente, no todos estos aspectos podrán ser considerados en la práctica dentro del análisis de resiliencia (en particular si se utiliza simulaciones computacionales, la simplificación será esencial). No obstante, lo que se implica en esta presentación es que todos esos aspectos deben ser considerados como de potencial inclusión y luego se debe definir si se les incluye o no en función de las capacidades específicas (y el marco global del trabajo). De ese modo, lo esencial es no realizar exclusiones *a priori*.

Lo esencial es considerar que con un mayor nivel de detalle no sólo se pude caracterizar mejor el nivel de adaptabilidad y de capacidad de recuperación a las condiciones iniciales de un sistema, sino que además se puede identificar con mayor precisión acciones relevantes que permiten aumentar la resiliencia e incluso someterlas a análisis de costo efectividad.

Se ha presentado una estrategia general para un análisis de seguridad del suministro eléctrico. Su implementación efectiva, como se ha indicado, dependerá de la definición del marco general (objetivos, alcances, profundidad), pero además de la disponibilidad de tiempo y recursos.

La realización de un ejercicio de análisis de seguridad de suministro, requiere tiempo (los ejemplos revisados consideran varios años). Para acotarlos, es condición básica identificar de manera preliminar un conjunto relativamente reducido de situaciones a examinar y luego en cada etapa ir acotando a través de criterios de priorización los "casos" a estudiar. Si se desarrolla modelos computacionales, esto puede implicar reducir el detalle en todos los niveles o, quizás generar criterios formales para examinar casos, o desarrollar métodos iterativos en que los modelos operan sobre la base de opiniones de expertos.

La experiencia muestra entonces, que se requiere tiempo para avanzar de manera significativa en este tipo de esfuerzos, en función de los recursos disponibles. Sobre los recursos mismos, dependerán también de las opciones metodológicas elegidas, las cuales dependen, a su vez, del marco del análisis. Si se trabaja principalmente con análisis experto, se requiere sólo un pequeño grupo de profesionales de apoyo para realizar los análisis cuantitativos puntuales y

para orientar el trabajo que, primordialmente, sería llevado a cabo por los expertos de las propias instalaciones o empresas involucradas.

En cualquier caso, el equipo que direcciona un trabajo de estos alcances debe tener capacidades importantes en gestión de proyectos y considerar la cantidad significativa de tiempo que implica recoger información y coordinar opiniones expertas. Si se opta por modelaciones computacionales como estándar se deberá considerar al mismo grupo de expertos para apoyar el desarrollo del modelo, además de los diseñadores de los modelos mismos. Los recursos se pueden reducir si se opta por modelos simplificados.

7. Referencias

Areas, D. (2009). "Probabilistic tsunami hazard assessment at Seaside, Oregon, for near- and far-field seismic sources", *Journal of Geophysical Research*, 114 (11)

Ayala-Carcedo, F., y Corominas, J. (2002). "Mapas de susceptibilidad a los movimientos de ladera con técnicas SIG", *Insitiuto Geológico y Minero de España Serie Medio Ambiente,* 4, 133-153

Ayala-Carcedo, F. (2001). "Análisis de sostenibilidad y alternativas al Plan Hidrológico Nacional", *Tecnoambiente Madrid*, 11 (106), 21-28

Baker III, G. (2012). A Vulnerability Assessment Methodology for Critical Infrastructure Facilities (In support of the National Capital Region Critical Infrastructure Vulnerability Assessment Project). Virginia: Institute for Infraestructure and Informatio Assurance James Madison University

Bruneau, M., et al. (2003). "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities", *EERI Spectra Journal*, 19 (4), 733- 752.

Calvo, F. (1997). "Algunas cuestiones sobre geografía de los riesgos", *Scripta Nova Revista electrónica de Geografía y Ciencias Sociales de la Universidad de Barcelona* [En línea], nº10.

Cardona, O. (2001). "Manejo ambiental y prevención de desastres: Dos temas asociados", en Ciudades en Riesgo: Degradación ambiental, riesgos urbanos y desastres en América Latina.

Chang, S. (2009). "Infrastructure Resilience to Disasters", *The Bridge,* 44 (3), 36-41

Disaster Risk Reduction Program- Florida International University. (2003). Status of Hazard Maps Vulnerability Assessments and Digital Maps in the Caribbean. The Caribbean Disaster Energency Response Agency.

Department of Homeland Security – EEUU. (2011). Strategic National Risk Assessment December 2011

EMG Consultores. (2012). Identificación de la Infraestructura Energética Nacional y sus Características para Enfrentar Eventos Catastróficos y Análisis de la Infraestructura de la Zona Norte (Informe final preparado para Ministerio de Energía). Santiago de Chile: EMG Consultores

Fridheim, H., et al. (2008). Risk and Vulnerability Analysis of Critical Infrastructures - The DECRIS Approach.

Geller, R., Liu., M., y Stein, S. (2012). "Why earthquake hazard maps often fail and what to do about it", *Tectonophysics* 562–563, 1–25

Giannopoulos, G., Filippini, R., y Schimmer, M. (2012). Risk assessment methodologies for Critical Infrastructure Protection. Part I: a state of the art. European Commission, Joint Research Centre y Institute for the Protection and Security of the Citizen.

Gough, O., y Muir-Wood, R. (2009). The provision of mapped hazard data – availability and best practice in South-East Asia, en OECD 2nd International Cat Risks Conference. Bangkok

Hart, S. (2002). A Method to Assess the Vulnerability of U.S. Chemical Facilities (Special report). Washington: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice

Johanson, J. (2010). Risk and Vulnerability Analysis of Interdependent Technical Infrastructures: Addressing Socio-Technical Systems (Tesis Doctoral). Universidad de Lund, Suecia

Laboratorio de Estudios Urbanos Universidad del BíoBío. (2010). "Estudio de Riesgos de Sismos y Maremoto para Comunas Costeras de la Región del Biobío" (Informe Final).

Lara, L., et al. (2011): "Peligros Volcánicos de Chile". Servicio Nacional de Geología y Minería, Carta geológica de Chile, Serie geología Ambiental 13: 34 p., 1 mapa escala 1:2.000.000.

Lövkvist-Andersen, A., et al. (2004). Modelling Society's Capacity to Manage Extraordinary Events, en Proceedings of the Society for Risk Analysis Conference 15-17 November. Paris

Mardones, M., y Vidal, C. (2001). "La zonificación y evaluación de los riesgos naturales de tipo geomorfológico: un instrumento para la planificación urbana en la ciudad de Concepción", *Eure* [En línea], 27 (81), 97-122.

National Infrastructure Advisory Council. (2009). "Critical Infrastructure Resilience, final report and recommendations" (Infrome final).

NCh 433. Of96. Diseño sísmico de edificios. Instituto Nacional de Normalización de Chile, Santiago de Chile, 1996

Noson, L. (2010). Hazard Mapping and Risk Assessment, The Regional Workshop on Best Practices in Disaster Mitigation

Santella, N., Steinberg, L., y Zoli, C. (2011). "Baton Rouge Post-Katrina: The Role of Critical Infrastructure Modeling in Promoting Resilience", *Homeland Security Affairs*, Volume 7, Article 7

Standards Norway. (2010). "Risk and Emergency Preparedness Assessment", *NORSOK Standard,* Edición 3, Z-013

Subsecretaría de Desarrollo Regional. (2011). Guía de Análisis de Riesgos Naturales para el Ordenamiento Territorial

Taleb, N. (2007). The Black Swan: The Impact of the Highly Improbable. New York: Random House and Penguin.

U.S. Department of Energy, Office of Energy Assurance. (2002). Vulnerability Assessment Methodology, Electric Power Infrastructure