Marco para la evaluación de políticas sobre la gobernanza de la resiliencia de la infrestructura crítica en América Latina

Mary Kate Fisher
Catherine Gamper

BID
Banco Interamericano de Desarrollo

Catalogación en la fuente proporcionada por la Biblioteca Felipe Herrera del Banco Interamericano de Desarrollo

Fisher, Mary Kate. Marco para la evaluación de políticas sobre la gobernanza de la resiliencia de la infraestructura crítica en América Latina / Mary Kate Fisher, Catherine Gamper. p. cm. Incluye referencias bibliográficas. 1. Infrastructure (Economics)-Security measures-Latin America. 2. Infrastructure (Economics)-Risk assessment-Latin America. I. Gamper, Catherine. II. Banco Interamericano de Desarrollo. División de Medio Ambiente, Desarrollo Rural y Administración de Riesgos por Desastres. III. Organización para la Cooperación y Desarrollo Económicos. IV. Título. IDB-CP-60

Autores:
Mary Kate Fisher
CNA División de Seguridad y Vigilancia
Catherine Gamper
Gobernanza Pública y Territorial OCDE
Dirección de Desarrollo

Editores:
Sergio Lacambra
Especialista Líder en Gestión de Riesgo de Desastres, Banco Interamericano de Desarrollo
Charles Baubion
Experto en Gobernabilidad de Riesgos, Gobernanza Pública y Dirección de Desarrollo Territorial Organización para la Cooperación y el Desarrollo Económico, OCDE
Leigh Wolfrom
Analista de Políticas, Dirección de Finanzas y Empresa. Organización para la Cooperación y el Desarrollo Económico, OCDE.

Palabras Clave:
Gobernanza, Resiliencia, Infraestructura crítica, Desastres, Riesgo.

JEL codes:
O18, O54 y Q54

Imágenes:
Claudio Osorio

Diseño y maquetación:
www.verogorri.com

www.iadb.org

Para mayor información, por favor contactar a:
Sergio Lacambra: *slacambra@iadb.org*
Catherine Gamper: *catherine.gamper@oecd.org*

Marco para la evaluación de políticas sobre la gobernanza de la resiliencia de la infrestructura crítica en América Latina

OCDE
MEJORES POLÍTICAS

DIÁLOGO
REGIONAL DE POLÍTICA

BID
Banco Interamericano de Desarrollo

Índice

1. Introducción[1]

La interconexión entre las cadenas de suministro y los sistemas tecnológicos y financieros que constituyen la base de la economía mundial los hace vulnerables a eventos imprevistos como los desastres naturales, las fallas en los sistemas técnicos vitales o los ataques maliciosos. Todo ello puede causar disrupciones y generar impactos a través de las fronteras que en ocasiones resuenan en todo el globo. Durante la última década, la OCDE y los países BRIC han incurrido en pérdidas económicas estimadas en US$1,5 billones como consecuencia de desastres de gran escala. La concentración cada vez mayor de población—especialmente proveniente de grupos vulnerables—y de activos económicos en zonas propensas a desastres figuran entre los principales factores coadyuvantes (OECD, 2014a).

La región de América Latina y el Caribe (ALC) se encuentra particularmente expuesta a amenazas naturales como terremotos y volcanes, así como a eventos climáticos extremos cuya intensificación podría agudizarse a consecuencia del aumento de la variabilidad climática (Economic Commission for Latin America and the Caribbean, 2015; World Bank, 2012). En un estudio general sobre los 15 países más expuestos a tres o más amenazas, siete están en la región (Dilley et al., 2005; Kreft et al., 2015). En particular, se espera que allí las áreas metropolitanas registren niveles más elevados de riesgos en el futuro. En un informe reciente se examinaron los riesgos económicos que pueden afectar a 300 ciudades de gran tamaño en todo el mundo. Allí se señala que el 20% de las 20 ciudades más vulnerables están en América Latina (Cambridge Centre for Risk Studies, 2015). Cuatro quintas partes de su población residen en áreas metropolitanas, lo que la convierte en la región más urbanizada del mundo. Asimismo, las ciudades latinoamericanas se encuentran entre las más desiguales del planeta, lo cual incrementa la concentración de gente pobre –y por lo tanto vulnerable—

La región de América Latina y el Caribe (ALC) se encuentra particularmente expuesta a amenazas naturales como terremotos y volcanes, así como a eventos climáticos extremos cuya intensificación podría agudizarse a consecuencia del aumento de la variabilidad climática

1 Los autores quieren agradecer los insumos y comentarios exhaustivos y constructivos que sobre las distintas versiones de este documento formularon Leigh Wolfrom (Directorio de Asuntos Económicos; OCDE); Jack Radisch y Charles Baubion (Directorio de Gobernanza Pública y Desarrollo Territorial; OCDE) y Sergio Lacambra Ayuso (Especialista Líder en Gestión del Riesgo de Desastres; Banco Interamericano de Desarrollo). Igualmente expresan su gratitud a Charles Baubion (OCDE) por sus comentarios pormenorizados sobre el borrador completo de este documento. Jack Radisch, Stéphane Jacobzone y John Roche (todos de la OCDE), y David Kaufmann (CNA) ofrecieron orientaciones claves sobre la nota conceptual inicial del proyecto. Este documento también se benefició de las discusiones que tuvieron lugar durante el Diálogo Regional de Políticas organizado por el Banco Interamericano de Desarrollo y la OCDE en Panamá en octubre de 2016. Teresa Deubelli prestó su valiosa asistencia en tareas de investigación mientras se realizaba la revisión del presente documento.

potencialmente expuesta a desastres naturales. En el pasado reciente, la región ha sufrido grandes inundaciones, como ocurrió en Colombia en 2010 y en 2011, en el norte de Chile en 2015, así como en Uruguay, Argentina y Brasil en 2016. Lo mismo sucede con los terremotos de gran magnitud como el que afectó a Ecuador en 2016 (Fernandois, 2011; The Economist, 2011; ERCC, 2015; USGS, 2016; Masoero, 2016; Davies, 2016).

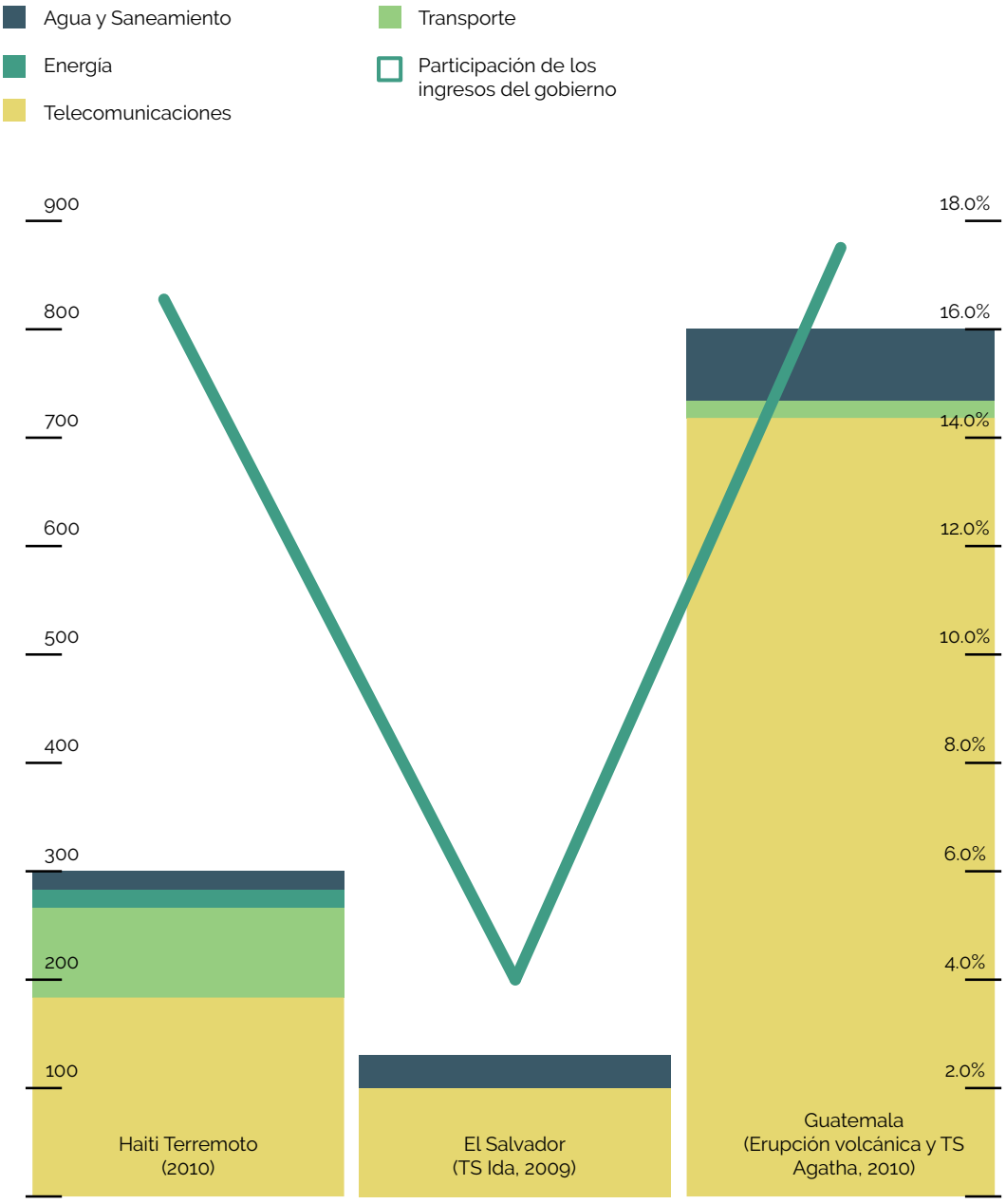
Considerando que las inversiones presentes y futuras en infraestructura constituyen una prioridad de primer orden para fomentar el desarrollo económico en ALC, es fundamental dotarlas de resiliencia, a saber, la capacidad que tenga la infraestructura crítica de absorber y soportar los efectos negativos de los desastres naturales, al tiempo que retiene sus funciones originales (OECD, 2014a; Chang et al., 2013). Durante las próximas décadas, la región se propone invertir una suma significativa de recursos en la construcción de infraestructura –parte de ella crítica— para estimular su productividad y lograr integrarse a las cadenas de suministro internacionales. Se considera que para expandir las posibilidades de producción de las empresas se necesita una oferta de energía y comunicaciones estable y efectiva en función de los costos. Existe la oportunidad para que muchos países de América Latina incorporen elementos de resiliencia en la rehabilitación y modernización de su infraestructura crítica actual, así como en los procesos de planificación de obras futuras.

La infraestructura crítica apuntala las economías, los gobiernos y las sociedades. Es por ello que su resiliencia no solamente determina el grado en que los gobiernos pueden verse afectados por amenazas naturales, accidentes y ataques internacionales, sino también su capacidad de responder y recuperarse de sacudidas adversas. Si no se construye y se maneja en forma apropiada, la disrupción de los sistemas de infraestructuras críticas como son los de energía, transporte, abastecimiento de agua y saneamiento, y comunicaciones puede actuar como vector y propagar el impacto de los desastres. Por ejemplo, el gran terremoto del Este de Japón en 2011 causó interrupciones masivas de electricidad que afectaron a cerca de 4,4 millones de hogares, mientras que las rutas ferroviarias y de navegación se mantuvieron cerradas por 18 días. El terremoto y su cascada de impactos causaron cerca de 16.000 muertes y daños económicos estimados en US$300 mil millones (OECD, 2014a).

El daño de los sistemas vitales puede causar dificultades sociales significativas al interrumpir el acceso a servicios esenciales como la electricidad o el agua potable, además de que produce efectos económicos colaterales al paralizar los negocios hasta mucho después de que haya ocurrido el hecho catastrófico. Estos servicios son fundamentales para el bienestar general de las poblaciones afectadas por un desastre significativo, y pueden o bien favorecer o dificultar su capacidad de recuperación.

En la región de ALC, los desastres de gran escala han puesto en evidencia importantes vulnerabilidades en la infraestructura crítica. Por ejemplo, en Colombia una cuarta parte de las vías pavimentadas sufrieron daños o quedaron

Figura 1.1 Tres ejemplos de las pérdidas y los daños estimados para el sector público por tipo de infraestructura



Fuente: La proporción de daños y pérdidas a cargo del sector público se tomó de los diagnósticos de necesidades posteriores al desastre que se realizaron para cada país (Haití: https://www.gfdrr.org/sites/default/files/GFDRR_Haiti_PDNA_2010_EN.pdf; El Salvador: https://www.gfdrr.org/sites/gfdrr/files/publication/GFDRR_PDNA_ElSalvador.pdf; Guatemala: https://www.gfdrr.org/sites/default/files/Evaluacion_de_danos_y_perdidas_AGATHA_Y_PACAYA_oct_8_2010_reduced.pdf). Para calcular los daños y pérdidas en que incurrieron los países como proporción de los ingresos gubernamentales para el año del respectivo desastre, las cifras correspondientes a tales ingresos se tomaron del World Economic Outlook del FMI de 2014.

destruidas durante las inundaciones y deslizamientos de 2010 (García, 2010). En Chile, el terremoto de 2010 y el subsecuente tsunami ocasionaron el colapso del sistema de comunicaciones, dificultando en buena medida la capacidad del gobierno para responder a la catástrofe. Los sistemas de salud y educación quedaron gravemente afectados: numerosos hospitales sufrieron daños y algunas escuelas públicas se mantuvieron cerradas hasta por 45 días. El terremoto y su cascada de efectos produjeron daños económicos por una cifra equivalente al 18% del PIB (OECD, 2014a).

La reconstrucción de infraestructura vital posterior a un desastre también puede representar una proporción significativa de todos los costos de reconstrucción a cargo del Estado. Los costos de recuperar la infraestructura pueden ser de gran magnitud y a menudo el gobierno tiene que asumirlos. En la figura 1.1 se observan los costos estimados en que incurrió el sector público en tres desastres recientes de gran magnitud en Haití, El Salvador y Guatemala, así como su proporción en relación con los ingresos del sector público. Asimismo ilustra que el impacto de las disrupciones que sufre la infraestructura crítica depende del sector afectado, siendo más costosas las que afectan al sector del transporte. En un estudio reciente se estableció que varios países de la región, entre ellos Guatemala, Honduras, Colombia, México y Brasil, podrían ver afectada la calificación de su deuda soberana debido al impacto de un ciclón tropical o una inundación con un periodo de retorno de 1 en 250 años por sus implicaciones en el crecimiento económico, las finanzas nacionales y el comercio exterior, con el agravante de que el cambio climático puede intensificar sus posibles impactos (Standard & Poor's Ratings Services, 2015).

En circunstancias óptimas, la infraestructura crítica resiliente puede resistir o absorber los efectos de un shock y recuperarse de manera que mejore la eficacia y prontitud con que se realizan las actividades de atención a la emergencia. Sin embargo, allí donde la infraestructura crítica no sea capaz de soportar los impactos de un shock, puede terminar actuando como multiplicadora de peligros, agravando la severidad del evento a medida que la cascada de efectos dentro de los distintos sectores y a través de ellos agrega capas adicionales de complejidad, y a menudo dificulta, e incluso previene, la ejecución de las labores de auxilio. El sector público desempeña un papel fundamental en el fomento de la resiliencia de la infraestructura crítica, por ejemplo evaluando las acciones de reducción de riesgos emprendidas por sus dueños/operadores, o también financiando actividades que mejoren el nivel de conciencia de aquellos sobre los riesgos existentes y las correspondientes

La reconstrucción de infraestructura vital posterior a un desastre también puede representar una proporción significativa de todos los costos de reconstrucción a cargo del Estado.

medidas de resiliencia. A pesar del progreso alcanzado por algunos países en materia de reducción de riesgos y aumento de su preparación, las medidas relativas a garantizar la resiliencia de la infraestructura crítica siguen siendo un desafío clave.

El objetivo de este informe es desarrollar un marco de evaluación de políticas sobre la gobernanza de la resiliencia de la infraestructura crítica. Con base en análisis prospectivos de buenas prácticas de resiliencia de infraestructura crítica se avanza a partir de las orientaciones pertinentes que sobre el particular ha dado la OCDE a través de su *Recommendation on the Governance of Critical Risks* (2014b) y su *Recommendation on Disaster Risk Financing Strategies* (próximo a publicarse). Asimismo se proporcionan guías adicionales sobre la aplicación de principios de gobernanza responsable y otros de gestión financiera que de allí se derivan para manejar los riesgos relacionados con infraestructura crítica. Los temas identificados informarán la elaboración de un borrador de cuestionario para los países individuales que sirva de base para realizar análisis comparativos posteriores sobre las políticas y prácticas en la gobernanza de la resiliencia de la infraestructura crítica entre varias naciones de América Latina y el Caribe. Dado que las inversiones en infraestructura son prioridades de primer orden para fomentar el desarrollo económico en la región, dotar de resiliencia a las inversiones actuales y futuras en ese sector es de primordial importancia. Los hallazgos que surjan de los estudios de caso serán usados para informar las políticas y las estrategias generales de los países para fortalecer la resiliencia de los activos y servicios de las infraestructuras críticas.

2. El imperativo de la resiliencia en la infraestructura crítica: lecciones del pasado

Buena parte de los objetivos actuales de los países en cuanto a lograr que su infraestructura crítica sea más resiliente se basa en información obtenida de experiencias pasadas con infraestructuras fallidas. Si bien es indispensable adoptar una óptica mucho más prospectiva en el diseño de estrategias de gestión de riesgos --en particular para el manejo de infraestructura crítica--, estas enseñanzas constituyen un punto de partida bastante informativo y pueden imprimirle el ímpetu necesario a la inversión en fortalecimiento de resiliencia.

En la siguiente sección se describen ejemplos de fallas de infraestructura pasadas y de las lecciones aprendidas. Allí se mostrará que los efectos asociados con aquellas por lo generan han sido vastos e imprevistos. Los ejemplos que se registran en esta sección fueron elegidos con la intención de mostrar diferentes tipos de fallas de infraestructura. El primer ejemplo es la súper tormenta Sandy en Nueva York y Nueva Jersey. Allí se describe el caso en que un evento climático extremo produjo fallas en infraestructuras críticas y sus efectos asociados en un área que recibió apoyo considerable destinado a la preparación frente a desastres después de los ataques terroristas del 11 de septiembre de 2001. En el segundo ejemplo se describe el gran terremoto del Este de Japón y su cascada de efectos, el tsunami y el accidente de la planta nuclear Fukushima Daiichi, todo lo cual evidenció la necesidad

de incorporar un enfoque de planificación de infraestructura crítica que abarque todos los peligros posibles. El tercer ejemplo ilustra un apagón de gran magnitud y su cascada de efectos en el noreste de Estados Unidos y Canadá en 2003, el cual ilustra las consecuencias de posponer el mantenimiento de infraestructura crítica y la insuficiencia de los sistemas estándares de redundancia. Los demás ejemplos --el terremoto de Perú en 2007 y el de Chile en 2010-- demuestran los efectos colaterales y las interconexiones de los sectores de servicios vitales para la población.

2.1 Huracán Sandy, Estados Unidos, 2011

A finales de octubre de 2012, la súper tormenta Sandy azotó a Nueva Jersey y a Nueva York. Sus secuelas se calcularon en cerca de US$68 mil millones en daños e impactos de gran magnitud en los sectores de energía, transporte, comunicaciones, agua y salud en la gran área metropolitana de Nueva York-Nueva Jersey (Flynn, 2015). Se estima que cerca de 8,5 millones de hogares se quedaron sin electricidad y que 5,4 millones de personas se vieron afectadas por la suspensión del servicio de subterráneo. Solamente los daños al sistema de transporte se calcularon en más de US$ 10 mil millones (OECD, 2014a). Después de que Sandy tocara tierra, a lo largo de la costa este de Estados Unidos quedaron en plena evidencia las interdependencias del sistema de abastecimiento y distribución de gasolina, estrechamente interconectado con el sector eléctrico. A diferencia de crisis previas de abastecimiento de gasolina a causa de otros huracanes en Estados Unidos, Sandy afectó principalmente a los consumidores y no a los productores. Algunas de las áreas más afectadas se encontraban en desventaja incluso desde antes de que el huracán tocara tierra, ya que las estaciones de venta de gasolina al detal sufrían escasez o habían agotado completamente sus existencias, debido al aumento de la demanda como resultado de los preparativos que la gente estaba haciendo para hacerle frente a la tormenta. Después de que Sandy golpeara, muchas de las estaciones que sí tenían existencias no podían dispensar gasolina porque sus bombas no funcionaban a falta de electricidad (NACS, 2013). Estas interdependencias entre los sectores eléctrico y de combustibles, así como su posible cascada de efectos, no se habían previsto.

Lecciones aprendidas

Se han identificado cuatro factores responsables por las fallas observadas en la infraestructura crítica (Flynn, 2015). Primero, las partes interesadas estaban poco conscientes de las interdependencias entre las infraestructuras críticas y del potencial para que ocurriera una cascada de efectos asociados con las interrupciones en los sistemas (p. ej., los vínculos entre la red de distribución y venta al detal de gasolina y el sistema eléctrico). En segundo lugar, la elaboración de estándares no ha evolucionado a la par con el desarrollo de diseños, herramientas y prácticas de ingeniería más modernos que podrían mejorar la resiliencia de los sistemas interdependientes. Elementos críticos de los servicios de transporte --túneles, puentes, líneas o estaciones ferroviarias, o estaciones de los sistemas metropolitanos de tránsito de Nueva Jersey/Nueva York que constitu-

yen los medios principales para movilizar personas y bienes-- se encuentran ubicados en zonas bajas que en muchos casos no han sido construidas para tolerar las inundaciones. En tercer lugar, los marcos actuales de gestión organizacional y de gobernanza regional no han sido lo suficientemente bien diseñados como para tomar en cuenta las interdependencias de sectores vitales: combustibles, electricidad, agua, transporte y comunicaciones. Por ejemplo, con excepción solo de los casos más graves, los planes de evacuación de las instalaciones de salud llevaron a que todos los pacientes fueran devueltos a una comunidad que en últimas no estaba preparada para manejar equipos médicos en sus hogares o para suministrar transporte para que el personal del cuidado de la salud se desplazara a atender a los enfermos que se encontraban recluidos en sus casas. En cuarto lugar, no hay suficientes incentivos económicos o de políticas para desarrollar resiliencia, y en muchos casos existen desincentivos financieros e institucionales que impiden que se haga. Por ejemplo, cuando ocurren desastres muchos de los operadores de los sectores público y privado optan por aceptar la ayuda federal en lugar de valerse de sus propios fondos para invertir en medidas de resiliencia. La falta de coordinación y colaboración suficientes a lo largo de las áreas metropolitanas de Nueva Jersey y Nueva York en el manejo de las amenazas que implican los desastres para las estructuras vitales regionales fue otro de los factores que contribuyeron a exacerbar los impactos de esta catástrofe (Flynn, 2015).

Ante la magnitud de las tareas de recuperación, el Presidente de Estados Unidos creó el Grupo de Trabajo para la Reconstrucción después del Huracán Sandy, el cual quedó a cargo de "identificar y trabajar para remover los obstáculos que se interponen a una reconstrucción resiliente, al tiempo que se consideran los riesgos presentes y futuros y se promueve la sostenibilidad de largo plazo de las comunidades y ecosistemas [que se encuentran] en el área afectada por Sandy" (Hurricane Sandy Rebuilding Task Force, 2013). En este informe, el Grupo de Trabajo señaló el impacto particularmente devastador que la tormenta tuvo en la infraestructura de energía (p. ej., apagones masivos y escasez de combustibles), comunicaciones, transporte, agua y manejo de aguas residuales, y salud de la región, con los consecuentes retrasos en los esfuerzos de atención y recuperación, y la pérdida de actividad económica. Con base en las lecciones aprendidas durante el proceso de recuperación, el Grupo de Trabajo formuló 69 recomendaciones, de las cuales en cerca de la mitad se hacía un llamado para que se desarrollara resiliencia en el curso de proceso mismo de recuperación (Hurricane Sandy Rebuilding Task Force, 2013).

En respuesta a los apagones masivos que siguieron al huracán Sandy en Nueva York y Nueva Jersey, la Agencia Federal de Gestión de Emergencias (FEMA por su sigla en inglés) estableció, a solicitud del Presidente, el Grupo de Trabajo para el Restablecimiento de la Energía. Este Grupo de Trabajo respaldó un esfuerzo masivo en tal sentido durante el cual las compañías de electricidad implementaron acuerdos de asistencia mutua para desplegar más de 70.000 trabajadores en las áreas afectadas. Esto permitió transportar por vía aérea 229 vehículos de restablecimiento de energía y 487 miembros del

personal técnico con el fin ayudar a Nueva York y a Nueva Jersey a rehabilitar el fluido eléctrico (FEMA, 2013)

2.2 El gran terremoto del Este de Japón, 2011

En 2011, un terremoto ocurrido frente a la costa de Japón causó daños significativos en tierra y produjo una serie de gigantescas olas de tsunami que afectaron gravemente la costa nororiental. A su vez, las inundaciones que produjo el tsunami en la zona continental provocaron un grave accidente nuclear en la planta Fukushima Daiichi (McGee et al., 2014). Si bien las instalaciones de la planta sobrevivieron al terremoto sin sufrir mayores daños e incluso se activaron correctamente los procedimientos de emergencia previstos para suspender su actividad, el diseño del sitio no permitió prevenir las inundaciones del tsunami, pues excedían de manera significativa la altura de las barreras existentes. El terremoto ocasionó la caída de la red eléctrica en el área, y cuando el tsunami rompió los muros de la planta, la inundación subsecuente dejó sumidas bajo el agua las unidades de fluido eléctrico operadas con diésel, así como las baterías secundarias DC de repuesto (Acton y Hibbs, 2012). Debido a la falta de electricidad, la planta no estaba en capacidad de producir suficiente refrigeración para tres de sus reactores, cuyos núcleos quedaron totalmente fusionados (nivel 7 en una escala de Evento Nuclear Internacional de 1 a 7), siendo este incluso peor que el del desastre de Chernóbil en 1986 (McGee et al., 2014). Se estima que 4,4 millones de hogares fueron afectados por la reducción del fluido eléctrico de TEPCO, la compañía eléctrica de Tokio. Asimismo, el tren de alta velocidad Shinkansen estuvo cerrado durante dos semanas (OECD, 2014a).

Lecciones aprendidas

Los análisis posteriores al suceso revelaron que la fusión nuclear se hubiera podido prevenir hasta cierto punto. Si en el diseño de la planta se hubiera incorporado el concepto de resiliencia es posible que los impactos hubieran sido menores. Por ejemplo, el sistema de refrigeración de la planta era funcionalmente dependiente de un abastecimiento garantizado de electricidad, y la respuesta del cuerpo de bomberos habría sido más oportuna y el impacto habría sido menor si las rutas de tráfico no hubieran quedado bloqueadas (Bach et al., 2013). Aunque es cierto que la industria nuclear japonesa tenía los estándares más elevados de todo el mundo en cuanto al manejo de riesgos sísmicos, es posible que esto hubiera impedido que se tomara en cuenta un rango más amplio de riesgos colaterales. Estos factores coadyuvantes demuestran el papel crítico que cumplen los reguladores efectivos, así como la necesidad de llevar a cabo visitas regulares de control de seguridad que den cuenta y conduzcan a la incorporación tanto de escenarios dinámicos y cambiantes, como de las mejores prácticas del momento (Acton y Hibbs, 2012).

2.3 El apagón del noreste de Estados Unidos y Canadá, 2003

El 14 de agosto de 2003, una falla ocasionada por el roce de una línea eléctrica de alto voltaje contra unos árboles de-

masiado crecidos condujo al apagón del sistema (Minkel, 2008). Un suceso de este tipo habría activado el sistema de alarma, pero este también falló. Mientras que los operadores trataban de identificar el problema, otras líneas eléctricas rozaron los árboles y se apagaron, lo cual condujo a crear una sobrecarga en las que continuaban operando. A las dos horas de que se presentara el problema original, las líneas afectadas por la sobrecarga se apagaron, desatando una cascada de fallas en el sureste de Canadá y en ocho estados del noreste de Estados Unidos (Minkel, 2008). El apagón impactó a una variedad de sectores de infraestructura críticos, entre ellos los de energía, comunicaciones, salud, alimentos, agua, transporte, protección, gobierno, manufactura y también el sistema financiero (Public Safety and Emergency Preparedness Canada, 2006). En últimas, el apagón afectó a 50 millones de personas y sus costos estimados fueron de US$6 mil millones (Minkel, 2008).

Lecciones aprendidas

El apagón de 2003 sirve como estudio de caso para ilustrar los retos asociados con la existencia de niveles variados y fragmentados de control, autoridad y rendición de cuentas en infraestructuras críticas (U.S.-Canada Power System Outage Task Force, 2004). El informe bilateral oficial en el cual se examina el apagón del nordeste de 2003 contiene una descripción de las causas directas y factores coadyuvantes del incidente, incluyendo los siguientes: "incapacidad de mantener el soporte adecuado en materia de poder reactivo; incapacidad de asegurar la operación del sistema dentro de límites seguros; manejo inadecuado de la vegetación; adiestramiento deficiente de los operadores; incapacidad de identificar condiciones de emergencia y comunicar la situación a los sistemas circunvecinos; y visibilidad regional inadecuada del sistema eléctrico como un todo" (U.S.-Canada Power System Outage Task Force, 2004). Esto condujo a que, por ejemplo, en la ciudad de Ottawa los puentes que cruzan hacia Quebec solo estuvieran parcialmente iluminados porque en Gatineau, Quebec, todavía había luz, aunque aparentemente no existía capacidad para enviar electricidad hacia la provincia de Ontario.

Estos hallazgos se tradujeron en varias lecciones notables expresadas a manera de recomendaciones. Por ejemplo, el Grupo de Trabajo sugirió que, en caso de presentarse conflictos, los reguladores, la industria eléctrica y sus grupos de interés relacionados adhirieran a estándares elevados de confiabilidad –usando mecanismos de mercados cuando y donde fuera posible-- por encima de los objetivos comerciales (U.S.-Canada Power System Outage Task Force, 2004). Asimismo se hizo énfasis en que tanto los reguladores como los consumidores reconocieran que la confiabilidad requiere inversiones y gastos operacionales con los que las empresas pueden no querer comprometerse, a menos que los reguladores les garanticen la recuperación de costos (U.S.-Canada Power System Outage Task Force, 2004). Como resultado del análisis sobre el incidente del apagón, el Congreso de Estados Unidos expidió la Ley de Política Energética de 2005 mediante la cual se habilitaba a la Comisión Federal de Regulación Energética (FERC por si sigla en inglés) para hacer cumplir los estándares de la nueva Corporación Norteamericana para la Confiabilidad de la Electricidad. Cin-

co años después de ocurrido el incidente, la FERC había aprobado 96 nuevos estándares de confiabilidad (Minkel, 2008).

2.4 Terremoto de Pisco, Perú, 2007

La costa peruana ha sido afectada por una serie de movimientos telúricos fuertes, y en agosto de 2007 un terremoto de magnitud 8,0 sacudió la tierra cerca de la ciudad de Pisco (USGS, 2007). Como resultado del "Terremoto del Sur", la ciudad de Ica y otras poblaciones costeras localizadas al sur de Lima se quedaron sin electricidad y sin servicio de teléfono. Los daños sufridos por las autopistas y los puentes, y la caída de postes telefónicos, impidieron que los rescatistas llegaran a las áreas afectadas. El sistema de salud sufrió graves impactos, con un total de 14 instalaciones destruidas y otras 112 afectadas. Desbordado por el número de pacientes, el hospital de Pisco no pudo prestar servicios debido a la falta de agua y electricidad. El servicio de agua quedó inhabilitado por un promedio de 16 días en el 81% de los hogares, y se requirió el uso de camiones-cisterna como alternativa principal para el abastecimiento de agua (World Bank, Water and Sanitation Program, 2011). Incluso seis semanas después del terremoto, algunas áreas de Pisco solo estaban recibiendo agua por una hora al día, lo cual complicó la prestación de servicios de salud (United Nations Office of the Resident Coordinator, 2007; Chapin et al., 2009). El costo de las reparaciones requeridas en los sistemas de agua y saneamiento fue el equivalente a lo que hubiera costado instalar un mínimo de 8.183 conexiones de agua y 7.925 de alcantarillado para beneficiar a más de 160.000 residentes. La restauración de los sistemas de agua y saneamiento a su condición previa a la catástrofe requirió el equivalente a 6,5 veces el presupuesto invertido en los rubros de agua y saneamiento por las autoridades provinciales en 2007. Si los proveedores de estos dos servicios hubiesen realizado el mantenimiento regular, el costo estimado de los daños hubiera sido seis veces menos (World Bank, Water and Sanitation Program, 2011).

Lecciones aprendidas

El Terremoto del Sur que azotó a Perú en 2007 reveló una serie de vulnerabilidades relacionadas con la interconexión de sectores vitales (agua y salud, y electricidad y salud). A raíz de las complicaciones observadas en relación con la existencia de daños estructurales significativos después del terremoto, el gobierno promulgó una nueva ley (la Ley N° 29078) mediante la cual se creó el Fondo para la Reconstrucción del Sur (FORSUR) y autorizó un crédito suplementario por US$ 31,6 millones destinado a la reconstrucción de infraestructura pública en las áreas afectadas por el terremoto (Chapin et al., 2009; Taucer et al., 2009). Esto se amplió al nivel nacional con la expedición de la Ley N° 29951 mediante la cual se otorgaron recursos específicos para financiar actividades de identificación de riesgos en los sectores de medio ambiente, salud, vivienda, y agua y saneamiento. La ley también validó la asignación de recursos de destinación específica para financiar la reducción de riesgos en los sectores de vivienda, educación, salud, transporte y agricultura. A partir de la experiencia acumulada con el terremoto de 2007, el gobierno también reestructuró (Ley N° 29664) las responsabilidades de gestión de emergencias y reducción de riesgos frente a desastres para asegurar que se dé

atención y financiación suficientes a las labores de identificación y reducción de riesgos, así como a los procesos de preparación y atención (IDB, 2015).

2.5 Terremoto de Chile, 2010

El terremoto que sacudió a la costa central de Chile el 27 de febrero de 2010 produjo daños estimados en US$30 mil millones, equivalentes al 18% del PIB; de ese total, US$20,9 mil millones (12,7% del PIB) correspondieron a daños en la infraestructura. El terremoto afectó a una región que alberga entre el 30 y el 40% de la capacidad manufacturera del país. Casi todas las actividades comerciales quedaron suspendidas en esa área durante varios días, y mientras que la mayoría de las industrias logró reiniciar producción, algunas de las más importantes –especialmente las de producción de pulpa de papel, vinos y refinación de petróleo-- redujeron sustancial o completamente su actividad comercial durante meses. En marzo de 2010 se estimó que la disminución de la actividad manufacturera en el país ascendía al 5%. La interrupción de la actividad económica continuó durante los tres meses siguientes; finalmente, en julio de 2010 se regresó a los niveles previos a la catástrofe (Muir-Wood, 2011). Los impactos del terremoto hubieran podido ser mucho peores si no hubiera sido por la planificación deliberada que se hizo en el sector energético, y por la existencia de códigos rigurosos de construcción antisísmica (Fermandois, 2011).

Lecciones aprendidas

A partir de una serie de reflexiones sobre los impactos del terremoto de 2010, el gobierno chileno emprendió una serie de acciones para hacer frente a las vulnerabilidades observadas. A nivel operacional se comprometió a resolver los cortes en las comunicaciones con inversiones en procesos de monitoreo en tiempo real y en sistemas robustos de telecomunicaciones con sus respectivos sistemas auxiliares (Fermandois, 2011). La Asociación de Aseguradoras de Chile (AACH) ha venido desarrollando un mapa para identificar todas aquellas áreas que sean susceptibles a los impactos de sismos y tsunamis dentro de la economía. Se espera que este mapa constituya una herramienta de uso público que contribuya al diseño de metodologías futuras para la gestión de riesgos frente a desastres. En cooperación con la agencia que regula y supervisa a la industria aseguradora, la AACH también está elaborando un modelo de riesgos para terremotos y tsunamis que será compartido con las autoridades del gobierno para que lo empleen en el diagnóstico de riesgos y en el desarrollo de políticas públicas de inversión pública y privada en infraestructura (OECD, 2015a). A pesar de contar con códigos de construcción sólidos, las pérdidas en materia de vivienda y otra infraestructura fueron extensas y no estaban aseguradas contra desastres. Para garantizar una recuperación inmediata de los daños en vivienda e infraestructura, el gobierno adoptó una posición proactiva aumentando los impuestos para destinarlos a esas tareas (Comerio, 2013).

2.6 Conclusiones

Los desastres ponen en evidencia las complejidades y vulnerabilidades de los sistemas interdependientes de infraestructura crítica. Las principales catástrofes

del pasado permiten hacerse una idea sobre la gama de posibles consecuencias y enseñanzas en materia de políticas públicas. En muchos casos, las estructuras de incentivos --como por ejemplo la asistencia gubernamental casi segura o garantizada después de una catástrofe-- pueden haber desestimulado una mayor inversión *ex ante* en medidas de resiliencia. Los operadores de infraestructura crítica podrían no cumplir con las regulaciones en materia de resiliencia si no se les da la certeza de que van a recuperar los costos de tales inversiones. Los esquemas de gobernanza también pueden cumplir una función crítica en lo que corresponde a impulsar la resiliencia. La incapacidad de alinear control, rendición de cuentas y autoridad puede conducir a que los operadores de infraestructura crítica no inviertan suficiente en resiliencia. Por ejemplo, el Gran Terremoto del Este de Japón ha mostrado la necesidad de dotar a los órganos responsables de la vigilancia regulatoria de la suficiente independencia para hacer cumplir y monitorear la implementación de medidas de resiliencia. Lograr que los esquemas efectivos de gobernanza funcionen es incluso más difícil cuando los impactos de un desastre atraviesan las fronteras de un país, tal y como sucedió durante el apagón de 2003 en Canadá y Estados Unidos. Para manejar los riesgos de infraestructuras transfronterizas vitales, los gobiernos deberían considerar la posibilidad de establecer mecanismos de coordinación y colaboración.

Sin embargo, la implementación de inversiones significativas solo puede ocurrir si existe un marco amplio y coordinado de riesgos que guíe la incorporación de tales lecciones, acciones e inversiones públicas y privadas en la mejora de la capacidad que tengan los sistemas de infraestructuras críticas de absorber, adaptarse y recuperarse de las perturbaciones causadas por las catástrofes.

3. El papel cambiante de la resiliencia

3.1 De la protección a la resiliencia de la infraestructura crítica

Por décadas, los gobiernos se han enfocado en la importancia de las infraestructuras críticas y sus vulnerabilidades asociadas. Hasta mediados de los años 2000, la mayoría de las políticas y actividades relacionadas se centraban en la protección de los activos. Dados los costos crecientes los desastres naturales, y con posterioridad a los atentados del 11 de septiembre de 2001 en los Estados Unidos, las bombas en Bali en 2002 y en Londres en 2005, y los ataques cibernéticos cada vez más frecuentes, los gobiernos pasaron de centrarse en la protección a privilegiar la resiliencia de la infraestructura crítica (Critical Five, 2014). En este contexto, la resiliencia puede definirse como la capacidad que tiene la infraestructura crítica de absorber disrupciones mientras retiene esencialmente la misma función que tenía antes del shock (OECD, 2014a; Chang et al., 2013). Una extensión de esta definición la ofrece Barami (2013), quien señala la naturaleza compleja y multifacética de la resiliencia de la infraestructura crítica. Este autor aplica un enfoque de varias capas basado en riesgos, el cual da cuenta de las complejas interdependencias que existen entre las infraestructuras, al tiempo que considera posibles soluciones aplicables a través del ciclo de vida del sistema (p.ej., diseño, construcción y operación). Así pues, la resiliencia se define no como un solo resultado o exclusivamente como la capacidad de recuperarse con posterioridad a un desastre exclusivamente, sino más bien como un proceso dinámico que aplica un método basado en riesgos y en el ciclo de vida para abordar las vulnerabilidades de los sistemas

críticos de infraestructura, buscando que estos sean más tolerantes a las fallas, más eficientes, más inteligentes, y que tengan una mayor capacidad de adaptarse a desafíos inesperados (Barami, 2013).

Bajo el paradigma de protección, las partes interesadas veían el manejo de riesgos fundamentalmente bajo la óptica de los activos y se enfocaban en la seguridad y en medidas físicas para prevenir del todo las disrupciones en la operación de estas infraestructuras. El cambio hacia una perspectiva basada en la resiliencia se produjo en parte cuando se reconoció que existía un grado considerable de incertidumbre sobre la intensidad y complejidad de desastres futuros, siendo el cambio climático uno de los factores que más influyeron. La naturaleza de escalas impredecibles exige entonces enfoques incrementales que no pueden eliminar --o incluso predecir suficientemente-- los impactos de las catástrofes, pero que sí pueden dotar a los activos y a los sistemas de la capacidad de ser restaurados y rehabilitados rápidamente. Por ejemplo, los impactos en la infraestructura crítica de un suceso como el huracán Sandy en un área que había recibido financiamiento considerable y participado en actividades sustanciales de protección con posterioridad a los ataques del 11 de septiembre de 2001, demostraron que las actividades de protección por sí solas no eran suficientes para hacer frente a todo un rango de posibles impactos en las infraestructuras críticas y otros riesgos asociados con sus interdependencias. Más aún, la magnitud de las actividades y medidas requeridas para proteger plenamente estas infraestructuras de todos los peligros hace que sus costos sean prohibitivos. De allí que fuera deseable dotarlas de la capacidad de absorber, adaptarse e incluso fallar de manera segura.

El énfasis en la resiliencia no excluye la protección, como tampoco las consideraciones de seguridad. Lo que sí hace es ampliar la lente de los marcos de la infraestructura crítica para incorporar allí acciones preventivas que la protejan de todos los peligros, se hagan efectivas a todo lo largo de ciclo de manejo de riesgos (Moteff, 2012), y operen con conceptos integradores como adaptabilidad, flexibilidad y robustez (Flynn, 2008; Barami, 2013). Esto también incluye el desarrollo de medidas de resiliencia financiera, a saber, la capacidad y los recursos necesarios para absorber y recuperarse de los desastres sin sufrir mayores apuros financieros (G20/OECD, 2012). Esto se puede lograr asegurando que los dueños/operadores de las infraestructuras críticas en los ámbitos nacional, subnacional o privado pongan en marcha los esquemas financieros apropiados para mitigar su exposición a los riesgos frente a desastres. Entre los enfoques disponibles figuran la transferencia de riesgos a través de mecanismos de aseguramiento o la destinación de recursos para la recuperación de costos de tales sucesos catastróficos (G20/OECD, 2012). Las asociaciones público-privadas, así como los subsidios públicos, pueden ser útiles para destrabar financiamiento adicional de inversiones en medidas estructurales y su mantenimiento que impulse en el largo plazo enfoques de resiliencia más efectivos en función de los costos que la financiación *ex post* (Barami, 2013; OECD, 2016).

3.2 Desafíos de gobernanza para la resiliencia de la infraestructura crítica

Cuando se trata de dotar de resiliencia a la infraestructura, surgen numerosos retos derivados de la presencia de una variedad de grupos de interés con diferentes objetivos e incentivos:

- Es posible que los dueños y los operadores de las infraestructuras críticas tien-

dan a no invertir lo suficiente en resiliencia, comparado con lo que sería socialmente óptimo. Dado que su preocupación principal son los intereses de su organización, los operadores de infraestructura crítica pueden estar pasando por alto los riesgos y la correspondiente cascada de costos que tiene para la sociedad la alteración de los servicios. A esto también puede contribuir la poca experiencia directa con desastres causantes de la paralización de infraestructuras críticas y otros efectos colaterales. Si no existen los requisitos legales pertinentes, y si los riesgos no se comunican de manera efectiva a grupos específicos, es probable que los proveedores carezcan de incentivos para ir más allá de evitar o mitigar el daño físico que puedan sufrir sus propios sistemas. En muchos casos, la responsabilidad legal de las disrupciones de las infraestructuras críticas corresponde a los proveedores de servicios que dependen de aquellas y no a sus operadores (p. ej., cuando un apagón en un edificio causa accidentes, cuál sería la responsabilidad legal del dueño del edificio?) (Chang et al., 2013)).

- Es posible que la falta de inversión suficiente en resiliencia se deba a que se confía demasiado en el gobierno como la única opción para obtener recursos financieros. Si hay evidencia previa de asistencia financiera post desastres para la rehabilitación y reconstrucción de infraestructura pública, es posible que no hayan los incentivos suficientes para invertir en medidas de resiliencia *ex ante* a los desastres, independientemente de si la infraestructura es pública o privada.
- Si los operadores de infraestructura crítica --particularmente en el sector privado-- tienen un marcado interés en maximizar eficiencia y lucro, podrían solicitar a sus ingenieros que diseñen sistemas que cumplan, pero que no excedan, los estándares de seguridad. Asimismo, es posible que se premie a los administradores por apalancar y aprovechar capacidad operativa no utilizada. Inevitablemente, los sistemas de infraestructura crítica diseñados y operados en este entorno se vuelven más vulnerables a los eventos climáticos extremos, al tiempo que sus capacidades para absorber y recuperarse rápidamente de los impactos disminuyen (Flynn, 2015).
- Es posible que los dueños y operadores de infraestructura crítica actúen de acuerdo con intereses organizacionales y no de acuerdo con intereses regionales o nacionales, lo cual puede resultar en un suministro subóptimo de medidas de resiliencia. Ejemplo de ello son las represas a lo largo de un río construidas por el operador de una planta hidroeléctrica, pero que también podrían proteger otras estructuras río abajo si se construyeran de manera apropiada. Puede que los operadores de las represas solo estén dispuestos a incorporar aquellas medidas de resiliencia que protejan a otros operadores de otras infraestructuras críticas río abajo si los costos incurridos en ellas son compartidos por todos. Si el problema de la acción colectiva se pasa por alto, los operadores río arriba podrían ignorar las necesidades relacionadas con las infraestructuras río abajo y dejarían pasar la opción de implementar medidas de resiliencia a niveles de costo óptimos.
- Los gobiernos no siempre están en capacidad de hacer que los operadores públicos y privados de infraestructuras críticas las doten de resiliencia. Es posible, por ejemplo, que las autoridades tengan problemas en establecer estándares y requisitos apropiados de resiliencia, ya que definir los objetivos de esta última puede ser una tarea compleja, mientras que el

diseño de los estándares puede involucrar una amplia variedad de competencias técnicas y una cooperación estrecha con los operadores de infraestructura para evaluar la factibilidad técnica y financiera vis a vis los objetivos de resiliencia deseados. Por ejemplo, es posible que los operadores de energía requieran diferentes medidas de resiliencia que las que necesitan los operadores de transporte y telecomunicaciones, incluso ante los mismos peligros. Debido a la complejidad y a la diversidad de las medidas apropiadas de resiliencia requeridas por ley, los gobiernos por lo general se valen de relaciones colaborativas con peritos expertos del sector privado para monitorear continuamente su implementación. Asimismo, es posible que los requisitos legales para la implementación de tales medidas creen problemas de competencia y falta de voluntad entre aquellos operadores que deben implementarlas. Además de que algunos operadores podrían no disponer del financiamiento necesario para cubrir el costo de dcihas medidas, este requerimiento genera una ventaja comparativa en otros operadores que no están obligados legalmente a realizar estas inversiones.

Para diseñar y poner en marcha las políticas correctas es clave identificar los respectivos desafíos y cuellos de botella. Al mismo tiempo, es importante considerar todas las consecuencias posibles derivadas de las opciones de política y regulatorias adoptadas para impulsar la resiliencia de las infraestructuras críticas. Por ejemplo, si después de un desastre los responsables por la formulación de políticas crean un entorno en el que se ofrecen incentivos solamente para que los dueños reparen la infraestructura hasta dejarla en su condición inicial --desperdiciando así la oportunidad natural de "construir de nuevo y mejor"--, habrá mayores posibilidades de que los operadores del sector de infraestructura hagan lo mismo, a menos que exista un beneficio adicional para su negocio por realizar esta mejora Como en cualquier otro negocio, los dueños y los operadores de las infraestructuras críticas sacrifican unas cosas por otras con base en los riesgos conocidos y las inversiones económicamente racionales, vis a vis la dinámica de un mercado competitivo y las restricciones de recursos. También es posible que las empresas no se unan a esfuerzos colaborativos dirigidos a incorporar resiliencia si ven que corren el riesgo de divulgar información que dé cuenta de sus vulnerabilidades, dado que esto puede tener un impacto en el valor de mercado de sus activos o en las inversiones en resiliencia (OECD, 2015a). Por último, es posible que se debilite la causa de la resiliencia si no se entienden bien, o se entienden de manera fragmentada, los posibles problemas y sus soluciones posibles. La precisión en la identificación y planteamiento de los problemas exige que los diversos grupos de interés tengan un conocimiento profundo del entorno.

Con base en la discusión anterior sobre el concepto de resiliencia en las infraestructuras críticas, en la siguiente sección se presentará un marco para la evaluación de políticas. Allí se describirán de manera pormenorizada los criterios claves de tal marco, entre ellos la gobernanza y los esquemas financieros que pueden informar la evaluación del nivel de resiliencia que requieren las estructuras críticas de los países. Se espera que en trabajos posteriores este marco, así como el cuestionario que aparece en al apéndice de este documento, informen tanto los estudios de caso de países individuales como los transnacionales, cuyos resultados se plasmarán en recomendaciones generales de políticas que guíen las labores de los países de aquí en adelante.

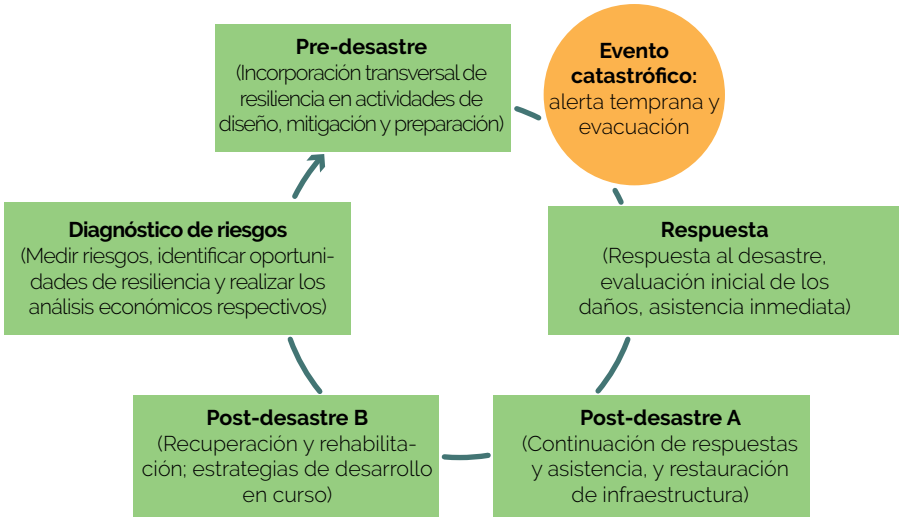
4. Cómo superar los retos y robustecer la resiliencia de la infraestructura crítica: borrador de marco de políticas

Dotar a la infraestructura crítica de resiliencia requiere adherirse a un proceso en el que sus riesgos particulares se gestionan dentro del ciclo general del manejo de riesgos frente a desastres. La mayor parte de la *planificación* de las actividades relativas a la resiliencia de tales estructuras tiene lugar durante las fases de diagnóstico y pre-desastre del ciclo de manejo de riesgos de catástrofe (figura 4.1). Pero también es importante mejorar la resiliencia a través de actividades que ocurren a lo largo de todo el ciclo de gestión de riesgos, como por ejemplo después de la evaluación de los daños, cuando la infraestructura afectada se construye otra vez, pero mejor.

Los países que estén dispuestos a emprender actividades de planificación y gestión de resiliencia en infraestructuras críticas deberían ponerse de acuerdo en las directrices de diagnóstico y evaluación, así como en los esquemas de gobernanza. Lo mismo en lo que se refiere a identificar aquellos mecanismos de financiamiento que puedan ser empleados para apoyar esfuerzos iniciales y ya en marcha de dotación de resiliencia para infraestructuras críticas. A continuación se ofrece un marco de evaluación de políticas, el cual posteriormente informará los cuestionarios de los estudios de caso de países:

- Definición de infraestructura crítica
- Diagnóstico de criticidad
- Diagnósticos de riesgos, vulnerabilidades e interdependencias

Figura 4.1. Ciclo de manejo de riegos frente a desastres



Fuente: Adaptado de OECD (2014a).

- Esquemas de gobernanza
- Instrumentos de política (p. ej., regulaciones, incentivos o mecanismos voluntarios)
- Desarrollo de estrategias nacionales para la resiliencia de infraestructuras críticas
- Financiamiento de infraestructuras críticas
- Monitoreo y evaluación
- Ejercicios prácticos y lecciones aprendidas a partir del evento

4.1 Definición de infraestructura crítica

Definir qué se entiende por infraestructuras críticas no es algo que se hace una sola vez y se revisa ocasionalmente. Por el contrario, la definición de infraestructuras críticas está sujeta a tendencias dinámicas nacionales e internacionales --entre ellas la dependencia cada vez mayor de tecnologías de información--, además de que en ella inciden la situación política y las amenazas contemporáneas. El proceso permanente de definir la infraestructura crítica depende de que se produzcan discusiones permanentes entre los diversos actores interesados (Stangl et al., 2012). En tal contexto, es importante que la definición resultante permita que las inversiones en resiliencia se enfoquen en los sectores de crucial importancia para la seguridad y estabilidad económica y social (Clancy, 2012).

Los enfoques usados para definir la infraestructura crítica varían de un país a otro (cuadro 4.1), si bien tienen temas comunes. Las funciones "críticas" son aquellas que se consideran esenciales para el bienestar económico y social en general, y para la protección y seguridad de la ciudadanía en particular. En la mayoría de las definiciones que usan los países también se reconoce la interdependencia entre esos sistemas, y se hace referencia específica a infraestructura física, sistemas de producción o redes de comunicación (Gordon y Dion, 2008). En el cuadro 4.1 se registran las definiciones de

Cuadro 4.1. definiciones de infraestructura crítica

Australia	"Aquellas instalaciones físicas, cadenas de suministro, redes de tecnologías de información y comunicación que si llegaran a quedar destruidas, degradadas o inutilizadas por un período prolongado, impactarían de manera significativa el bienestar social y económico de la nación o afectarían la capacidad de Australia de poner en marcha su defensa y garantizar la seguridad nacional".
CANADÁ	"La infraestructura crítica se refiere a aquellos procesos, sistemas, instalaciones, tecnologías, redes, activos y servicios esenciales para la salud, protección, seguridad o bienestar económico de los canadienses, y para el funcionamiento efectivo del gobierno. La infraestructura crítica puede ser autónoma o estar interconectada y ser interdependiente dentro de las provincias, territorios y fronteras nacionales o entre ellas. Las disrupciones de la infraestructura crítica podrían resultar en la pérdida catastrófica de vidas, efectos económicos adversos y daño significativo de la confianza pública".
ALEMANIA	"Las Infraestruturas críticas (IC) são estruturas organizacionais e físicas e instalações de importância tão vital para a sociedade e a economia de uma nação, que sua falha ou degradação resultaria em escassez sustentada de suprimentos, interrupção significativa de segurança e proteção pública ou outras consequências dramáticas".
NUEVA ZELANDA	"La infraestructura crítica es aquella necesaria para suministrar servicios críticos cuya interrupción tendría serios efectos adversos en Nueva Zelanda como un todo, o en una proporción significativa de la población, y que requerirían ser restablecidos de manera inmediata. En Nueva Zelanda, la infraestructura crítica ha sido identificada como aquellos activos y sistemas que se requieren para mantener en funcionamiento la gobernanza, incluyendo el imperio de la ley y el orden, y la seguridad nacional y económica; las telecomunicaciones e internet; la energía, incluyendo la generación y distribución de electricidad, y la distribución de petróleo y gas; la banca y las finanzas; el transporte, y los servicios de emergencia".
SUECIA	"Aquellos activos, sistemas o partes de los mismos localizados en los Estados miembros de la Unión Europea que sean esenciales para mantener funciones sociales, salud, protección, seguridad, bienestar económico o social de la gente, y cuya disrupción o destrucción tendría un impacto significativo en un Estados miembro como resultado de la incapacidad de mantener sus funciones".
REINO UNIDO	"Todos aquellos activos de infraestructura (física o electrónica) vitales para la integridad y suministro continuo de servicios esenciales de los cuales depende el Reino Unido, cuya pérdida o situación de riesgo tendrían consecuencias económicas o sociales graves o causarían la pérdida de vidas".
ESTADOS UNIDOS	"La infraestructura crítica representa sistemas y activos físicos o virtuales de importancia tan vital para Estados Unidos que la inutilización o destrucción de tales sistemas y activos tendría un impacto debilitante en la seguridad, seguridad económica nacional, salud pública nacional o protección, o una combinación de las anteriores".

Fuentes: (Australia) Critical Infrastructure Resilience Strategy (2010) y Critical Infrastructure Resilience Strategy: Plan (2015); (Canadá) National Strategy for Critical Infrastructure (2009) and Action Plan for Critical Infrastructure 2014-2017; (Alemania) National Strategy for Critical Infrastructure Protection (2009); (Nueva Zelanda) Presentación ante la Conferencia internacional sobre Riesgos y Desastres, Davos, 28 de agosto de 2008. Critical Infrastructure Resilience: Perspective from New Zealand. Patrick Helm, Department of the Prime Minister & Cabinet, New Zealand; (Suecia) Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure (2014); (Reino Unido) Strategic Framework y Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards (2010) y Keeping the Country Running: Natural Hazards and Infrastructure (2011); (Estados Unidos) The National Infrastructure Protection Plan 2013 Partnering for Critical Infrastructure Security and Resilience; OECD (2015b). Establishing Effective Public –Private Partnerships for Risk Management. What are the Possible Options for Government? OECD High Level Risk Forum, Diciembre de 2015.

Cuadro 4.2. Ejemplos de sectores y subsectores de infraestructura crítica

Ejemplos	Australia	Canadá	Francia	Alemania	Países Bajos	Nueva Zelanda	Suiza	Reino Unido	Estados Unidos
Energía	●	●	●	●	●	●	●	●	●
Alimentación (y agricultura)	●	●	●	●	●		●	●	●
Agua (y aguas residuales)	●	●	●	●	●	●	●	●	●
Transporte	●	●	●	●	●	●	●	●	●
Salud	●	●	●	●	●		●	●	●
Banca y finanzas	●	●	●	●	●		●	●	●
Comunicaciones	●	●				●		●	●
Gobierno		●	●	●	●		●	●	●
Manufactura e industria		●	●	●	● [1]		●		● [2]
Protección		●							
Infraestructura social						●			
Laboratorios	●								
Química	●								●
Defensa	●		●						●
Instalaciones comerciales									●
Represas					●				●
TIC	●	●	●	●	●		●	●	●
Nuclear									●
Servicios de emergencia	●	●	●	●	●		●	●	●
Aplicación y cumplimiento de la ley			●	●	●				

Notas: 1) Industrias química y nuclear 2) Manufactura crítica, reactores nucleares, materiales, residuos, industria química
Fuente: Critical Five (2014). Forging a Common Understanding for Critical Infrastructure; OCDE (2015b).

infraestructura crítica en seis países de la OCDE: Alemania, Australia, Canadá, Nueva Zelanda, el Reino Unido y Estados Unidos.

En un informe a través del cual busca acopiar elementos comunes sobre qué se entiende por infraestructura crítica, Australia, Canadá, Nueva Zelanda, el Reino Unido y Estados Unidos comparten una narrativa: *La infraestructura cr*ítica, también conocida como infraestructura de importancia nacional, *se puede definir de manera general como aquellos sistemas, activos, instalaciones y redes que proporcionan servicios esenciales para la seguridad nacional, la seguridad económica, la prosperidad, y la salud y seguridad de sus respectivas naciones* (Critical Five, 2014).

En la región de América Latina y el Caribe, un informe reciente sobre los resultados del Índice de Gobernanza y Políticas Públicas sobre Manejo de Desastres (iGOPP) realizado por el Banco Interamericano de Desarrollo reveló que, de 17 países encuestados, 14 han definido la infraestructura crítica en sus marcos jurídicos. En México, por ejemplo, la infraestructura estratégica se define como aquella que se considera indispensable para el suministro de bienes y servicios públicos y cuya destrucción o disrupción representa una amenaza para la seguridad nacional. Por su parte, Chile ha elaborado una clasificación de estructuras, lo cual incluye una categoría para edificaciones y otras estructuras (p. ej., hospitales y estaciones de bomberos) que son esenciales en el contexto de un desastre (IDB, 2015).

En términos de los sectores que proveen infraestructura física, en su nivel más básico estos comprender sistemas vitales como el agua, el saneamiento, la electricidad, el transporte y las telecomunicaciones, que son los que habilitan las funciones esperadas del entorno urbanizado, así como los sistemas de respuesta a emergencias y otras infraestructuras (NRC, 2009). En muchos países de la OCDE, los sectores vitales también abarcan las finanzas, la salud y los alimentos. Al igual que con la definición de infraestructura crítica, los sectores y subsectores precisos que esta comporta varían de un país a otro (cuadro 4.2).

4.2 Diagnóstico de criticidad

Con base en la definición de infraestructura crítica, convendría llevar a cabo diagnósticos de criticidad para identificar activos, sistemas y redes que sean verdaderamente críticos (DHS, 2013; Zaballos y Juen, 2016). Es posible que la criticidad sea vista de distintas maneras en los diferentes niveles de gobierno y entre los dueños y operadores privados. Es por ello que se hace necesario comunicar las perspectivas de criticidad a través de actividades estructuradas para compartir información durante todo el proceso de manejo de riesgos de la infraestructura crítica, y elaborar listas de aquella infraestructura que sea crítica en los varios niveles jurisdiccionales (DHS, 2013). La figura 4.2 ilustra una jerarquía de criticidad usada en el estado de Victoria, Australia.

Los diagnósticos de criticidad se fundamentan en los vínculos existentes entre riesgos e impactos. Los enfoques más comunes para diagnosticar la criticidad en el contexto de los impactos se centran en las consecuencias del evento como son la incidencia de lesiones o las pérdidas (Theoharidou et al., 2009). El impacto por lo general se evalúa a la luz de tres características principales:

I. Alcance o distribución especial: el área geográfica que podría quedar afectada por la pérdida o falta de disponibilidad de infraestructura crítica;

II. Gravedad o intensidad o magnitud: la consecuencia de la interrupción o destrucción de una infraestructura crítica particular; y

III. Efectos de tiempo o distribución temporal: el punto en el que la pérdida de un elemento podría a tener un impacto serio (inmediato, uno o dos días, una semana, etc.).

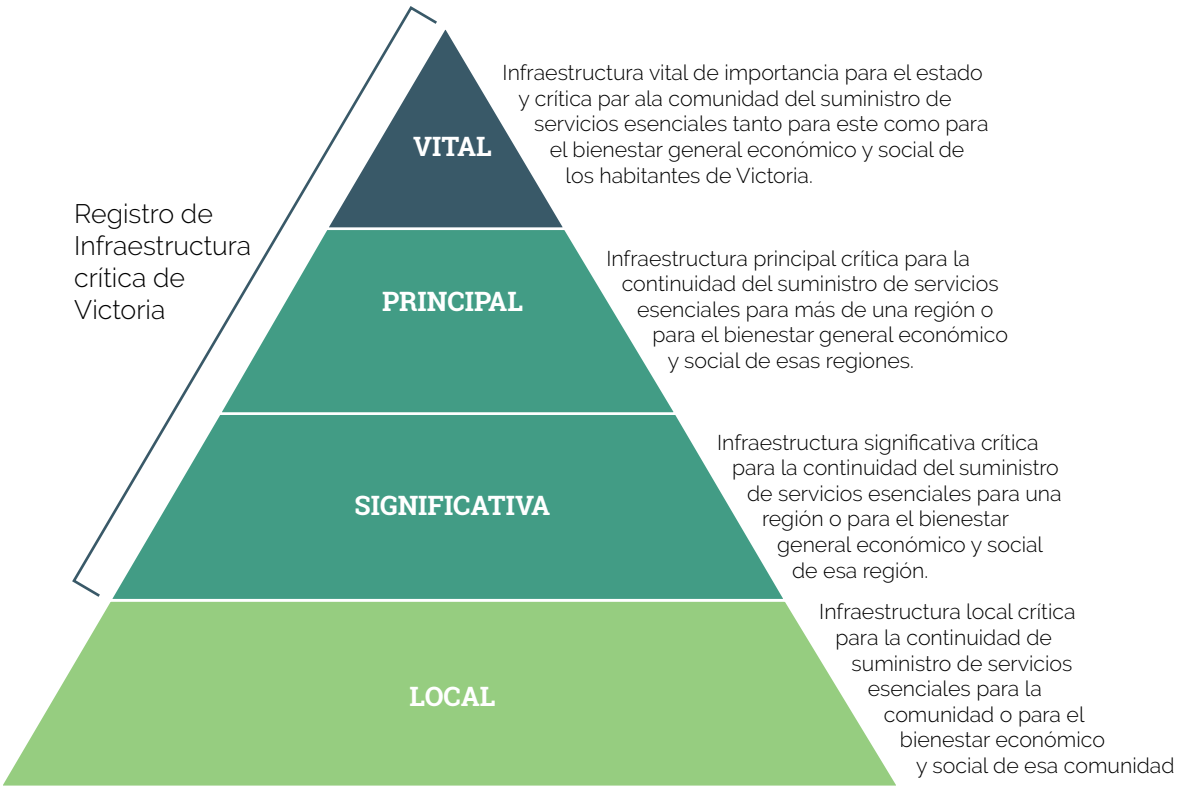
Por ejemplo, la Comisión Europea define un conjunto mínimo de criterios para el diagnóstico de infraestructura crítica, entre ellos:

I. impactos públicos, incluyendo la población afectada y la incidencia de pérdida de vidas, enfermedades médicas, lesiones serias y evacuación;

II. impactos económicos, incluyendo efectos en el PIB, pérdidas económicas, y degradación de productos y servicios;

III. impactos ambientales, incluyendo el efecto en el público y en el medio ambiente circundante;

FigurA 4.2 Ejemplo de una jerarquia del nivel de criticidad de la infraestructura: el caso de Victoria, Australia



Fuente: Victoria, Australia State Government (diciembre de 2012). A Roadmap for Victorian Critical Infrastructure Resilience.

IV. interdependencias, es decir, aquellas que existen entre los elementos de infraestructuras críticas;

V. impactos políticos, incluyendo confianza en el gobierno e

VI. impactos psicológicos, incluyendo los observados en la población (Theoharidou et al., 2009).

La Comisión evalúa los criterios anteriormente esbozados con base en su alcance (local, regional, nacional e internacional) y momento (durante el evento y después) (Theoharidou et al,. 2009).

4.3 Diagnóstico de riesgos, vulnerabilidades e interdependencias

4.3.1 Entender los riesgos y vulnerabilidades

En estos diagnósticos se identifican las vulnerabilidades y riesgos relativos que podrían afectar a las infraestructuras críticas; igualmente se evalúan el impacto y las consecuencias, así como la probabilidad de que se presente un suceso peligroso. Estos diagnósticos informan a los responsables de la toma de decisiones en los sectores público y privado sobre el nivel de protección y sobre la necesidad de hacer inversiones en resiliencia, así como sobre las medidas extraordinarias disponibles durante los tiempos de crisis (Critical Five, 2014; DHS, 2013; OECD, 2014a; Zaballos y Juen, 2016; OECD, próximo a publicarse). También sirven para identificar medidas apropiadas para que las infraestructuras críticas sean más robustas y resilientes. Entre estas figuran las medidas de endurecimiento y reconfiguración, por ejemplo a través de elevación, aislamiento hidrófugo o seco, o remoción de impedimentos físicos que restrinjan el flujo de aguas en ríos y llanuras de inundación, así como de la elevación de generadores y otros equipos auxiliares, mejor monitoreo y planes adecuados de respuesta frente a las emergencias. Además de facilitar la selección de las medidas apropiadas de resiliencia, los diagnósticos de riesgos y vulnerabilidad ayudan a integrar esos esfuerzos dentro del ciclo de vida general de la infraestructura.

Dados los diversos perfiles de riesgo de la infraestructura crítica, los diagnósticos de vulnerabilidad y riesgo deben tener en cuenta toda la gama de peligros naturales y antropogénicos –incluyendo ataques terroristas y cibernéticos--, así como los errores técnicos y humanos, y las fuerzas que los subyacen. Tales diagnósticos amplios no solo deben tomar en cuenta los escenarios de riesgo más probables, sino también aquellos que, aunque menos probables, de todas maneras puedan materializarse. Un enfoque holístico de todos los peligros puede ayudar a poner en evidencia vulnerabilidades complejas e identificar interdependencias que atraviesan sectores y riesgos (G20/OECD, 2012; OECD, próximo a publicarse). Cada vez son más los países donde se reconoce la necesidad de tomar en cuenta todo el espectro de desastres posibles (OECD, próximo a publicarse). En la Estrategia Nacional de Infraestructura Crítica de Alemania, por ejemplo, se considera toda una variedad de amenazas posibles, entre ellas peligros naturales, fallas técnicas o errores humanos (como por ejemplo fallas sistémicas, accidentes por negligencia o fallas institucionales) y terrorismo, crimen y conflicto (lo cual incluye sabotaje), otras

formas de comportamiento criminal (piratería y ataques cibernéticos), y guerra civil u otras confrontaciones (Federal Republic of Germany, 2009). En la Estrategia Nacional de Infraestructura Crítica de Canadá se insiste en la necesidad de realizar análisis que abarquen todos los riesgos, es decir, los de índole accidental, los intencionales y los naturales (Canadian Government, 2009).

El diagnóstico de riesgos se puede realizar usando una variedad de metodologías que van desde enfoques deterministas hasta métodos probabilísticos. Con los primeros se analizan e interpreta los sucesos catastróficos históricos y los datos retrospectivos disponibles a la luz de nuevos hechos como el cambio climático y los avances tecnológicos, los cuales pueden cambiar su forma y sus efectos. Estos análisis retrospectivos pueden ampliarse mediante escenarios y simulaciones de desastres. Para perfeccionar los estimativos realizados a través de análisis deterministas, es necesario expandir los diagnósticos de riesgo para infraestructura crítica con cálculos probabilísticos (G20/OECD, 2012; OECD, próximo a publicarse). A la luz de los nuevos patrones de riesgos que han surgido como resultado de los cambios socioeconómicos, la dinámica ambiental y los avances tecnológicos, es necesario llevar a cabo estos diagnósticos de riesgo y vulnerabilidad de manera regular y sus métodos deben adaptarse a lo largo del tiempo (OECD, 2014a; G20/OECD, 2012; OECD, próximo a publicarse). Por ejemplo, se debe tener en cuenta que los autores de actos humanos deliberados –ataques terroristas, por ejemplo—pueden adaptar sus métodos de acuerdo con las medidas preventivas, con lo cual se reduce la confiabilidad de los cálculos probabilísticos para escenarios deliberados (Brown y Cox, 2011). Asimismo, la disponibilidad y calidad de los datos definen

Recuadro 4.1. Metodologías de diagnóstico de riesgos para infraestructura crítica en Europa y América del Norte

- **Clúster de usuarios de redes de transporte y energía en relación con actividades antiterroristas (COUNTERACT).** COUNTERACT es parecido a una metodología organizacional de diagnóstico de riesgos, aunque con un foco relativamente más estrecho en los sectores de energía y transporte, y en las amenazas terroristas. Mediante la aplicación de un marco para el diagnóstico de riesgos de seguridad desagregados en análisis de riesgos y diagnóstico de vulnerabilidades, esta herramienta permite identificar vacíos en la prevención y mitigación de amenazas y detectar la posibilidad de optimizar las salvaguardias disponibles.

- **Enfoque integrado para la protección de infraestructura crítica.** La Estrategia Nacional de Seguridad y Protección de los Países Bajos introduce una metodología de diagnóstico de riesgos de tres pasos en el contexto de la infraestructura crítica. Partiendo del proceso de diagnóstico de riesgos nacionales, se emplean criterios de impacto económico, físico y social para determinar el grado de criticidad de la infraestructura y las disrupciones que puede sufrir. El diagnóstico de vulnerabilidad permite discernir cuáles son los principales riesgos, amenazas y vulnerabilidades, así como el grado de resiliencia de tal infraestructura. Por último, en este informe se prevé la realización de acuerdos para mantener o incrementar la resiliencia de la infraestructura allí donde se requiera.

- **Metodología para el diagnóstico de riesgos y resiliencia de infraestructuras y sistemas críticos (CRISRRAM).** CRISRRAM es una metodología desarrollada por la Comisión Europea en la cual se emplea un enfoque de todos los peligros y de "sistemas de sistema" para abordar los riesgos y vulnerabilidades de la infraestructura crítica a nivel de activos, de sistema y de la sociedad. Con el fin de abordar la complejidad del diagnóstico de riesgos, CRISRRAM emplea un enfoque de escenarios y recomienda que se evalúen todos los escenarios de un peligro y también de múltiples peligros. Para seleccionar los escenarios se debe conducir un Diagnóstico de Amenazas Posibles.

- **RAMCAP-Plus.** Esta metodología fue desarrollada por la Asociación Americana de Ingenieros Civiles desde un enfoque para el diagnóstico de todos los riesgos y resiliencias. Abarca todas las infraestructuras desde el doble objetivo de protección y resiliencia. Esta metodología consta de siete pasos: caracterización de activos; caracterización de amenazas; análisis de consecuencias; análisis de vulnerabilidades; diagnóstico de amenazas; diagnóstico de riesgos y resiliencia; y gestión de riesgos y resiliencia. Esta herramienta ha sido diseñada para ser usada tanto por los operadores de infraestructuras críticas como por los responsables de la toma de decisiones.

Fuente: Giannopoulos, Filippini y Schimmer (2012); Theocharidous y Giannopoulos (2015); OECD (2017).

Recuadro 4.2 HAZUR: Cómo funcionan las interdependencias de las infraestructuras críticas en las ciudades

Después de una sequía, aunada a problemas con la construcción de la carrilera para un tren de alta velocidad y un apagón significativo en 2007, el Concejo de la ciudad de Barcelona colaboró con el IQS, un centro de investigación universitario, para dar inicio al proyecto '3S: Seguridad del Suministro de Servicio'. Con ello se buscaba identificar los puntos débiles y los riesgos que pueden afectar a las infraestructuras críticas en el área metropolitana de Barcelona, y mejorar los planes operacionales para facilitar la continuidad de los servicios en la ciudad en caso de cualquier peligro.

A partir del proyecto 3S, un derivado del mismo auspiciado por el sector privado llamado 'OPTICITIS' mejoró el enfoque de aquel hasta convertirlo en una herramienta que podría contribuir a habilitar la resiliencia de infraestructuras críticas en otras ciudades. OPTICITIS desarrolló la metodología HAZUR y una plataforma informática en línea para hacer diagnósticos de resiliencia de las ciudades y de redes de infraestructura de repuesto, así como para proporcionar un mecanismo destinado a monitorear activamente la resiliencia de las ciudades. HAZUR da cuenta de las interdependencias e incorpora información ciudadana transmitida por operadores del sector privado y registrada a través de una red de sensores. El programa informático también se usa para mapear el estado operativo de las infraestructuras y sus interdependencias, y para identificar rápidamente las interrupciones. Este programa también se puede usar para modelar el impacto de un peligro en la red de infraestructura crítica de una ciudad.

Además de programa informático HAZUR, OPTICITS también elaboró un programa de certificación en resiliencia urbana, acompañado por una red de Expertos Certificados en Resiliencia Urbana.

Fuentes: HAZUR. Introduction to Urban Resilience with HAZUR online course. Consultado en: https://learn.canvas.net/courses/921/pages/4-dot-3-study-cases-barcelona; HAZUR Resilient Systems homepage. Consultado en: http://opticits.com/#hazur ; Ajuntament de Barcelona. http://resilient-cities.iclei.org/fileadmin/sites/resilient-cities/files/Resilient_Cities_2012/Program_Updates/Presentation/F/F3/Manuel_Valdes_response_to_crises_in_infrastructures.pdf

el riesgo, la vulnerabilidad y las capacidades para diagnosticar las interdependencias. En el recuadro 4.1 se dan ejemplos de diagnósticos de riesgo para infraestructuras críticas realizados en Europa y Estados Unidos.

En los distintos países, los diagnósticos de riesgos de infraestructuras críticas difieren en su alcance y enfoque (nivel de activos, de sistemas o de sectores), y también según la audiencia destinataria (responsables por la formulación de políticas, operadores) (European Commission, 2012; OECD, próximo a publicarse). La mayoría de los diagnósticos de riesgos se realizan a nivel del sector o del activo; los diagnósticos que atraviesan varios sectores o los de "sistemas de sistemas" se usan menos (European Commission, 2012). A la luz de los riesgos complejos surgidos de las vulnerabilidades e interdependencias entre sectores de infraestructura críticos, esto podría constituir una limitación (Giannopoulos et al., 2012).

El enfoque de diagnóstico de riesgos está íntimamente correlacionado con la audiencia destinataria. Si bien los diagnósticos de riesgos en el ámbito nacional se dirigen principalmente a los responsables por la formulación de políticas y sirven para identificar riesgos y vulnerabilidades claves, así como las medidas para contrarrestarlos, es posible que los operadores de infraestructuras críticas encuentren más pertinentes los diagnósticos de sectores específicos. Y aunque los diagnósticos de riesgos nacionales son menos definidos y se apoyan de manera predominante en evaluaciones determinísticas, proporcionan un contexto útil para los diagnósticos de riesgos de sectores particulares. Por ejemplo, en el Reino Unido los diagnósticos de riesgos nacionales anuales detallados basados en escenarios constituyen la base de los planes de resiliencia de infraestructuras sectoriales (Zaballos y Juen,

2016). Otros países como Finlandia realizan diagnósticos de riesgos y vulnerabilidades de infraestructura crítica como parte de sus diagnósticos de riesgos nacionales, y consideran tanto la cascada de efectos como las interdependencias transfronterizas y los riesgos específicos de infraestructuras críticas (European Commission, 2012; OECD, próximo a publicarse).

4.3.2 Entender las interdependencias y la cascada de impactos

La existencia de un grado de interdependencia e interconexión sin precedentes entre los sistemas de infraestructuras críticas ha aumentado la prevalencia de vulnerabilidades potenciales, y en particular la posibilidad de que se produzca una cascada de efectos (Gordon y Dion, 2008; US Department of Homeland Security, 2013). Esto último se observa cuando las disrupciones en uno o más sistemas de infraestructura originan otras disrupciones subsecuentes dentro de los sistemas y procesos relacionados con el sistema o sistemas afectados inicialmente (Gordon y Dion, 2008). Últimamente, el uso generalizado de sistemas de tecnologías de la información y las comunicaciones ha contribuido a aumentar sustancialmente la eficiencia, pero al mismo tiempo ha creado fuentes adicionales de disrupciones para las infraestructuras críticas pues los sistemas o redes que los subyacen podrían quedar en peligro (US Department of Homeland Security, 2013). Existe la necesidad de identificar de manera dinámica las interdependencias de las infraestructuras críticas para evitar que se diseñen soluciones de alcance limitado que puedan ocasionar consecuencias graves inintencionadas (NRC, 2009). La metodología Hazur que se describe en el recuadro 4.2 ofrece ejemplos prác-

Recuadro 4.3 Enfoque de diagnóstico de interdependencia en los Estados Unidos de América

- **Criticidad Accesibilidad Recuperación Vulnerabilidad Espiabilidad Redundancia (CARVER2).** CARVER2 ha sido diseñado para hacer análisis de infraestructura crítica desde la óptica de los responsables por la formulación de políticas. El enfoque de CARVER2 incluye todos los peligros y abarca tanto amenazas terroristas como desastres naturales; asimismo permite comparar y jerarquizar la infraestructura crítica dentro de los diversos sectores y de manera transversal. La infraestructura crítica se evalúa de acuerdo con seis criterios, siendo el diagnóstico de impactos el núcleo del ejercicio. Para implementar esta metodología se han creado una herramienta independiente para PC y una versión servidor/cliente (CARVER2Web).

- **Modelado de Simulación de Infraestructura Crítica (CIMS por su sigla en inglés).** Utilizado por el Laboratorio Nacional de Idaho, el enfoque CIMS fue desarrollado para que los responsables por la toma de decisiones a nivel de ciudad o de condado puedan tomar medidas y responder rápidamente a la emergencia en la fase de recuperación. CIMS permite la visualización de la interoperabilidad de la infraestructura y desarrollar modelos en tiempo real usando información de fuentes de acceso libre (p.ej. mapas simples o fotos aéreas combinadas con información con un alto grado de agregación). Dado que se enfoca en las interdependencias, el CIMS tiene un enfoque transectorial, si bien con un alto grado de abstracción; se espera que sirva como una herramienta de diagnóstico de interdependencias e impactos con un enfoque en la resiliencia social.

Fuente: Giannopoulos, Filippini y Schimmer (2012).

ticos sobre cómo identificar y mapear estas interdependencias.

Los diagnósticos sobre interdependencias ayudan a identificar los posibles vínculos y cascadas de efectos dentro de los sistemas de infraestructuras críticas y a crear conciencia sobre su existencia entre los diversos grupos de interés. Igualmente coadyuvan a desarrollar procesos y a implementar mecanismos de reemplazo o repuesto para mitigar esa posible cascada de efectos. Los diagnósticos sobre interdependencias pueden conducir a la clasificación de estructuras críticas adicionales en aquellas circunstancias donde se haga evidente la importancia primordial de una estructura específica en el contexto de una red.

Las interdependencias de la infraestructura crítica pueden adoptar las siguientes formas (Rinaldi et al. 2001; Macaulay, 2016):

- Físicamente: Dos infraestructuras son físicamente interdependientes si el estado de cada una de ellas depende del producto o productos materiales de la otra.
- Cibernéticamente: Una infraestructura tiene una interdependencia cibernética si su estado depende de información transmitida a través de la infraestructura de información.
- Geográficamente: Las infraestructuras son geográficamente interdependientes si un evento ambiental local puede producir cambios en el estado de todas ellas.
- Lógicamente: Dos infraestructuras son lógicamente interdependientes si el estado de cada una depende del estado de la otra por la vía de un mecanismo que no representan una conexión física, cibernética o geográfica.

En el recuadro 4.3 se ofrecen ejemplos de enfoques de diagnósticos contemporáneos de interdependencias de infraestructuras críticas en Estados Unidos.

Los diagnósticos de riegos, vulnerabilidades e interdependencias constituyen la base misma de las estrategias y planes de implementación efectivos de resiliencia de las infraestructuras críticas. Por su intermedio, tanto los responsables por la formulación de políticas como los operadores pueden definir eficientemente enfoques nacionales, subnacionales y transectoriales para robustecer la resiliencia de la infraestructura crítica con base en los riesgos, vulnerabilidades e interdependencias identificados. Una vez que se conocen estos factores, las partes interesadas pueden formular objetivos de resiliencia a la luz de las probabilidades de que las amenazas se materialicen, priorizando los más importantes en su contexto particular.

Los diagnósticos de riesgos, vulnerabilidades e interdependencias mediante los cuales se cuantifica la exposición potencial a los riesgos de desastres son críticos para realizar análisis costo-beneficio de inversiones particulares en resiliencia, así como para determinar si se transfiere parte de esa exposición a los mercados de aseguramiento y/o de capitales. Los enfoques de modelado de catástrofes formales tienen en cuenta peligros, vulnerabilidades (estructurales) e impacto financiero, y pueden proporcionar estimados de Pérdidas Anuales Promedio y Pérdida Máxima Probable necesarios para hacer un manejo financiero efectivo de los riesgos de desastres.

4.4 Esquemas de gobernanza

La propiedad y operación de la infraestructura crítica, así como los modelos operacionales, varían de un país a otro. En algunos de

ellos, la mayor parte de la infraestructura crítica es de propiedad de los gobiernos subnacionales o nacionales y operada por ellos, o por otras agencias y autoridades públicas responsables por los activos, sistemas y servicios que aquellas proporcionan. En otros, una porción cada vez mayor de la infraestructura crítica es de propiedad privada u operada por este sector. Las alianzas público-privadas (APP) también se han vuelto bastante frecuentes como instrumento para operar los activos de infraestructura. En Chile y México, por ejemplo, el 20% de las inversiones del sector público en infraestructura se canaliza a través de APP (Hawkesworth, 2011; OECD, 2015c).

Independientemente de los esquemas institucionales, los costos de recuperación de infraestructuras críticas afectadas por desastres naturales siguen siendo absorbidos por los gobiernos nacionales. Tales costos constituyen la mayor parte del gasto gubernamental después de una catástrofe, especialmente en ausencia de mecanismos de transmisión de riesgos como los seguros (G20/OECD, 2012). El hecho de que la propiedad, operación y responsabilidad financiera de estas infraestructuras se encuentre entrelazada, aunado al interés público, permite que los gobiernos justifiquen la lógica que subyace a exigir que quienes participan en su propiedad u operación tengan la capacidad técnica y financiera para garantizar su resiliencia.

Se necesitan esquemas institucionales efectivos para garantizar la resiliencia de los activos y operaciones de la infraestructura de un país. Un primer paso esencial consiste en identificar a las partes interesadas, para luego diseccionar sus funciones y responsabilidades en relación con la infraestructura crítica como parte del proceso de desarrollo del marco de política. Una buena manera de determinar "quién es responsable de qué y cuándo" en la resiliencia de la infraestructura crítica es consagrando tales funciones y responsabilidades en la legislación y regulación de los países, lo cual permitirá establecer una estructura de gobernanza efectiva. El examen de políticas y marcos jurídicos también servirá para identificar posibles vacíos existentes en la definición de funciones y responsabilidades. Estos pasos deberían incluir el examen de las responsabilidades a través de los diversos niveles y sectores de gobierno, así como de las funciones que desempeñan los dueños y/u operadores públicos y privados de infraestructura crítica.

Para asegurar que los actores responsables identificados incorporen medidas de resiliencia en la infraestructura crítica de su propiedad o de cuya operación están a cargo, el gobierno tiene una serie de instrumentos a mano para facilitar el proceso, entre ellos las regulaciones técnicas y económicas. Su incorporación transversal en el proceso de inversión pública también es una herramienta esencial para asegurar que la nueva infraestructura sea mejor diseñada y más resiliente. Por último, el gobierno necesita dotar a los actores de plataformas efectivas de coordinación y colaboración.

La regulación técnica expedida por los gobiernos puede incluir medidas de resiliencia que tomen en cuenta los impactos potenciales de un desastre. Por ejemplo, los reguladores de energía nuclear han estudiado la manera en que los riesgos de inundación y las temperaturas de los ríos impactan la seguridad futura de las plantas nucleares. Suiza expidió una serie de normas nuevas que toman en cuenta los posibles cambios en las temperaturas de los ríos a consecuencia del cambio climático, lo cual a su vez tiene efectos sobre los reservorios y las represas hidroeléctricas (OECD, 2016).

Los reguladores también pueden definir

Recuadro 4.4 Participación de grupos de interés en el intercambio de información sobre infraestructura crítica

Con el propósito de facilitar las relaciones eficientes y efectivas entre los diversos grupos de interés que comparten responsabilidades por la resiliencia de la infraestructura crítica, varios países han desarrollado programas y enfoques para fomentar las conexiones basadas en la confianza entre el gobierno y los dueños y operadores privados.

- **Programa de Asesores de Seguridad y Protección (PSA) del Departamento de Seguridad Nacional de Estados Unidos:** A través de este programa se favorece la participación proactiva de los aliados del gobierno y los dueños y operadores del sector privado que tienen responsabilidad sobre infraestructuras críticas. El PSA planifica, coordina y realiza encuestas y diagnósticos de seguridad y resiliencia de infraestructuras críticas de importancia nacional. A través de este programa también se llevan a cabo actividades de divulgación, y se proporciona acceso a propietarios, operadores y otros grupos de interés a recursos, capacitación e información sobre resiliencia. Durante y después de un incidente, los asesores sirven de enlace entre los funcionarios del gobierno y los dueños y operadores de infraestructuras críticas del sector privado.

- **Red Confiable de Intercambio de Información de Australia (TISN) para la Resiliencia de la Infraestructura Crítica**. La TISN ofrece un entorno seguro y no competitivo en el cual todos aquellos con intereses en las infraestructuras críticas pueden colaborar y participar en iniciativas encaminadas a desarrollar resiliencia. Esta red permite que dueños y operadores de grupos sectoriales intercambien información y cooperen regularmente dentro de los diversos sectores y a través de ellos para abordar los retos de seguridad y de continuidad de las empresas.

- **Portal de Infraestructura Crítica de Canadá.** Este portal cumple con uno de los objetivos de la Estrategia y Plan Nacional de Infraestructura Crítica de Canadá, cual es la promoción oportuna del intercambio de información y protección entre aliados vinculados a la infraestructura crítica. Se trata de un área de trabajo colaborativa virtual donde se comparte información no clasificada y en la que participan miembros de la comunidad a cargo de infraestructuras críticas.

- **Red de Alerta de Información de la Unión Europea sobre Infraestructura Crítica (CIWIN).** CIWIN es un sistema de intercambio de información desarrollado como componente de apoyo del Programa Europeo para la Protección de Infraestructura Crítica. La CIWIN facilita el intercambio de información sobre amenazas comunes, vulnerabilidades y medidas y estrategias apropiadas para mitigar los riesgos que afectan a las infraestructuras críticas entre los miembros de la Unión Europea y la Comisión Europea. Además de su función de intercambio de información, la CIWIN sirve como sistema de alerta temprana para riesgos y amenazas graves.

- **Centros de Análisis e Intercambio de Información (ISAC).** Los ISAC específicos a cada sector y pueden ser o bien una extensión del gobierno nacional (como en el caso del ISAC de Telecomunicaciones en Estados Unidos, el cual está administrado por el Sistema Nacional de Comunicaciones dentro del Departamento de Seguridad Nacional), o ser completamente manejados por la industria (como sucede con el ISAC del Agua de Estados Unidos, una extensión sin fines de lucro del gremio profesional del sector hídrico). Los ISAC son considerados fuentes de buenas prácticas de seguridad, así como de indicaciones, advertencias y evaluaciones sobre peligros y amenazas.

Fuentes: U.S. DHS, Protective Security Advisors. Consultado en: https://www.dhs.gov/protective-security-advisors; Australian Government, Trusted Information Sharing Network. Consultado en: http://www.tisn.gov.au/Pages/default.aspx; Australian Government (2015). Critical Infrastructure Resilience Strategy Policy Statement. Consultado en: http://www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPolicyStatement.PDF; Canadian Critical Infrastructure Information Gateway, Consultado en: https://cigateway.ps.gc.ca/_layouts/pscbranding/psclogon.aspx?ReturnUrl=%2f_layouts%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F; Canadian Critical Infrastructure Information Gateway Terms and Conditions of Service, Consultado en: https://cigateway.ps.gc.ca/_layouts/pscbranding/trms-eng.pdf; Critical Infrastructure Warning Information Network, Consultado en: http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm; Smedts, B. (2010). Critical Infrastructure Protection Policy in the EU: State of the Art and Evolution in the (Near) Future. Royal High Institute for Defence, Center for Security and Defence Studies Focus Paper 15. Consultado en: http://www.irsd.be/website/images/livres/focuspaper/FP15.pdf; Lewis, T.G. (2006). Critical Infrastructure Protection in Homeland Security, Defending a Networked Nation. John Wiley & Sons. Sample Consultado en: http://samples.sainsburysebooks.co.uk/9780471789536_sample_381483.pdf; U.S. Department of Homeland Security. (2013) National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience. Consultado en: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

cuáles son los resultados esperados obligatorios en materia de confiabilidad del servicio. En Finlandia, por ejemplo, los proveedores de electricidad han asegurado que las interrupciones no excederán las seis horas en las áreas densamente pobladas, o 36 horas en otras. En Francia, los operadores de infraestructuras críticas tienen que producir planes de protección y estar preparados frente a toda clase de peligros, incluyendo los naturales (OECD, 2016).

La regulación económica es otro instrumento que el gobierno puede emplear para asegurar que los proveedores de infraestructuras críticas integran medidas de resiliencia. Sin embargo, aquí entran a jugar una serie de elementos delicados en materia de competencia y precios al consumidor. Es por ello que los gobiernos deben ser lo suficientemente flexibles y permitir que los proveedores adhie-

Figura 4.2 Gobernanza de infraestructura crítica en Estados Unidos

Gobernanza de infraestructura crítica en Estados Unidos

Consejos de Coordinación Sectorial (SCC)	Consejo Transectorial de Infraestructura Crítica	Consejos Coordinadores Gubernamentales (GCC)	Consejo Federal de Alto Liderazgo (FSLC)	Consejo Coordinador Gubernamental Estatal, Local, Tribal y Territorial (SLTTGCC)	Consejo Coordinador de Consorcio Territorial (RC3)	Organizaciones para el Intercambio de Información
Consejos del sector privado	Consejo del sector privado	Consejos gubernamentales	Consejo federal	Consejo federal	Consejo de aliados	Organizaciones no gubernamentales
Dueños y operadores, y sus representantes	Presidente y vicepresidentes de los SCC	Representantes de varios niveles de gobierno	Altos funcionarios de la SSA y otros departamentos y agencias federales	Representantes de las entidades gubernamentales del SLTT	Grupos y coaliciones regionales de varias partes del país	Por ejemplo, Centros de Análisis e Intercambio de Información (ISAC)
Puntos principales de colaboración entre el gobierno y el sector privado: planificación y coordinación de políticas, y una gama de actividades sectoriales	Coordina temas, iniciativas e interdependencias transectoriales	Permite la coordinación intergubernamental, transjurisdiccional e interagencias dentro y entre sectores; se asocia con los SCC para esfuerzos público-privados	Facilita la comunicación y la coordinación en todo el gobierno federal	Promueve la participación de los socios del SLTT; sirve de estructura organizativa y de coordinación interjurisdiccional sobre las estrategias de los gobiernos estataes y locales	Coordina grupos y coaliciones que participan en varias iniciativas dirigidas a garanticar la seguridad y resiliencia de la IC	Funciones operacionales y de difusión; facilita el intercambio de información entre el gobierno y el sector privado; colabora transectorialmente por medio de un consejo nacional

Fuente: U.S. Department of Homeland Security (2013), National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience.

Figura 4.3 Gobernanza de la infraestructura crítica en Australia

Gobernanza de la infraestructura crítica en Australia			
Red Confiable de Intercambio de Información (TISN)	Grupos sectoriales	Grupos Asesores Expertos	Comunidades de Intereses (CoI)
Foro de cooperación	Foro de cooperación	Grupos asesores	Foro de cooperación
Dueños y operadores de IC: siete grupos sectoriales de IC y dos de asesores expertos	Actores gubernamentales y dueños y operadores individuales de IC	Expertos	Actores gubernamentales y dueños y operadores individuales de IC
Cooperación y coordinación entre dueños y operadores de IC; intercambio de información sobre amenazas y vulnerabilidades; desarrollo de estrategias y soluciones conjuntas; promoción de CIC (incluyendo la necesidad de invertir en infraestructuras confiables y resilientes	Puente entre el gobierno y los dueños individuales; ayuda a dueños y operadores compartiendo con ellos información sobre temas relacionados con amenazas y vulnerabilidades genéricas; identifica medidas apropiadas para mitigar riesgos	Ofrece asesoría sobre aspectos generales de la IC que requieran conocimiento experto (sobre asuntos relativos a la TISN o por fuera de ella)	Consulta transectorial entre actores gubernamentales y dueños y operadores de IC sobre cuestiones específicas; se convoca cuando un tema específico de IC exige atención, y se puede desintegrar una vez el asunto haya dido abordado satisfactoriamente.

Fuente: Australian Government (2010), Critical Infrastructure Resilience Strategy

ran a las regulaciones económicas en cumplimiento de otros requisitos regulatorios (OECD, 2016). La posibilidad de adoptar esquemas de distribución de costos para las inversiones en la resiliencia de infraestructuras críticas también hace parte de la tarea de establecer sistemas efectivos de gobernanza.

La incorporación transversal de la resiliencia en los procesos de inversión pública también es esencial. La manera más efectiva de minimizar las pérdidas económicas futuras a causa de los desastres es hacer que las infraestructuras nuevas ya sean resilientes. En Perú, por ejemplo, todas las inversiones públicas se someten a una evaluación en la que se establece el posible impacto de los desastres naturales, y con base en ello se identifican las medidas apropiadas de reducción de riegos para integrarlas a su diseño (Lavell et al., 2016).

Los gobiernos no necesariamente poseen la capacidad técnica de definir y monitorear objetivos de resiliencia complejos, y por lo tanto deben acudir a relaciones colaborativas con las fuentes de experticia disponibles en el sector privado para llevar a cabo estas tareas. La existencia de esquemas de gobernanza que faciliten estos intercambios regulares, el intercambio de información y el fomento de la confianza mutua son elementos necesarios para asegurar la integración efectiva de medidas de resiliencia en la planificación de infraestructura, tal y como se especifica en el recuadro 4.4. Los

actores gubernamentales pueden facilitar el desarrollo de soluciones técnicas (p. ej., portales de intercambio de información y colaboración) que se constituyan en entornos confiables y seguros para que los diversos grupos interesados de los sectores público y privado intercambien ideas, información y experiencias relevantes para la resiliencia de la infraestructura crítica regularmente (Bach et al., 2013; Lewis, 2006).

Los programas recíprocos de educación y toma de conciencia sobre infraestructura crítica diseñados para mejorar el conocimiento en todo el espectro de grupos de interés de los sectores público y privado pueden servir de base para una mejor preparación y, por extensión, resiliencia (Lewis, 2006). Dueños y operadores deben conocer bien los recursos, requerimientos y planes de la infraestructura crítica. Por su parte, los responsables por la formulación de políticas deben acumular suficientes conocimientos para desarrollar políticas sólidas que fomente la seguridad y la resiliencia, aunque sin imponer cargas excesivas a sus dueños y operadores, y sin agregar –sin proponérselo-- otras vulnerabilidades (Lewis, 2006). En el recuadro 4.4 se encuentran varios ejemplos de enfoques exitosos de participación conjunta de grupos de interés y de esquemas seguros para compartir información sobre infraestructuras críticas.

Los gobiernos nacionales generalmente convocan comisiones transjurisdiccionales y transectoriales cuyo mandato consiste en coordinar la totalidad de la infraestructura crítica del país. Las comisiones que se forman a nivel nacional para iniciar el desarrollo de un marco para la planificación y el manejo de la resiliencia de la infraestructura crítica pueden seguir operando más allá de los esfuerzos iniciales y actuar como junta asesora permanente, cuya tarea es ofrecer ideas en tiempo real sobre cambios en el panorama de la in-

Recuadro 4.5 Estrategias de protección de la infraestructura crítica nacional

- En la **Estrategia Nacional Canadiense para la Infraestructura Crítica** se establece la ruta para mejorar la resiliencia de la infraestructura crítica de Canadá frente a nuevas amenazas. Para tal fin se adopta un enfoque colaborativo a través del cual se asegura que las actividades de los gobiernos federal, provincial y territorial se complementen, y además respeten las leyes de cada jurisdicción. Allí se esbozan los mecanismos para lograr un mejor intercambio de información y su protección. Asimismo se indica que la resiliencia de la infraestructura crítica se puede lograr con una combinación apropiada de medidas de seguridad para incidentes intencionales y accidentales a través de prácticas empresariales de continuidad para afrontar disrupciones, así como planificando la gestión de emergencia para garantizar que se cuenta con los procedimientos correspondientes para abordar alteraciones imprevistas y desastres naturales. En el ámbito nacional, le estrategia clasifica la infraestructura crítica en 10 sectores: energía y servicios públicos, finanzas, alimentos, transporte, gobierno, tecnología de la comunicación y la información, salud, protección, agua y manufactura.

- En la **Estrategia Básica de Suiza para la Protección de la Infraestructura Crítica** se esbozan las metas estratégicas y los principios claves para la protección de la infraestructura crítica en Suiza. Esta abarca la definición de enfoques amplios de protección; la identificación y compilación de elementos y objetos de la infraestructura crítica en un inventario clasificado; el establecimiento de plataformas público-privadas transectoriales; y el intercambio de información sobre riesgos --diagnóstico y sistemas de alerta especialmente— entre los varios grupos de interés. En la estrategia también se aborda el apoyo federal requerido para afrontar los problemas con la infraestructura crítica en caso de que sus recursos no den abasto. En la estrategia se considera 10 sectores críticos: gobierno, energía, manejo de residuos, finanzas, servicios de salud, industrias, información y comunicación, alimentos, seguridad pública y transporte.

Fuentes: Canadian Government, 2009; Federal Office for Civil Protection, 2012.

fraestructura crítica del país a nivel nacional. De otro modo, estas comisiones podrían ser nombradas por un tiempo definido que concluya con la presentación de sus hallazgos. En Estados Unidos, por ejemplo, en 1996 el Presidente expidió una orden ejecutiva a través de la cual se creó la Comisión Presidencial para la Protección de Infraestructura Crítica (PCCIP por su sigla en inglés), la cual marcó el inicio de un enfoque estratégico de la infraestructura crítica como determinante clave de la seguridad nacional (PCCIP, 1997).

La composición de una estructura de gobernanza efectiva variará necesariamente de un país a otro y estará influenciada principalmente por el balance que exista entre las funciones y responsabilidades públicas y privadas en torno a ella. Independientemente de lo anterior, gobernar su resiliencia requiere que exista un enfoque transparente y colaborativo que incorpore a una variedad de grupos de interés, como por ejemplo el gobierno nacional, distintos sectores y niveles de la administración pública, y expertos técnicos. En las figuras 4.2 y 4.3 se registran las estructuras de gobernanza de Estados Unidos y Australia respectivamente.

4.5 Estrategias y planes nacionales de resiliencia para infraestructuras críticas

Cada vez son más los países y regiones que han reconocido la necesidad de proteger su infraestructura crítica de manera conjunta y coordinada por intermedio de planes o estrategias nacionales (Wiseman y McLaughlin, 2014; OECD, 2017). La elaboración de una estrategia de resiliencia para la infraestructura crítica en el ámbito nacional reconoce implícitamente que la resiliencia no se puede lograr plenamente a nivel del operador o del activo debido a que existen responsabilidades compartidas por la infraestructura crítica, y también interdependencias (Giannopoulos et al., 2012).

Las estrategias de protección de la infraestructura crítica normalmente se in-

Figura 4 5. Relación entre la estrategia cir y el plan de implementación cir: el caso de australia

Fuente: Australian Government. (2015b). Critical Infrastructure Resilience Strategy.

troducen con una definición de lo que se entiende por infraestructura crítica, acompañada de criterios nacionales con los que se evalúa la criticidad de la infraestructura, y finalmente con una lista de los sectores e infraestructuras que se consideran críticos en el contexto específico del país. La Estrategia Suiza para la Protección Básica de infraestructura Crítica, por ejemplo, considera que existen 10 sectores críticos y clasifica la criticidad de 28 subsectores como alta, muy alta y regular, entendiendo por criticidad la importancia relativa de los subsectores para los ciudadanos y la economía (Federal Office for Civil Protection, 2012).

Las estrategias nacionales para la infraestructura crítica proporcionan un marco de políticas común que permite que exista un enfoque colaborativo para fortalecer su resiliencia. Así sucede en los países que cuentan con estrategias de protección y resiliencia. Por ejemplo, la Estrategia Nacional de Canadá para la Infraestructura Crítica identifica explícitamente el papel de las alianzas entre el gobierno federal, los gobiernos provinciales/territoriales y los operadores como condición para lograr la resiliencia de la infraestructura crítica (Canadian Government, 2009). La estrategia canadiense identifica la resiliencia y los objetivos de seguridad de la infraestructura crítica bajo tres áreas principales que incluyen: (i) construir alianzas transgubernamentales y transectoriales; (ii) implementar un enfoque de manejo de riesgos que abarque todos los peligros y se apoye en esfuerzos colaborativos público-privados; y (iii) compartir y proteger la información de los distintos grupos de interés (Canadian Government, 2009). La Estrategia Nacional Alemana para la Protección de Infraestructura Crítica (estrategia CIP) también indica específicamente la necesidad de contar con directrices estratégicas para promover acciones conjuntas exitosas entre quienes participan en su gestión. Para garantizar la seguridad de la infraestructura crítica, la CIP sirve de base para el desarrollo de sub-metas que se implementan bajo planes y programas adicionales (Federal Republic of Germany, 2009), entre ellos el plan de implementación de la estrategia nacional de resiliencia de infraestructura crítica, los planes sectoriales específicos y también planes transectoriales.

Las estrategias para la infraestructura crítica deberían constituir la base de la coordinación y comunicación continuas. Allí se deberán identificar además los diversos grupos de interés con sus respectivas funciones y responsabilidades. Estos elementos son comunes a numerosas estrategias de nivel nacional. Por ejemplo, el Programa Nacional de Protección de la Infraestructura Crítica de Polonia se enfoca en forjar alianzas entre los diversos grupos de interés y el Foro Nacional para la Protección de la Infraestructura, el cual reúne a representantes de la infraestructura critica de propiedad pública y privada, para coordinar la resiliencia de la misma en ese país (OECD, 2017).

Entre los países que cuentan con protección para su infraestructura física, así como en algunos de los marcos de resiliencia más recientes, el enfoque de dos partes, a saber, definición de una *estrategia de resiliencia* y un *plan de implementación* vinculado pero separado, no es único utilizado. En algunos países, el plan de implementación está relacionado con una estrategia de seguridad nacional más amplia y representa un enfoque híbrido estratégico-operacional, tal y como sucede en el Reino Unido y en Estados Unidos.

En el Reino Unido, la resiliencia de la infraestructura crítica se guía a nivel estratégico por la Estrategia de Seguridad Nacional, en la cual se explicita que una de las tareas principales es "mejorar la resiliencia

de aquella infraestructura que se considere esencial para mantener al país funcionando ante un ataque, daño o destrucción" (United Kingdom, 2011), así como por el Diagnóstico Nacional de Riesgos, el cual sirve como marco para la planificación de implementación basada en riesgos (United Kingdom, 2016). El gobierno publicó el documento *Keeping the Country Running: Natural Hazards and Infrastructure* (KCR), el cual contiene directrices para la implementación del programa de resiliencia de la infraestructura crítica en el Reino Unido. El KCR cuenta con un enfoque relativamente híbrido en el cual se detallan ambas estrategias y se ofrecen guías prácticas específicas para mejorar la resiliencia en los sectores de infraestructura crítica (United Kingdom, 2011).

La implementación de las actividades de resiliencia relacionadas con la infraestructura crítica se define mejor a través del perfeccionamiento regular de los Planes de Resiliencia Sectoriales (United Kingdom, 2016). Cuando se pone en marcha, el plan de implementación de la Estrategia de Resiliencia de la Infraestructura Crítica operacionaliza tal estrategia detallando acciones específicas con su respectiva línea de tiempo. Por ejemplo, Nueva Zelanda emplea las directrices estratégicas descritas pormenorizadamente en su *The Thirty Year New Zealand Infrastructure Plan 2015* y las implementa a través de un Apéndice al Plan de Acción, así como de su *Ten-Year Capital Intentions Plan* (New Zealand, 2015). En la figura 4.5 se ilustra la relación entre la Estrategia de Resiliencia de Infraestructura Crítica (CIR) y el Plan de Implementación de la CIR en Australia (Australian Government, 2015b).

Es posible que los planes de implementación requieran el desarrollo de planes sectoriales específicos, y también planes transectoriales y transgubernamentales. En los planes de implementación se deberán establecer metas específicas de incorporación de resiliencia en la infraestructura crítica para los distintos grupos de interés que sean medibles, alcanzables y realistas. Por ejemplo, el KCR del Reino Unido incluye una lista de control de resiliencia para dueños y operadores de infraestructura crítica, así como una serie de guías sobre intercambio de información y sobre la identificación de dependencias e interdependencias. Partiendo del KCR, los Planes de Resiliencia Sectoriales del Reino Unido incorporan estándares de desempeño sectoriales y también estándares nacionales e internacionales más amplios (United Kingdom, 2016). En ese país, los sectores críticos aplican los estándares específicos (técnicos) de la British Standards Institution (BSI) y de ISO. Lo mismo en lo que se refiere a estándares de riesgo, seguridad y manejo de crisis, gobernanza corporativa, y estándares de resiliencia organizacional (United Kingdom, 2016). Un plan nacional de implementación de la estrategia de resiliencia de infraestructura crítica también puede servir como línea de referencia para que los grupos de interés desarrollen programas pertinentes continuos de monitoreo y medición. De esta manera, los planes de implementación sirven como un vínculo tangible entre la estrategia nacional que toma en cuenta el diagnóstico de riesgos, vulnerabilidades e interdependencias, y los programas continuos de monitoreo y sus resultados.

4.6 Financiamiento de la infraestructura crítica

Como se indicó anteriormente, en muchos países de la OCDE la propiedad o la operación de los sistemas de infraestructura crítica a menudo se ejerce a través de esquemas mixtos en

Recuadro 4.6 Herramienta de transferencia de riesgos para manejar la exposición del sector público

Son varias las herramientas de transferencia de riegos que se pueden desarrollar para manejar la exposición de las finanzas públicas a la reconstrucción post-desastre de activos públicos:

• **Aseguramiento de activos públicos:** Los propietarios individuales pueden comprar una cobertura de seguros específica para aquellos activos públicos de los cuales son responsables (individualmente o como parte de una cartera). El costo del seguro puede reducirse eligiendo deducibles altos para las pólizas adquiridas (p. ej., para que cubra uno o más extremos climáticos), o incluyendo un conjunto diverso de activos en una sola póliza. Los países pueden aprovechar las ventajas en materia de precios centralizando la compra de pólizas en un solo departamento (o incluso por medio de un vehículo de aseguramiento público). Por ejemplo, Costa Rica está creando un vehículo de aseguramiento de activos públicos a través de un asegurador público, al tiempo que transfiere solo las pérdidas excesivas a los mercados financieros internacionales. Son varios los países que también operan aseguradoras públicas, bien a nivel nacional o subnacional, con el fin de suministrar aseguramiento para los activos públicos (p. ej., Australia, Filipinas, Indonesia). En Colombia, la agencia de adquisiciones públicas está creando una póliza de seguros grupal a la cual tienen acceso los departamentos para asegurar sus activos.

• **Aseguramiento del gasto público:** Otro enfoque consiste en efectuar una transacción de transferencia de riesgos cuyos pagos se hagan dependiendo de si sucede o no una catástrofe, con lo cual se tiene una fuente de recursos destinada a financiar los gastos de reconstrucción. En muchos casos, estas transacciones se estructuran para que los pagos se efectúen con base en la magnitud específica del desastre (p. ej., un terremoto de una magnitud específica, o una tormenta o inundación de un cierto nivel), lo cual tiene el beneficio adicional de que el pago se hace más rápidamente (si bien existe el riesgo de que no corresponda a los niveles reales de pérdidas). Los enfoques de transferencias de riesgos se pueden estructurar a través de iniciativas en que se combinan recursos (caso del Servicio Caribeño de Seguros de Riesgos de Catástrofe) --cuyos beneficios se generan por la vía de un conjunto de riegos más variado— a través de un esquema de reaseguramiento basado en un detonante paramétrico, o a través de la emisión de bonos de catástrofes (que básicamente son bonos que no pagan si ocurre un desastre específico, lo cual permite que se transfieran fondos del tenedor al emisor cuando este último es afectado por una catástrofe).

Los países deberán evaluar cuál es la mejor manera de asegurar suficiente financiamiento para cubrir aquellos riesgos que retienen, es decir, los que no se transfieren a través de esquemas de aseguramiento u otros mecanismos. Los servicios de crédito contingente que ofrecen los bancos multilaterales de desarrollo pueden ofrecer una fuente inmediata de recursos para reestablecer servicios interrumpidos por un desastre. Por ejemplo, el BID tiene uno de esos servicios por un monto total de US$1.486 millones que cubre a la República Dominicana, Perú, Ecuador, Nicaragua, Honduras y Panamá. Otras instituciones multilaterales como el Banco Mundial y el Banco de Desarrollo de América Latina (CAF), y también las agencias bilaterales de cooperación como la Agencia Internacional de Cooperación de Japón (JICA por sus siglas en inglés), cuentan con mecanismos similares.

Fuente: G20/OCDE, 2012; OCDE, 2015a

los que participan los sectores público y privado. Por ejemplo, es posible que las redes del ferrocarril sean de propiedad pública, mientras que el servicio de trenes está a cargo de intereses privados. Por otra parte, la producción de energía puede estar en manos privadas, pero su precio puede estar sumamente regulado por el Estado. Desde la perspectiva del interés público, las grandes inversiones para incorporar resiliencia en los sistemas de infraestructura crítica, o las inversiones públicas en general, deberían conllevar una negociación abierta y estructurada sobre quién carga con qué porción de los costos de los desastres, tanto *ex ante* en el proceso de inversión, construcción y mantenimiento de las medidas preventivas, como *ex post* en lo que tiene que ver con los costos de reconstrucción y rehabilitación. Más aún, el cumplimiento y la implementación de los estándares y objetivos acordados debería ser objetivamente monitoreado y verificado. El reto consiste en definir esquemas deseables de gobernanza para estos procesos de pre- y post-inversión, esenciales para proteger el interés público.

Los planes de inversión e implementación para la infraestructura crítica, así como las inversiones públicas en general, deberían incluir estrategias de financiamiento en que se especifique, por ejemplo, quién es responsable de una cierta porción de los costos relacionados con los desastres, tanto en términos de inversiones *ex ante* en medidas de resiliencia, como en lo que se refiere a financiar la recuperación. Dado que las restricciones fiscales en el sector público son cada vez más frecuentes, los gobiernos deben considerar la posibilidad de estimular la incorporación transversal de resiliencia en las infraestructuras críticas. Países como Perú y Costa Rica ya están dando pasos para asegurar que se incorporen aspectos de resiliencia en las inversiones públicas. En Perú, los análisis de riesgos y su reducción son elementos comunes del ciclo de proyecto de las inversiones públicas. Entre tanto en Costa Rica, todas las inversiones tienen que estar alineadas con el plan nacional de desarrollo, el cual, entre otras cosas, requiere que se tomen en cuenta el cambio climático y los riesgos frente a desastres (Zapata, 2016; Martínez, 2016).

Es posible que los gobiernos tengan diversas herramientas para fomentar la incorporación de resiliencia en las infraestructuras críticas. En términos de financiación *ex ante*, podrían optar por subsidiar la construcción de infraestructura protectora y otras medidas de resiliencia --endurecimiento y reconfiguración, por ejemplo-- para aquella infraestructura crítica del nivel subnacional o para la que se encuentra en manos privadas. O podrían cubrir la totalidad de los costos de las medidas protectoras destinadas a la infraestructura crítica estatal o para aquella clasificada como vital o principal, independientemente de su estructura de propiedad. En algunos países como Austria, existe un fondo de reserva de destinación específica que sirve tanto para financiar la recuperación y las labores de auxilio posteriores a un desastre, como las inversiones *ex ante* en medidas de prevención y mitigación (OECD. 2016).

Otra posibilidad es que los gobiernos nacionales opten por financiar actividades que eleven la conciencia de los operadores y dueños (nacionales, subnacionales y privados) de infraestructuras críticas sobre los riesgos, vulnerabilidades y medidas de resiliencia. Estos recursos se pueden destinar al diagnóstico de riesgos de tales infraestructuras, o a determinar sus relaciones de dependencia e interdependencia, o a capacitaciones y ejercicios específicos destinados a fortalecer capacidades técnicas. Si se combinan con otras medidas, estas herramientas de diagnóstico

pueden conducir a facilitar una mayor resiliencia de la infraestructura crítica. Por ejemplo, los gobiernos pueden establecer requisitos legales para que se demuestre que se han hecho las inversiones necesarias *ex ante* en medidas de reducción de impactos de desastres, tomando en cuenta los riegos identificados durante la fase de diagnóstico. Otro enfoque relacionado puede ser el de "premiar" a aquellos dueños/operadores que hayan implementado las medidas de resiliencia necesarias con un financiamiento de apoyo más generoso para la recuperación posterior el desastre. Este enfoque crea un sistema de incentivos positivos, aunque puede tener sus desventajas, en la medida en que puede conducir a que haya diferentes niveles de resiliencia en estas infraestructuras críticas.

- Dada la posible exposición de los gobiernos nacionales a los costos relacionados con la reconstrucción de infraestructura averiada como consecuencia de un desastre, es posible que los gobiernos nacionales deseen concebir estrategias de financiamiento o de distribución de costos para recuperarlos:

- Para aquellos activos de infraestructura crítica que son de propiedad del Estado, los gobiernos nacionales deberían determinar la manera más eficiente de financiar la reconstrucción en función de los costos. En tal sentido, deberán decidir si, ante esta exposición, les conviene más el auto-aseguramiento o la transferencia de riesgos. Por ejemplo, México ha emprendido un ejercicio de modelado de exposición pública el cual, además de infraestructura crítica, abarca los riesgos frente

Recuadro 4.7 Mecanismos innovadores de financiación de resiliencia de infraestructura crítica

A partir de las fallas de infraestructura crítica que se registraron a raíz de la súper tormenta Sandy, el gobierno de Nueva Jersey puso en marcha un mecanismo de financiamiento para fomentar el desarrollo de infraestructura crítica resiliente. El Banco de Resiliencia Energética (ERB por sus sigla en inglés) de Nueva Jersey --el primero en su género en Estados Unidos-- fue creado con US$200 millones de recursos federales provenientes de la Community Development Block Grant-Disaster Recovery para apoyar el desarrollo de recursos distribuidos de energía en instalaciones críticas en todo el estado, de modo que puedan seguir operando durante apagones futuros.

> "ERB proporciona préstamos y donaciones para satisfacer las necesidades de financiamiento. Las donaciones y los préstamos condonables se ofrecerán para cubrir hasta el 40% de necesidades de recursos, mientras que los préstamos baratos amortizables se otorgarán para el 60% restante. Es posible que unas y otros requieran contribución de capital. Cualquier componente de condonación del principal exigirá que se presente evidencia de que se cumple con los requisitos mínimos de desempeño, tal y como se indica en la guía del programa."

Las tecnologías elegibles deben tener capacidad de aislamiento (es decir, de operar independientemente de la red eléctrica), de "arrancar a oscuras" o blackstart (es decir, sin conexión directa con la red eléctrica), y de operar "a carga crítica". El programa incluye una escala descendente de fondos de contrapartida con base en las características de los solicitantes (con o sin fines de lucro) y en una evaluación de las necesidades del proyecto, su factibilidad y las utilidades de la inversión.

Fuentes: New Jersey Board of Public Utilities. NJ Energy Resilience Bank. News Release, 20 de octubre de 2014.

a desastres. A partir de ello ha comenzado a transferir las capas más superficiales de esa exposición (es decir, las relacionadas con sucesos más graves pero menos frecuentes) a los mercados de reaseguramiento y de capitales. Centralizar la adquisición de seguros para aquella infraestructura crítica que es propiedad del Estado (p. ej., a través de un solo vehículo de aseguramiento o póliza de "grupo") podría reportar ventajas, pues cuando se asegura un grupo de activos más diversos se suelen conseguir mejores primas. En Colombia, por ejemplo, el Ministerio de Finanzas exige de los activos de propiedad del Estado estén debidamente asegurados.

- Para los activos de infraestructura subnacionales de propiedad pública, los gobiernos nacionales deberían procurar que las administraciones subnacionales gestionen correctamente su exposición a los riesgos frente a desastres. Se necesitan esquemas de distribución de costos de reconstrucción entre los niveles nacional y subnacional para garantizar que tales riesgos se manejan de manera correcta. En estos esquemas se podrían tener en cuenta los esfuerzos realizados por los gobiernos subnacionales por asegurar su propia resiliencia. En El Salvador, Honduras, Bolivia, Colombia, Costa Rica, Nicaragua, Panamá y Perú se han establecido mandatos legales a través de los cuales se exige el aseguramiento de infraestructuras subnacionales de propiedad pública. Es posible que los gobiernos nacionales quieran monitorear o fijar requisitos de resiliencia financiera, como por

Cuadro 4.4 Criterios de desempeño de la resiliencia

Criterios	Expectativa
Eficiencia	Este criterio requiere que un sistema de infraestructura desempeñe sus funciones de manera tal que cumpla con requisitos funcionales específicos (eficiencia técnica) al menor costo posible (efectividad en función de los costos). Entre las métricas de eficiencia figuran los costos de construir y mantener un sistema complejo de infraestructura dentro de las limitaciones de su desempeño técnico, confiabilidad y continuidad del servicio.
Sustentabilidade	Este criterio evalúa el grado en que el sistema usa recursos –naturales, humanos, fabricados—de manera sostenible. Por sostenibilidad se entiende un patrón de uso de recursos que "satisfice las necesidades de hoy, al tiempo que protege los recursos para su uso futuro". Para que sean sostenibles, las infraestructuras críticas deben ser diseñadas y operadas dentro del contexto de sus impactos en los ecosistemas circunvecinos ahora y en el futuro. Entre las métricas que se usan para evaluar la sostenibilidad de una infraestructura figuran el grado en el que los insumos de construcción y operación se usan de acuerdo con los estándares económicos y ambientales de largo plazo desarrollados para ese sistema.
Capacidade de sobrevivência	Este criterio de resiliencia es la prueba de fuego de la protección, seguridad y supervivencia de la gente, activos de infraestructura y el ecosistema. De acuerdo con este criterio, una infraestructura satisface los estándares de resiliencia si tiene la capacidad de soportar los daños con impactos adversos mínimos – pérdida de vidas, impactos ecológicos, daños estructural—en la gente, las operaciones, la economía y el medio ambiente.

ejemplo demostrar suficiente capacidad de autoaseguramiento, o evaluar posibles opciones de transferencia de riesgos para tales exposiciones. Al igual que los gobiernos nacionales, los gobiernos subnacionales también podrían centralizar la compra de pólizas de seguros para sus activos con el fin de aprovechar ventajas en materia de precios en los mercados de transferencia de riesgos. En Australia, por ejemplo, el Tesoro requiere que los gobiernos subnacionales presenten informes regulares sobre sus esquemas de aseguramiento y pueden reducir la tasa de repartición de costos para efectos de reconstrucción en aquellos estados donde se considera que los esquemas de aseguramiento son insuficientes.

- Cuando se trate de activos de infraestructura de propiedad privada, el gobierno nacional podría imponer requisitos de resiliencia financiera como por ejemplo niveles suficientes de aseguramiento, o niveles equivalentes de capacidad de autoaseguramiento demostrada. Esto con el fin de asegurar un manejo correcto de la exposición financiera por parte de los operadores privados y así reducir los impactos adversos en la eventualidad de un desastre. En la región de América Latina y el Caribe, por ejemplo, solo México y Chile han establecido estándares de aseguramiento para los servicios públicos operados por propietarios privados.

Los mecanismos privados de transferencia de riegos como los seguros también pueden contribuir a cambiar la cultura de riesgo actual. Si los aseguradores logran alinear las primas con los riesgos reales y sus pérdidas asociadas, los dueños/operadores de infraestructura contarán con un incentivo que los lleve a reducir la probabilidad –y por ende las consecuencias-- del riesgo asegurado, en un esfuerzo por disminuir las primas (Flynn, 2015). El papel del sector público en este esquema consiste en evaluar las acciones de reducción de riesgos emprendidas por los dueños/operadores. Esto requerirá que se realice investigación y desarrollo acerca de nuevos estándares de mitigación, y que se identifiquen medios de bajo costo para lograr su cumplimiento (Flynn, 2015). Es importante que aquellos países que han tendido a suministrar niveles elevados de financiación para cubrir los costos de reparaciones y reemplazos después de un desastre replanteen su proceder (Flynn, 2015). Esto por cuanto si en gobierno proporciona financiación sustancial después del evento catastrófico que cubra la mayor parte de las pérdidas, los dueños/operadores privados no solo descontarán los riesgos actuales, sino que además percibirán al Estado como un asegurador de hecho que además no cobra prima (Flynn, 2015). Un enfoque alternativo sería exigir que los dueños/operadores mantengan un nivel determinado de cobertura.

La aplicabilidad de mecanismos de financiamiento específicos variará necesariamente según el contexto de cada país, y se definirá fundamentalmente por el balance que exista entre los sectores público y privado en términos de sus funciones y responsabilidades con respecto a la infraestructura crítica.

4.7 Monitoreo y evaluación

Una vez que se han definido las metodologías de evaluación y se han comenzado las actividades de gestión de riesgos y de fo-

mento de resiliencia –como por ejemplo la implementación de medidas de robustecimiento o redundancia--, se iniciará la recolección de datos para establecer una línea de referencia que permita hacer comparaciones (NRC, 2009; OECD, 2014a). Por ejemplo, en un contexto post desastre, la resiliencia se puede evaluar o bien mediante la cuantificación de la funcionalidad del sistema con posterioridad al hecho, o determinando la cantidad de tiempo requerida para lograr los niveles de desempeño previos al mismo (Tierney y Bruneau, 2007). Asimismo, la identificación y seguimiento de la métrica dota a los actores interesados de los medios necesarios para cuantificar tanto la manera en que sus actividades e inversiones definen su desempeño, como el modo en que sus acciones se relacionan con su perfil de riesgo.

La autoridad que supervisa los diagnósticos independientes y el monitoreo de la resiliencia de la infraestructura crítica varía de un país a otro y dependerá de la distribución de su propiedad y operación entre los sectores público y privado. En muchos países de la OCDE, las operaciones de seguridad del sector privado están regidas por marcos jurídicos y regulatorios. Entre tanto, en Estados Unidos el mecanismo principal de acción colectiva para mejorar la resiliencia de la infraestructura crítica ha sido –y seguramente seguirá siendo— la colaboración voluntaria entre actores de los sectores público y privado (U.S. Department of Homeland Security, 2013).

Aunque Cutter (2015) aborda la medición de la resiliencia y sus herramientas correspondientes en un contexto específicamente comunitario, las directrices que allí presenta aplican también a la medición de la resiliencia de la infraestructura crítica en general:

- Dado que los sistemas de infraestructura crítica no son idénticos, y que sus interdependencias varían de un sector a otro y entre los contextos nacional, subnacional y regional, medir su resiliencia requiere una caja de herramientas que comprenda una variedad de indicadores.
- Las comunidades necesitan conceptos simples y técnicamente viables que se puedan implementar en el ámbito comunitario. Será necesario entonces ajustar y modificar las herramientas para que respondan a las necesidades de las comunidades, y promoverlas de manera tal que la resiliencia tenga sentido desde el punto de vista económico.
- Las herramientas de medición de resiliencia deben tener la capacidad de determinar y priorizar necesidades y metas; sopesar los costos (inversiones) y los beneficios (resultados); y evaluar los efectos de las diferentes políticas y enfoques (Cutter, 2014).

Según Barami (2013), los sistemas de infraestructura que incorporan resiliencia muy probablemente cumplen con los tres criterios de alto desempeño que se registran en el recuadro 4.4, y que pueden servir de base para su evaluación y monitoreo.

El monitoreo permanente de la resiliencia de las infraestructuras críticas requerirá que se hagan inversiones en sistemas de captura de datos. Estos deberán registrar información transectorial que sirva para determinar hasta qué punto se están reduciendo los riesgos de que se produzca una cascada de impactos, al tiempo que contribuyen a que los diversos actores entiendan mejor las dependencias e interdependencias cambiantes de tales infraestructuras. De la misma manera, los sistemas de monitoreo deben incorporar la capacidad de proporcionar actualizaciones de datos en tiempo casi real. Los enfoques

mixtos que comportan tecnologías de teledetección, georreferenciación y sistemas de alimentación de datos instantáneos necesitan financiamiento para desarrollar la arquitectura del sistema, la activación de equipos en el terreno, el mantenimiento de bancos de datos relacionales y la capacitación necesaria en el uso de tales aplicaciones.

4.8 El uso de ejercicios y de las enseñanzas posteriores a los eventos

Dotar de resiliencia a la infraestructura crítica es un proceso permanente y dinámico. Para asegurar su sostenibilidad y relevancia, es necesario contar con mecanismos que permitan capturar e internalizar las enseñanzas derivadas de experiencias tangibles como ejercicios, capacitaciones, e incluso incidentes de la vida real. Los ejercicios y capacitaciones --enfocados en la coordinación y comunicación de los diversos actores interesados, en las interdependencias de las infraestructuras críticas y en la comprensión de las cascadas de impactos que estas pueden generar--, así como el intercambio de información, ayudan a que se comprendan mejor las estrategias, planes y programas relacionados con la infraestructura crítica, al tiempo que crea oportunidades para realizar acciones conducentes a la adaptabilidad del elemento humano a la efectividad operacional de la infraestructura crítica. Estos ejercicios y capacitaciones también mejoran la coordinación existente entre toda la variedad de actores que fomentan la resiliencia de la infraestructura crítica. Finalmente, es importante que los programas de resiliencia sean en sí mismos adaptables a un panorama cambiante. Los ejercicios proporcionan un "espacio seguro" para poner a prueba los supuestos y acciones que se incorporan en los planes de infraestructura crítica, y sus resultados sirven para identificar las debilidades y los vacíos existentes en su planificación y gestión.

Las lecciones que surgen de los ejercicios, capacitaciones e incidentes de la vida real son esenciales para mejorar los programas de resiliencia. Hasta qué punto esta información se pueda emplear de manera constructiva dependerá del desarrollo y perfeccionamiento regular de mecanismos diseñados para recolectar y analizar las lecciones aprendidas. Para ello, el sector público puede liderar el desarrollo e implementación de procesos y sistemas que muestren cómo se recolectan y analizan las lecciones aprendidas, y cómo ese análisis se traduce en la identificación de acciones correctivas y ajustes a la estrategia nacional de resiliencia de infraestructuras críticas, así como a su plan de implementación y a otras iniciativas relacionadas. En la estrategia CIP de Alemania se indica que las enseñanzas deberían surgir de análisis de amenazas que se actualizan de manera continua, así como de otros análisis de incidentes nacionales y domésticos. Igualmente se señala que tales lecciones deben ser posteriormente incorporadas a los estándares de las infraestructuras críticas que los diversos actores desarrollan de manera colaborativa (Federal Republic of Germany, 2009). En el Plan de Acción de Suecia para la Protección de Funciones Sociales Vitales e Infraestructura Crítica se hace eco de la importancia de traducir las enseñanzas en mejoras concretas: "*en caso de disrupciones serias, es necesario incluir en el trabajo las perspectivas existentes antes durante y después, de manera que la sociedad sea capaz de resistir, manejar, recuperarse, aprender y avanzar a partir de tales disrupciones*" (Swedish Civil Contingencies Agency, 2014).

Referencias

Acton, J. M. y Hibbs, M. (2012). Why Fukushima Was Preventable Carnegie Paper Carnegie Endowment for International Peace. Consultado en: http://carnegieendowment.org/2012/03/05/why-fukushima-was-preventable-pub-47361

Australian Government (2015b). Critical Infrastructure Resilience Strategy Policy Statement. Consultado en: http://www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPolicyStatement.PDF

Australian Government, Trusted Information Sharing Network. Consultado en: http://www.tisn.gov.au/Pages/default.aspx

Australian Government. (2010). Critical Infrastructure Resilience Strategy. Consultado en: http://ccpic.mai.gov.ro/docs/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf

Australian Government. (2015a). Critical Infrastructure Resilience Strategy: Plan. Consultado en: http://www.aph.gov.au/DocumentStore.ashx?id=a58ed84e-67fe-42e2-8394-f9344db6d52d&subId=407872

Bach, C., Bouchon, S., Fekete, A., Birkmann, J., y Serre, D. (2013). Adding value to critical infrastructure research and disaster risk management: the resilience concept. SAPI EN. S. Surveys and Perspectives Integrating Environment and Society (6.1). Consultado en: https://sapiens.revues.org/1626

Barami, B. (2013). Resumen preparado para Beyond Bouncing Back: A Roundtable on Critical Transportation Infrastructure Resilience realizada en el Volpe Center el 30 de abril de 2013. Extractado de un informe técnico titulado A Risk-Based Infrastructure Resiliency Framework. John A. Volpe National Transportation Systems Center, U.S. Department of Transportation, 55 Broadway, Cambridge, MA, 02142. Consultado en: https://www.volpe.dot.gov/sites/volpe.dot.gov/files/docs/Infrastructure%20Resiliency_A%20Risk-Based%20Framework.pdf

Brown, G. y Cox, L. (2011). How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysts. *Risk Analysis,* Vol. 31, No. 2, 2011. Consultado en: https://doi.org/10.1111/j.1539-6924.2010.01492.x

Cambridge Centre for Risk Studies, Cambridge Risk Atlas Part I: Overview and Results World Cities Risk 2015-2025, septiembre de 2015. Consultado en: cambridgeriskframework.com/getdocument/24

Canadian Critical Infrastructure Information Gateway Terms and Conditions of Service, Consultado en: https://cigateway.ps.gc.ca/_layouts/pscbranding/trms-eng.pdf

Canadian Critical Infrastructure Information Gateway, Consultado en: https://cigateway.ps.gc.ca/_layouts/pscbranding/psclogon.aspx?ReturnUrl=%2f_layouts%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F

Canadian Government. (2009). Canadian National Strategy for Critical Infrastructure. Consultado en: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx

Canadian Government. (2014). Action Plan for Critical Infrastructure 2014-2017. Consultado en: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-eng.pdf

Centre of European Policy Studies (CEPS). (2010). Protecting Critical Infrastructure in the EU. CEPS Task Force Report, Bernhard Hammerli (Chair) and Andrea Renda (Rapporteur). Consultado en: https://www.ceps.eu/system/files/book/2010/12/Critical%20Infrastructure%20Protection%20Final%20A4.pdf

Chapin, E., Daniels, A., Elias, R., Aspilcueta, D. y Doocy, S. (2009). Impact of the 2007 Ica earthquake on health facilities and health service provision in southern Peru. Prehospital and disaster medicine, 24(04), 326-332. Consultado en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.176.3202&rep=rep1&type=pdf

Chang, S.; McDaniels, T.; Fox, J.; Dhariwal, R.; Longstaff, H. (2013). "Toward Disaster-Resilient Cities: Characterizing Resilience of Infrastructure Systems with Expert Judgments". *Risk Analysis*. Vol. 34/3, Wiley. Retrieved from: http://onlinelibrary.wiley.com/doi/10.1111/risa.12133/full

Clancy, M. (2012). First: Define Critical Infrastructure. SC Magazine, For IT Professionals. Consultado en: http://www.scmagazine.com/first-define-critical-infrastructure/article/250410/

Comerio, M. (2013). Housing Recovery in Chile: A Qualitative Mid-program Review. PEER Report 2013/01. Pacific Earthquake Engineering Research Center. Consultado en: http://peer.berkeley.edu/publications/peer_reports/reports_2013/web-PEER-2013-01-Comerio.pdf

Critical Five (2014). Forging a Common Understanding for Critical Infrastructure. Consultado en: https://www.dhs.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf

Critical Infrastructure Warning Information Network, Consultado en: http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm

Cutter, S. (2015). Developing a Framework for Measuring Community Resilience. From: Committee on Measures of Community Resilience: From Lessons Learned to Lessons Applied; Resilient America Roundtable; Policy and Global Affairs; National Research Council. Washington (DC): National Academies Press (US); 2015 Mar 26. Consultado en: http://www.ncbi.nlm.nih.gov/books/NBK285736/

Cutter, S. (2014). The Landscape of Resilience Measures. Presentación ante Resilient America Roundtable Workshop on Measures of Community Resilience. Febrero. Consultado en: http://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_152239.pdf

Davies, R. (2016). Floodlist: Brazil Floods and Landslides – 1 Dead, 3 Missing in Recife After 235 mm of Rain in 12 Hours Consultado en: http://floodlist.com/america/brazil-landslide-recife-pernambuco-may-2016

Dilley, M., Chen, R.S., Deichmann, U., Lerner-Lam, A. L. y Arnold, M. (2005). Natural Disaster Hotspots: A Global Risk Analysis. Washington, DC: World Bank. Consultado en: https://openknowledge.worldbank.org/handle/10986/7376

Economic Commission for Latin America and the Caribbean (ECLAC) (2015). The economics of climate change in Latin America and the Caribbean Paradoxes and challenges of sustainable development. Consultado en: http://repositorio.cepal.org/bitstream/handle/11362/37311/S1420655_en.pdf

Emergency Response Coordination Centre (ERCC), European Commission, Humanitarian Aid and Civil Protection. (2015). ECHO Daily Map 27/3/2015 Chile – Floods. Consultado en: http://erccportal.jrc.ec.europa.eu/getdailymap/docId/1109

European Commission. (2006). Communication from the Commission on a European Programme for Critical Infrastructure Protection COM (2006) 786 final. Consultado en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

European Commission. (2012). Commission Staff Working Document: On the Review of the European Programme for Critical Infrastructure Protection (EPCIP). Consultado en: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011887%202012%20INIT

European Commission. (2015). Resilience of Critical Infrastructure Protection: Guidelines. Consultado en: http://www.recipe2015.eu/UserDocsImages/pdf/GUIDELINES_final_042006.pdf

European Commission. (2016). Principles of Resilience for Critical Infrastructures: Compendium of Presentations. Consultado en: http://www.recipe2015.eu/UserDocsImages/pdf/Conference%20Presentations.pdf

European External Action Service. About EU Humanitarian Response in Haiti. Consultado en: https://eeas.europa.eu/delegations/haiti/documents/page_content/keys_facts_and_figures_about_eu_humanitarian_response_in_haiti_en.pdf

Federal Emergency Management Agency (FEMA) (2013). Hurricane Sandy FEMA After-Action. Consultado en: https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf

Federal Emergency Management Agency (FEMA). (2004). Risk Management Series, Design Guide for Improving School Safety in Earthquakes, Floods, and High Winds. Consultado en: https://www.fema.gov/pdf/plan/prevent/rms/424/fema424_cvr-toc.pdf

Federal Office for Civil Protection (2012). Nationale Strategie zum Schutz kritischer Infrastrukturen. Consultado en: https://www.admin.ch/opc/de/federal-gazette/2012/7715.pdf

Federal Republic of Germany, Federal Ministry of the Interior. (2009). National Strategy for Critical Infrastructure Protection (CIP Strategy). Consultado en: http://www.bbk.bund.de/SharedDocs/Downloads/BBK/EN/CIP-Strategy.pdf?__blob=publicationFile

FEMA (2013). Hurricane Sandy FEMA After-Action. Retrieved from: https://www.fema.gov/media-library-data/20130726-1923-25045-7442/sandy_fema_aar.pdf

Fermandois, A. (2011). "Chile and its earthquake: Preparedness, response and lessons", Government of Chile, Ambassador's Office. Consultado en: http://dels.nas.edu/resources/static-assets/materials-based-onreports/presentations/AmbassadorFermandois.pdf

Flynn, S. E. (2008). America the Resilient: Defying Terrorism and Mitigating Natural Disasters. Foreign Affairs. Tampa, FL: Council on Foreign Relations. Consultado en: https://hazdoc.colorado.edu/handle/10590/3003

Flynn, S.E. (2015). Bolstering Critical Infrastructure Resilience After Superstorm Sandy: Lessons for New York and the Nation. Consultado en: http://www.northeastern.edu/resilience/wp-content/uploads/2015/04/Bolstering-Critical-Infrastructure-Resilience-After-Superstorm-Sandy.pdf

G20/OECD (2012). Methodological Framework for Risk Assessment and Risk Financing. Consultado en: http://www.oecd.org/gov/risk/G20disasterriskmanagement.pdf

García, C. (2010). AP/NBC News Article: 20,000 Miles of Highway Hit by Colombia Floods. Consultado en: http://www.nbcnews.com/id/40606798/ns/weather/t/miles-highway-hit-colombia-floods/#.V972P_5THIU

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 (JRC), Institute for the Protection and Security of the Citizen. Consultado en: http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf

Gordon, K. y Dion, M. (2008). Protection of Critical Infrastructure and the role of investment policies relating to national security. OECD Publishing.

Hawkesworth, I. (2011), From Lessons to Principles for the use of Public-Private Partnerships, Public Governance and Territorial Development, Public Management Committee, 32nd Annual Meeting of the Working Party of Senior Budget Officials, junio, Luxemburgo. Consultado en: http://www.oecd.org/gov/budgeting/48144872.pdf

HAZUR. Introduction to Urban Resilience with HAZUR online course. Consultado en: https://learn.canvas.net/courses/921/pages/4-dot-3-study-cases-barcelona; HAZUR Resilient Systems homepage. Consultado en: http://opticits.com/#hazur

Helm, P. (2008). Presentación ante International Disaster and Risk Conference, Davos, 28 de agosto de 2008. Critical Infrastructure Resilience: Perspective from New Zealand. Consultado en: https://idrc.info/fileadmin/user_upload/idrc/former_conferences/idrc2008/presentations2008/Helm_Patrick_Owen_Critical_Infrastructure_Protection_A_Perspective_from_New_Zealand.pdf

IMF (2016). World Economic and Financial Surveys, Regional Economic Outlook, Western Hemisphere Managing Transitions and Risks Consultado en: http://www.imf.org/external/pubs/ft/reo/2016/whd/eng/pdf/wreo0416.pdf

Inter-American Development Bank (IDB). (2015). Index of Governance and Public Policy in Disaster Risk Management. Technical Note N IDB-TN-720. Consultado en: https://publications.iadb.org/bitstream/handle/11319/6717/iGOPP_Index_Governance_Public_Policy_Disaster_Risk_Management.PDF

Kreft, S., Eckstein, D., Junghans, L., Kerestan, C. y Hagen, U. (2015). Global Climate Risk Index 2015. Who Suffers Most from Extreme Weather Events? Weather-related Loss Events in 2013 and 1994 to 2013. Documento Informativo. Consultado en: https://germanwatch.org/en/download/10333.pdf

Kunreuther, H., Michel-Kerjan, E., y Porter, B. (2003). Assessing, managing, and financing extreme events: Dealing with terrorism (No. w10179). National Bureau of Economic Research.

Lavell, A., Standon-Geddes, Z., Zapata-Rondón, N. y Kraft, K. (2016). Disaster and Climate-Risk Sensitive Planning for Public Investment Decisions: Learning from two public-sector experiences of Lao PDR and Peru. Understanding Risk Conference Contribution 2016. Consultado en: https://understandrisk.org/wp-content/uploads/Disaster-and-Climate-Risk-Sensitive-Planning-for-Public-Investment-Decisions.pdf (6 de febrero de 2017).

Lewis, T.G. (2006). Critical Infrastructure Protection in Homeland Security, Defending a Networked Nation. John Wiley & Sons. Sample Consultado en: http://samples.sainsburysebooks.co.uk/9780471789536_sample_381483.pdf

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., Flynn, S.E. y Seager, T. P. (2013). Measurable resilience for actionable policy. *Environmental science & technology*, 47(18), 10108-10110.

Macaulay, T. (2016). Critical *Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies*, CRC Press, Boca Raton

Martinez, F. (2016). *Diálogo Regional de Política: Gestión del Riesgo de Desastres y la Inversión Pública: Costa Rica*. Consultado en: http://idbdocs.iadb.org/WSDocs/getDocument.aspx?DOCNUM=40723154

Masoero, A. (2016). Floodlist: Argentina and Uruguay – Floods Displace Thousands After 4 Days of Heavy Rain April 8, 2016. Consultado en: http://floodlist.com/america/argentina-uruguay-floods-april-2016

McGee, S., Frittman, J., Ahn, S. y Murray, S. (2014). Risk Relationships and Cascading Effects in Critical Infrastructures: Implications for the Hyogo Framework. Prepared for the Global Assessment Report on Disaster Risk Reduction 2015, United Nations Office for Disaster Risk Reduction. Consultado en: http://www.preventionweb.net/english/hyogo/gar/2015/en/bgdocs/McGee%20et%20al.,%202014.pdf

Minkel, J. R. (2008). The 2003 Northeast Blackout--Five Years Later. *Scientific American*, 13. Consultado en: http://www.scientificamerican.com/article/2003-blackout-five-years-later/

Moteff, J. (2012). Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress. U.S. Congressional Research Service Report No. R42683. Consultado en: https://www.fas.org/sgp/crs/homesec/R42683.pdf

Muir-Wood, R (2011). Designing Optimal Risk Mitigation and Risk Transfer Mechanisms to Improve the Management of Earthquake Risk in Chile, OECD Working Papers on Finance, Insurance and Private Pensions, No. 12, OECD Publishing. http://www.oecd.org/daf/fin/insurance/48794964.pdf

NACS (2013). 2013 NACS Retail Fuels Report. Consultado en: http://www.nacsonline.com/YourBusiness/FuelsReports/GasPrices_2013/Pages/How-Hurricane-Sandy-Affected-the-Fuels-Industry.aspx

National Research Council (NRC). (2009). Sustainable critical infrastructure systems: a framework for meeting 21st century imperatives. Toward sustainable critical infrastructure systems: framing the challenges workshop committee. National Research Council, Washington, DC.

New Jersey Board of Public Utilities. NJ Energy Resilience Bank Now Accepting Applications. News Release, October 20, 2014. Consultado en: http://www.state.nj.us/bpu/newsroom/announcements/pdf/20141020_erb_press.pdf

New Zealand. (2015). The Thirty Year New Zealand Infrastructure Plan 2015. Consultado en: http://www.infrastructure.govt.nz/plan/2015

OECD (2011). Future Global Shocks Improving Risk Governance, OECD Reviews of Risk Management Policies. Consultado en: http://www.keepeek.com/Digital-Asset-Management/oecd/governance/future-global-shocks_9789264114586-en#.V99lj_5THIU#page4

OECD (2015a). Disaster Risk Financing. A Global Survey of Practices and Challenges. OECD Publishing.

OECD (2015b). Establishing effective Public Private Partnerships for risk management. What are the possible options for government? Discussion Note. High Level Risk Forum. Consultado en: https://one.oecd.org/document/GOV/PGC/HLRF(2015)5/en/pdf

OECD (2015c). Towards a Framework for the Governance of Infrastructure. Consultado en: https://www.oecd.org/gov/budgeting/Towards-a-Framework-for-the-Governance-of-Infrastructure.pdf

OECD (2016). Boosting Resilience through Innovative Risk Governance: The Case of Alpine Areas in Austria. OECD Publishing.

OECD (2017). Toolkit for Risk Governance. Consultado en: https://www.oecd.org/governance/toolkit-on-risk-governance/goodpractices/#?hf=10&b=0&sl=trig&s=-desc(document_lastmodifieddate)

OECD (próximo a publicarse). Implementing the Recommendation on the Governance of Critical Risk: Overview of country progress, OECD Publishing, Paris.

OECD (próximo a publicarse). National Risk Assessments: A Cross Country Perspective. OECD Publishing.

OECD (próximo a publicarse). OECD Recommendation on Disaster Risk Financing Strategies. http://www.oecd.org/finance/insurance/public-consultation-drf.htm

OECD. (2014a). Boosting Resilience through Innovative Risk Governance. OECD Publishing.

OECD. (2014b). Recommendation of the Council on the Governance of Critical Risks. Consultado en: http://www.oecd.org/gov/risk/recommendation-on-governance-of-critical-risks.htm

Office of the United Nations Recovery Coordinator (UNORC). (2007). United Nations Office of the Resident Coordinator: Situation Report No. 21: Earthquake in Peru, 1–6; September 28, 2007. Consultado en: http://reliefweb.int/sites/reliefweb.int/files/resources/FA4CEB19FF-916D9C852573670072 54F9-Full_Report.pdf

Pelling, M., Basher, R., Birkmann, J., Cutter, S., Desai, B., Fakhruddin, S.H.M., Ferrugini, F., Mitchell, T., Oliver-Smith, T., Rees, J. y Kuniyoshi, T. (2014). Issue Brief: Disaster Risk Reduction and Sustainable Development. Prepared by the Integrated Research on Disaster Risk (IRDR) Programme for the Seventh Session of the UN General Assembly Open Working Group on Sustainable Development Goals. Consultado en: sustainabledevelopment.un.org/getWSDoc.php?id=2133

President's Commission on Critical Infrastructure Protection (PCCIP). (1997). Critical Foundations: Protecting America's Infrastructure. Consultado en: https://www.fas.org/sgp/library/pccip.pdf

Public Safety and Emergency Preparedness Canada. (2006). Incident Analysis: Ontario–U.S. Power Outage—Impacts on Critical Infrastructure, Number: IA06-002. Consultado en: http://cip.management.dal.ca/publications/Ontario%20-%20US%20Power%20Outage%20-%20Impacts%20on%20Critical%20Infrastructure.pdf

Rinaldi, S. M., Peerenboom, J. P. y Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, 21(6), 11-25. Consultado en: http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf

Smedts, B. (2010). Critical Infrastructure Protection Policy in the EU: State of the Art and Evolution in the (Near) Future. Royal High Institute for Defence, Center for Security and Defence Studies Focus Paper 15. Consultado en: http://www.irsd.be/website/images/livres/focuspaper/FP15.pdf

Standard & Poor's Ratings Services. (2015). The Heat is On: How Climate Change Can Impact Sovereign Ratings, Ratings Direct, 25 November.

Stanford University, Civil and Environmental Engineering. Performance Based Engineering. Consultado en: https://cee.stanford.edu/programs/structural-engineering-geomechanics/research/performance-based-engineering

Stangl, R., Siedschlag, A., Silvestru, D., Fritz, F. y Jerković, A. (2012). Comprehensive Security Research to Contribute to Critical Infrastructure Protection: Contributions to Security Governance in Disaster Risk Reduction. 12th Congress INTERPRAEVENT 2012 – Grenoble / France Conference Proceedings. Consultado en: http://www.interpraevent.at/palm-cms/upload_files/Publikationen/Tagungsbeitraege/2012_1_585.pdf

Swedish Civil Contingencies Agency (MSB). (2014). Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure. Julio. Consultado en: https://www.msb.se/RibData/Filer/pdf/27412.pdf

Taucer, F., Alarcon, J. y So, A. (2009). 2007 August 15 magnitude 7.9 earthquake near the coast of Central Peru: analysis and field mission report. *Bull Earthquake Eng* (2009) 7: 1. Consultado en: http://link.springer.com/article/10.1007%2Fs10518-008-9092-3

The Guardian (2017). Chile battles devastating wildfires: 'We have never seen anything on this scale'. Retrieved from: https://www.theguardian.com/world/2017/jan/25/chile-fire-firefighting-international-help

The Economist (2011). Colombia's floods: That damned Niña. Retrieved from: http://www.economist.com/node/21541419

Theocharidou, M. y Giannopoulos, G. (2015). Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. European Commission, Joint Research Centre (JRC), Institute for the Protection and Security of the Citizen. Consultado en: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf

Theoharidou, M., Kotzanikolaou, P. y Gritzalis, D. (2009). Risk-based criticality analysis. En International Conference on Critical Infrastructure Protection (pp. 35-49). Springer Berlin Heidelberg.

Tierney, K., y Bruneau, M. (2007) Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction. Transportation Research Board, TR News 250, May - June 2007. Consultado en: http://onlinepubs.trb.org/onlinepubs/trnews/trnews250_p14-17.pdf

U.S. Department of Homeland Security. (2013) National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience. Consultado en: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

U.S. Department of Homeland Security. (2014). Forging a Common Understanding for Critical Infrastructure, Shared Narrative. Consultado en: https://www.dhs.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf

U.S. Department of Homeland Security. Protective Security Advisors. Consultado en: https://www.dhs.gov/protective-security-advisors

U.S.-Canada Power System Outage Task Force. (2004). Final Report on the August 4, 2003 Blackout in the United States and Canada: Causes and Recommendations. Consultado en: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

United Kingdom, Cabinet Office. (2010). Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards. Consultado en: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic-framework.pdf

United Kingdom, Cabinet Office. (2011). Keeping the Country Running: Natural Hazards and Infrastructure – A Guide to improving the resilience of critical infrastructure and essential services. Consultado en: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61342/natural-hazards-infrastructure.pdf

United Kingdom, Cabinet Office. (2016). Summary of the 2015-16 Sector Resilience Plans. Abril. Consultado en: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/526351/2015_16_summary_of_the_srp.pdf

United Nations (UN). (2015). Sendai Framework for Disaster Risk Reduction 2015-2030, United Nations. http://www.preventionweb.net/files/43291_sendaiframeworkfordrren.pdf

United Nations Office for Disaster Risk Reduction (UNISDR). (2008). Links between disaster risk reduction, development and climate change. Consultado en: https://www.unisdr.org/we/inform/publications/8383

USGS (2007). USGS Earthquake Hazards Program. Poster of the Ica, Peru Earthquake of 15 August 2007 - Magnitude 8.0. Consultado en: http://earthquake.usgs.gov/earthquakes/eqarchives/poster/2007/20070815.php

USGS (2016). USGS Earthquake Hazards Program. Poster of the Coastal Ecuador Earthquake of 16 April 2016 - Magnitude 7.8. Consultado en: https://earthquake.usgs.gov/earthquakes/eqarchives/poster/2016/20160416.php

Victoria, Australia State Government. (2012). A Roadmap for Victorian Critical Infrastructure Resilience. Diciembre. Consultado en: http://pandora.nla.gov.au/pan/143319/20131029-1113/A_Roadmap_for_Victorian_Critical_Infrastructure_Resilience.pdf

Wiseman, E. y McLaughlin, T. (March, 2014). Critical Infrastructure Protection and Resilience Literature Survey: State of the Art. Department of National Defence of Canada Contract Report DRDC-RDDC-2015-C160. Consultado en: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc200/p801837_A1b.pdf

World Bank, Water and Sanitation Program. (2011). Economic Impact of the 2007 Earthquake in Peru on the Drinking Water and Sanitation Sector: Full Study. Consultado en: https://www.wsp.org/sites/wsp.org/files/publications/WSP-LAC-Economic-Impact-Earthquake-Full-Study.pdf

World Bank. (2012). Disaster Risk Management in Latin America and the Caribbean Region: GFDRR Country Notes. Consultado en: http://www.gfdrr.org/sites/gfdrr.org/files/DRM_LAC_CountryPrograms.pdf

World Economic Forum (WEF) and Boston Consulting Group (BCG). (2013). Strategic Infrastructure Steps to Prepare and Accelerate Public-Private Partnerships. Consultado en: http://www3.weforum.org/docs/AF13/WEF_AF13_Strategic_Infrastructure_Initiative.pdf

Zaballos, A. G. y Jeun, I. (2016). Best Practices for Critical Information Infrastructure Protection (CIIP): Experiences from Latin America and the Caribbean and Selected Countries. IDB and the Korea Internet and Security Agency (KISA). Consultado en: https://publications.iadb.org/handle/11319/7848

Zapata, N, (2016). Caso peruano: la gestión de riesgos en contexto de cambio climático en la inversión pública. Consultado en: http://idbdocs.iadb.org/WSDocs/getDocument.aspx?DOCNUM=40723173

Theoharidou, M., Kotzanikolaou, P., e D. Gritzalis (2009). *Risk-based criticality analysis. In International Conference on Critical Infrastructure Protection* (pp. 35-49). [Análise de criticidade baseada no risco. Em Conferência Internacional sobre Proteção de Infraestruturas Críticas]. Springer Berlin Heidelberg.

Tierney, K., and Bruneau, M. (2007) *Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction.* [Conceitualização e Medição de Resiliência: Uma Chave para a Redução doss Prejuízo de Desastres]. Conselho de Pesquisa sobre Transporte, TR News 250, maio-junho de 2007. Disponível em:

Universidade de Stanford, Engenharia Civil e Ambiental. *Performance Based Engineering*. [Engenharia Baseada em Desempenho]. Disponível em: https://cee.stanford.edu/programs/structural-engineering-geomechanics/research/performance-based-engineering USGS (2007). *USGS Earthquake Hazards Program. Poster of the Ica, Peru Earthquake of 15 August 2007 - Magnitude 8.0.* [Programa de Riscos Sísmicos da USGS. Cartaz do Terremoto de Ica, Peru, de 15 agosto de 2007 - Magnitude 8.0]. Disponível em: http://earthquake.usgs.gov/earthquakes/eqarchives/poster/2007/20070815.php

USGS (2016). *USGS Earthquake Hazards Program*. [Programa de Riscos Sísmicos da USGS. Cartaz do Terremoto na Costa do Equador de 16 de abril de 2016 - Magnitude 7,8]. Disponível em: https://earthquake.usgs.gov/earthquakes/eqarchives/poster/2016/20160416.php

Victoria, Governo da Austrália. (Dezembro de 2012). *A Roadmap for Victorian Critical Infrastructure Resilience*. [Roteiro para a Resiliência de Infraestruturas Críticas de Victoria]. Disponível em: http://pandora.nla.gov.au/pan/143319/20131029-1113/A_Roadmap_for_Victorian_Critical_Infrastructure_Resilience.pdf

Wiseman, E. e McLaughlin, T. (March, 2014). *Critical Infrastructure Protection and Resilience Literature Survey: State of the Art. Department of National Defence of Canada Contract Report DRDC-RDDC-2015-C160.* [Pesquisa de Literatura sobre Proteção e Resiliência de Infraestruturas Críticas: Estado da Arte. Departamento de Defesa Nacional do Canadá, Relatório de Contrato RDDC-RDDC-2015-C160]. Disponível em: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc200/p801837_A1b.pdf

Zaballos, A. G. e Jeun, I. (2016). *Best Practices for Critical Information Infrastructure Protection (CIIP): Experiences from Latin America and the Caribbean and Selected Countries.* [Melhores Práticas para a Proteção de Informações sobre Infraestruturas Críticas (CIIP): Experiências da América Latina e do Caribe e de Países Selecionados]. BID e Agência de Internet e Segurança da Coreia (KISA). Disponível em: https://publications.iadb.org/handle/11319/7848

Zapata, N, (2016). *Caso peruano la gestión de riesgos en contexto de cambio climático en la inversión pública* [Caso peruano de gestão de riscos no contexto da mudança climática no investimento público no Peru]. Disponível em: http://idbdocs.iadb.org/WSDocs/getDocument.aspx?DOCNUM=40723173

www.iadb.org