www.piarc.org
2015R01ES

SEGURIDAD DE LA INFRAESTRUCTURA CARRETERA

TF2-Grupo de Trabajo sobre Seguridad

WORLD ROAD ASSOCIATION
MONDIALE DE LA ROUTE
AIPCR PIARC

SOBRE LA ASOCIACIÓN MUNDIAL DE LA CARRETERA

La Asociación Mundial de la Carretera es una asociación sin fines lucrativos fundada en 1909 para favorecer la cooperación internacional y el progreso en el sector de la carretera y el transporte por carretera.

Este informe es el resultado de un proyecto especial realizado por la Asociación Mundial de la Carretera una vez que el asunto fue identificado como prioritario por el Comité Ejecutivo de la Asociación.

Este informe está disponible en la página web de la Asociación Mundial de la Carretera.

http://www.piarc.org

Asociación Mundial de la Carretera (AIPCR/PIARC)
Tour Pascal B, 19e étage
92055 La Défense cedex, FRANCE
Número Internacional Normalizado para Libros (ISBN) 978-2-84060-364-1

Portada © Jurewicz, Fotolia

SEGURIDAD DE LA INFRAESTRUCTURA CARRETERA

Asociación mundial de la Carretera

AUTORES Y AGRADECIMIENTOS

Este documento fue preparado bajo los auspicios y con la aprobación del Grupo de Trabajo 2 en «Seguridad de las carreteras», presidido por Roberto Arditi, SINA/ASTM-SIAS de Italia, con los siguientes participantes:

- *Steve Ernst, Departamento de Transporte, Estados Unidos.*
- *Jürgen Krieger, Instituto Federal de Investigación de Carreteras, Alemania.*
- *Bine Pengal, Instituto Esloveno de Construcción e Ingeniería Civil, Eslovenia*
- *Dominique Schmitt, Instituto Francés de Ciencias y Tecnología del Transporte, Francia.*

Un reconocimiento especial a los consejos y aportaciones preparados por el Centro de Gobierno Británico para la Protección de la Infraestructura Nacional (CPNI), cuyos agentes fueron los primeros en proponer la redacción de este informe.

Algunos miembros de la Asociación Mundial de la Carretera, ajenos al Grupo de Trabajo, y otros expertos, contribuyeron a este informe brindando un aporte científico al taller internacional organizado por el Grupo de Trabajo 2 de la Asociación Mundial de la Carretera y auspiciado por las autoridades británicas en Londres, el 10 de junio de 2014.

La versión en español del presente informe ha sido realizada y revisada por la Secretaría de Comunicaciones y Transportes de México.

RESUMEN EJCUTIVO

2015R01ES

SEGURIDAD DE LA INFRAESTRUCTURA CARRETERA

Hay una amplia gama de amenazas que potencialmente afectan la infraestructura y la operación de las carreteras: por ejemplo, las amenazas a individuos, a operadores y en general dirigidas a la sociedad. Este informe aborda las amenazas dirigidas a la infraestructura.

Las carreteras han sido con anterioridad objetivo de organizaciones terroristas. La infraestructura del transporte es la base de la economía nacional y proporciona libertad de tránsito. La protección de los ciudadanos ya sean los usuarios de carreteras, peatones o personal de mantenimiento, es un asunto de gobierno. Una amplia gama de riesgos puede afectar la infraestructura de carreteras, puentes y túneles. Se debe considerar el terrorismo, el crimen cibernético, robos y engaños. Para los eventos de baja frecuencia y de alta consecuencia, es difícil evitar la complacencia y esto puede impactar en la motivación de las fuerzas de seguridad, la reacción de los usuarios a quienes les es difícil saber lo que se debe informar como sospechoso y las acciones de las autoridades a cargo de las carreteras para determinar la relevancia y la relación costo-beneficio de las medidas preventivas o de protección.

Un entendimiento correcto y un adecuado manejo de la seguridad de la infraestructura vial no sólo es importante para salvaguardar la infraestructura misma, sino también es pertinente para cubrir la protección de los valores sociales y económicos para aquellas actividades que dependen de la infraestructura carretera, la protección del ambiente e incluso la seguridad de otros modos de transporte.

El objetivo de este informe es:

- ofrecer una visión general de la gama de amenazas y problemas que afectan a los usuarios, las operaciones y a la infraestructura carretera.
- promover la reflexión y el análisis dentro de la comunidad carretera a fin de sensibilizar y permitir a las autoridades y operadores de carreteras avanzar con buenas prácticas internacionales sobre la *"Seguridad de la Infraestructura de Carreteras"*.

El informe describe los siguientes temas de interés para la seguridad de las carreteras:

- evaluación de la seguridad física;
- diferentes enfoques metodológicos;
- seguridad y programas de seguridad;
- aplicación de los conocimientos en seguridad mediante el diseño;
- modernización de la infraestructura existente.

ÍNDICE

NECESIDAD DE ESTE DOCUMENTO

Una infraestructura vial confiable es necesaria para la movilidad sostenible y hace una importante contribución a la calidad de vida de los ciudadanos. Para lograr un nivel satisfactorio de confiabilidad en las carreteras, es necesario considerar la seguridad y protección tanto de la infraestructura como del tráfico. Las necesidades de la infraestructura vial están cambiando con la composición y creciente volumen de tráfico y con las necesidades cambiantes de la sociedad.

Es posible que las carreteras no tengan una atracción alta como objetivos potenciales, pero las organizaciones terroristas se han dirigido con anterioridad a la infraestructura de transporte. La infraestructura del transporte es la base del bienestar de la economía nacional y ofrece libertad de tránsito. La protección de los ciudadanos ya sean usuarios de la carretera, peatones o personal de mantenimiento, es un asunto que corresponde a los gobiernos, pero una amplia gama de riesgos y amenazas impactan a la infraestructura carretera, de puentes y de túneles. Ofrecemos protección contra accidentes, crímenes y otras amenazas de seguridad al usuario, pero ahora también debemos considerar al terrorismo, crimen cibernético, robos y engaños *(foto 1)*. Para aquellos eventos de baja frecuencia y alta consecuencia, es difícil evitar la complacencia y esto puede impactar en la motivación de las fuerzas de seguridad, la reacción de los usuarios a quienes les es difícil saber lo que se debe informar como sospechoso y las acciones de las autoridades a cargo de las carreteras para determinar la relevancia y la relación costo-beneficio de las medidas preventivas o de protección.

Un entendimiento correcto y un adecuado manejo de la seguridad de la infraestructura vial no sólo es importante para salvaguardar la infraestructura misma, sino también es pertinente para cubrir la protección de los valores sociales y económicos para aquellas actividades que dependen de la infraestructura carretera, la protección del ambiente e incluso la seguridad de otros modos de transporte.

Foto1 - Camino interrumpido por acción directa

El objetivo de este informe es:

- proporcionar una visión general de la gama de amenazas a la seguridad y los problemas que afectan a la infraestructura vial, a las operaciones y a los usuarios;
- promover la reflexión y el análisis dentro de la comunidad carretera a fin de sensibilizar y permitir a las autoridades y operadores carreteros avanzar con buenas prácticas internacionales sobre *«Seguridad de Infraestructura Carretera»*.

ANTECEDENTES

La infraestructura vial es vulnerable y accesible por necesidad y ofrece un medio conveniente de movilidad para aquellos que desean hacer daño. Es posible que la infraestructura vial se perciba como un objetivo fácil si hay pocas medidas protectoras de seguridad visibles en el lugar. Si las vialidades son también lugares concurridos, como en los centros de las ciudades, entonces pueden resultar aún más atractivas como objetivos para aquellas personas con intenciones maliciosas. Las buenas medidas protectoras de seguridad han demostrado disuadir y desplazar esas amenazas.

Debido a la naturaleza de los eventos riesgosos creados por el hombre, es difícil anticipar problemas de seguridad en términos de tiempo y lugar. Impredecibles o poco probables, incluso los eventos catastróficos son posibles y una de las funciones de las autoridades a cargo de las vialidades es reducir las posibles consecuencias de los ataques, haciendo esos ataques más difíciles de llevar a cabo y/o potencialmente menos efectivos. El costo es siempre un problema y un buen propósito es esforzarse en buscar estrategias que sean proporcionadas y rentables. La trascendencia del activo debe tomarse en cuenta para cualquier contramedida.

Un proceso de evaluación de los riesgos para la seguridad vial y un plan efectivo para la implementación de las medidas de mitigación ayuda a las autoridades, a los administradores de las vialidades y a los operadores de las carreteras a hacer inversiones y decisiones de una forma científica y realista.

"La seguridad mediante el diseño" es más fácil y menos costosa que aplicar medidas a los elementos de infraestructura existentes (modernización). De hecho, una cuestión importante es no sólo que las medidas de seguridad de modernización pueden no ser tan robustas como las que se incluyen en el proceso de diseño inicial, sino que también esas medidas de modernización pueden ser extremadamente costosas, lo que requiere un proyecto independiente, provocando retrasos. Incorporar seguridad al comienzo del proceso de diseño, tiene muchas ventajas tanto en ahorros en costos como en efectividad.

Foto 2A - Puente I-40 cerca de Oklahoma City (Oklahoma, Estados Unidos) que falló cuando una barcaza, fuera del canal y que viajaba aguas arriba, golpeó y dañó una columna del puente, causando la caída del claro

Foto 2B - Isla de rocas colocada en un gran puente que protege a la pila de las colisiones de los buques así como de un acto de terrorismo

Tanto para los actos intencionales del terrorismo como para los actos no intencionales como la colisión de una barcaza, las pilas de los puentes se pueden proteger con islas de roca, delfines o defensas. Es posible que las islas de roca sean la mejor opción de seguridad contra impactos intencionales y explosivos (como la que se muestra en la *foto 2B*), pero es probable que ésta opción solo esté disponible si el proceso de planificación haya considerado el impacto de la huella de la isla en la vía del canal ya que agregar esa característica en fases avanzadas del diseño es costosa en función del tiempo y del dinero.

Existe el reto del *"Cisne negro*[1]*"*, evento de baja frecuencia y alto impacto que es difícil de pronosticar y el reto que surge de eventos más predecibles que requieren de nuestra constante atención. La seguridad de la infraestructura vial está sujeta a estos dos desafíos. Sin duda, hay que ocuparse de los acontecimientos previsibles, diarios y a menudo es una buena opción y tal vez rentable, tomar acciones para eliminar o reducir consecuencias catastróficas de los acontecimientos que no son frecuentes.

Es posible que algunos incidentes de seguridad sean de bajo nivel de impacto y alta frecuencia de ocurrencia (por ejemplo ataques contra conductores de vehículos pesados, fraude electrónico en los peajes, robo de metales). Tienen un impacto agregado y erosivo pero no atraen la atención de los medios de comunicación. En Europa, un gran número de conductores de camiones es atacado y robado[2], ya que con frecuencia se percibe que las instalaciones para estacionarse más seguras son demasiado costosas.

El terrorismo representa un incidente de alto impacto pero de baja frecuencia, que atrae consigo una extensa cobertura de los medios de comunicación. Normalmente se requiere una importante inversión en medidas de protección de la seguridad para mitigar este tipo de ataque.

Es importante entender la naturaleza de las amenazas a la red, elementos que son críticos, en la cual están las principales vulnerabilidades, antes de que se pueda ordenar una respuesta adecuada.

Con el fin de aplicar las contramedidas sobre elementos críticos, se necesita una evaluación de la amenaza y vulnerabilidad que implica la consideración de la capacidad e intención maliciosa de los hostiles, identificación de posibles escenarios y determinación de la vulnerabilidad de los activos y sus componentes importantes. La identificación de las vulnerabilidades y su criticidad es esencial para priorizar el gasto, pero con frecuencia estos términos se intercambian de manera equivocada. También es necesario considerar la resiliencia de la infraestructura crítica así como cualquier interdependencia con otras infraestructuras y sectores.

Las alianzas con diferentes actores son clave para el éxito en la protección de las infraestructuras críticas. Se debe tener en cuenta a las instalaciones vecinas y a las relaciones con todo aquel con un rol en la seguridad y con otros que no necesariamente tengan una responsabilidad directa de la seguridad. La negociación y las alianzas son habilidades importantes cuando se trabaja con operadores de sitios adyacentes, cuyas instalaciones pueden formar parte de las

[1] Nassim Nicholas Taleb: El cisne negro - el impacto de lo altamente Improbable
[2] De acuerdo con ITF (15 de febrero de 2013, Palacio de las Naciones, Génova): 1 conductor de cada 6 (17%) fue atacado en los últimos 5 años (30% más de una vez). Fuente: ***http://www.unece.org/trans/events/2013/inlandsecurity_forum13.html***

infraestructuras críticas. La complacencia también puede ser un desafío, por lo tanto la capacitación y difusión de la información es vital para asegurar que los interesados estén actualizados y comprometidos desde el principio en el proceso de protección de su infraestructura.

Las soluciones de seguridad independientes son difíciles de poner en práctica sin un marco legal. Se pueden lograr soluciones de seguridad rentables cuando existen sinergias con medidas de seguridad obligatorias.

¿Qué constituye el riesgo?

Amenaza
Los peligros antropogénicos o causados por los humanos pueden dar como resultado un desastre. En este caso, las amenazas antropogénicas son las que tienen un elemento de intención humana, negligencia, o error; o que involucran una falla de un sistema creado por el hombre. Tienen como resultado pérdida de vidas y/o propiedades. Afectan además el bienestar físico, mental y social de las personas. Esto es opuesto a las amenazas naturales como inundaciones o terremotos.

Vulnerabilidad
Son las características, parámetros y condiciones de una estructura, infraestructura, sistema o población que lo hacen susceptible a los efectos adversos de una amenaza. Los factores que definen la vulnerabilidad son de naturaleza física, social, económica y ambiental. La vulnerabilidad varía significativamente dentro de una comunidad y con el tiempo.

Activos críticos
Activos que tienen gran potencial para impactar en el logro económico, operacional y en los objetivos de seguridad de las autoridades nacionales.

Resiliencia
Es la habilidad para preparar y planificar, absorber, recuperar y adaptarse con mayor éxito de los eventos adversos.

Medidas blandas
Estas son medidas que se asumen en la operación, organización y capacitación del personal. La modernización de los activos puede incluirse en la gama de medidas suaves.

Riesgo
Una medida de la probabilidad de ocurrencia de daño a la vida, salud, propiedad y/o al ambiente, como resultado de un peligro determinado.

Lea más en: http://www.businessdictionary.com/definition/risk.html#ixzz3TYSBPTJu

No hay ningún método universalmente aceptado para la evaluación y gestión de los riesgos de seguridad. Entre los expertos, el debate está en curso en cuanto a lo que es apropiado, eficaz, económico y qué compensaciones y tolerancias del usuario existen. Un enfoque de diseño basado en el riesgo del tipo *"todos los riesgos"* no es todavía de vanguardia. La monetización (o estimación diferente) de la pérdida de vidas, interrupción del servicio y cuantificación de valor icónico, apuntalan este tipo de enfoque. Un proceso de constante revisión sería recomendable para la criticidad y vulnerabilidad.

La velocidad del cambio en la sociedad, la complejidad, la tecnología y la interconectividad tienen un impacto sobre la seguridad. La sociedad está experimentando una revolución que se basa en el internet y en la tecnología y hay oportunidades sin precedentes para explotar nuevos sistemas. La tecnología está jugando un papel clave en los sistemas viales cada vez más complejos, con posibilidades de utilizar sistemas inteligentes de transporte y la constante necesidad de mantenerse al día con los desarrollos y las nuevas vulnerabilidades. El mundo está experimentando una importante ola de innovación relacionada con oportunidades de comunicación cada vez mayores (móviles, internet, etc.). Este tipo de innovación está entrando en la tecnología automotriz, mejorando la seguridad y eficacia del transporte a través de vehículos conectados entre sí (desde sistemas cooperativos hasta vehículos autónomos) y con la infraestructura. Aunque se esperaba que diera un resultado positivo para los ciudadanos, la seguridad del sistema de transporte será más compleja, ya que la nueva amenaza de ciberataques podría afectar directamente la seguridad de las operaciones de carreteras, túneles y puentes. Aunque el costo de la seguridad es una preocupación, las preguntas *"¿quién posee el riesgo?"* y *"¿existen medidas rentables?"* están entre las más difíciles a considerar.

EVALUACIÓN DE LA SEGURIDAD FÍSICA

Las amenazas a la infraestructura vial son muy variadas, por ejemplo por parte del terrorismo, armas de lanzamiento, dispositivos explosivos improvisados instalados en vehículos, explosivos colocados a mano, explosivos de contacto, dispositivos de corte no explosivos, cargas de corte, lanzas térmicas, fuego (hidrocarburos, materiales peligrosos), impactos, robo de metales, vandalismo, intrusos, crimen, contaminación, peligros naturales, drogas y alcohol y daño accidental. No hay una definición internacionalmente aceptada de las infraestructuras críticas. El riesgo es una función de las consecuencias y las vulnerabilidades del activo componente.

Foto 3 - Secuelas de una explosión en una autopista

No es posible proteger todo, por lo tanto debe utilizarse un enfoque de seguridad proporcional y estratificado, que incluye una consideración de lo que es crítico en el lugar y conceptos de disuasión, detección y retraso. Para enfrentar todas las amenazas mencionadas se requiere un enfoque integral: se necesita tener en cuenta la naturaleza de la infraestructura y el medio ambiente, del personal y la seguridad cibernética.

Se requiere de la planificación, coordinación y control para mejorar la detección y la capacidad de respuesta. Herramientas como los circuitos cerrados de televisión con análisis de video han demostrado ser útiles para el buen funcionamiento (por ejemplo utilizar los circuitos cerrados de televisión para verificar una alarma). Se pueden implementar medidas adicionales en tiempos de amenazas crecientes. En algunos países, las administraciones carreteras capacitan al personal

en materia de seguridad: capacitación en reconocimiento de fuerzas hostiles, pruebas de penetración y en ejercicios reales de planificación de contingencia y respuesta interinstitucional.

Las evaluaciones de criticidad son un problema complejo que requiere inversión social. Un proceso de evaluación debe ser trazable, transparente y reproducible. Se requiere una combinación de técnicas de ingeniería y modelos apropiados para la comparación y toma de decisiones. Las preguntas típicas son:

[1] ¿Cómo decide un propietario gastar dinero para proteger una carretera, un puente o un túnel[3]?
[1] ¿De qué manera necesita el dueño describir los términos de referencia del contrato?
[1] ¿De qué manera un dueño o un operador integra la seguridad en los planes de gestión de activos?

Foto 4 - Construcción de nueva infraestructura

Una planeación eficaz incluye la identificación y selección de elementos críticos en la red de carreteras, examina los componentes críticos para cada elemento importante en la red (puente o túnel por ejemplo), el análisis de la amenaza, la identificación de las personas con intenciones criminales, identificación de los medios de ataque, análisis de vulnerabilidad de la infraestructura, elaboración de escenarios de amenaza mediante la evaluación de amenazas, vulnerabilidades y consecuencias, definición de las contramedidas a través de la combinación del nivel de riesgo de los elementos críticos con acciones específicas.

> *El interés por la seguridad física no se limita a la inteligencia y a las de actividades de patrullaje. Se pueden fácilmente lograr soluciones más efectivas cuando el asunto es incluido en programas de gestión de activos y gestión de proyectos.*

Es recomendable la investigación nacional y de cooperación y desarrollo con programas que abarcan la seguridad física, personal y cibernética, – esto significa que el desarrollo de contramedidas es objetivo. Es necesario un diseño integral de medidas de seguridad. Incluso la seguridad cibernética puede tener un impacto en la seguridad física.

[3] Protegiendo de esta manera incluso el funcionamiento de la red global.

Es aún más difícil la evaluación de la probabilidad de ataques y el estiramiento de los recursos que pueden producirse en caso de ataques simultáneos. En términos generales, la falta de información sobre la probabilidad de un ataque hace más difícil identificar la rentabilidad. Si una contramedida tiene múltiples beneficios, es posible que eso sea útil para el proceso de decisión.

Los indicadores para la evaluación estructural podrían ser la durabilidad general y la resistencia bajo diversas amenazas, el riesgo estructural, el tiempo requerido para la reparación después de un daño y el costo de reparación estimado.

Los indicadores para la evaluación de la seguridad del usuario podrían ser la evaluación de riesgos cuantitativa con respecto a las limitaciones locales y escenarios específicos, el cálculo de probabilidades, las consecuencias y los riesgos acumulados y la posible aplicación de medidas de mitigación. Los indicadores para la evaluación de costos de ciclo de vida (LCC) son los costos de inversión inicial (construcción, equipamiento, contramedidas, etc.), seguimiento de costes (mantenimiento y reparación), los costos de desmantelamiento y los ingresos posibles en casos de alianzas público-privadas (PPP).

Los indicadores para la evaluación de la criticidad del sistema son el impacto en la red de infraestructura circundante, pérdida parcial o completa de una estructura y pérdida del servicio.

Los criterios blandos incluyen el valor simbólico de un activo como un puente o un túnel.

Criterios de filtro bastos para evaluar los riesgos de puentes y túneles son: TDPA alto (tráfico diario promedio anual) o camiones (vehículos de carga pesada), construcción sensible por debajo, sobre o cerca de la estructura; período de reconstrucción largo; alto valor simbólico (atractivo para los ataques provocados por el hombre); puentes de arcada larga y túneles. La evaluación de la criticidad se puede realizar transformando valores físicos en clases de utilidad (p. ej. 1 a 5), ponderación de los indicadores y utilizando valores predeterminados uniformes con información del propietario. Cuando la criticidad del sistema de tráfico se basa en los tiempos de viaje adicional, otros indicadores pueden agregarse como las emisiones, los accidentes etc.

Algunas observaciones sobre el proceso de organización:

- en algunos sectores y disciplinas, los operadores están pensando en la seguridad antes que en las capas de renivelación; la seguridad vende y las organizaciones creen que ellos entienden mejor sus operaciones y están dispuestos a actuar, asumiendo que hay espacio en su presupuesto;
- la presencia en la organización de una cultura de seguridad dedicada a la protección de la Infraestructura podría ser útil para consolidar el asesoramiento a los propietarios, operadores, reguladores y policía;
- las soluciones que solo se enfocan en la seguridad son difíciles de poner en práctica sin un marco legal.

En algunos países las prioridades son adelantarse a los posibles atacantes y educar e influir en los dueños - que es posible no hayan experimentado ataques. Se puede utilizar información

de amenazas para planear la dirección y la progresión de intenciones maliciosas y metodologías de ataque.

DIFERENTES ENFOQUES METODOLÓGICOS

Los propietarios de la infraestructura vial (en la mayoría de los casos son las autoridades que administran las carreteras) son responsables de la conservación en general, en consecuencia, desde la perspectiva del usuario, el procedimiento, por sí mismo, no es tan importante. Lo importante es el resultado final que debe ser comprensible y adaptado de forma que el procedimiento se adapte fácilmente al razonamiento y a las formas burocráticas. Es la única manera en que las soluciones obtendrán financiamiento y se implementarán. Por lo tanto, es más la cuestión sobre lo qué los expertos pueden aprender de los dueños y las autoridades administradoras de carreteras y sus razonamientos que puede ser de beneficio en el diseño de los enfoques metodológicos.

Hay muchos enfoques y variantes al hacer una evaluación de seguridad (criticidad y vulnerabilidad) de una cierta estructura en una red de carreteras. Estos enfoques varían según el sector de la infraestructura misma (transporte, energía, gestión del agua, etc.), según los diferentes países, la historia y experiencias de ataques directos a la infraestructura y así sucesivamente. El resultado final de dicho análisis sin embargo deberá incluir al menos la siguiente información para el propietario:

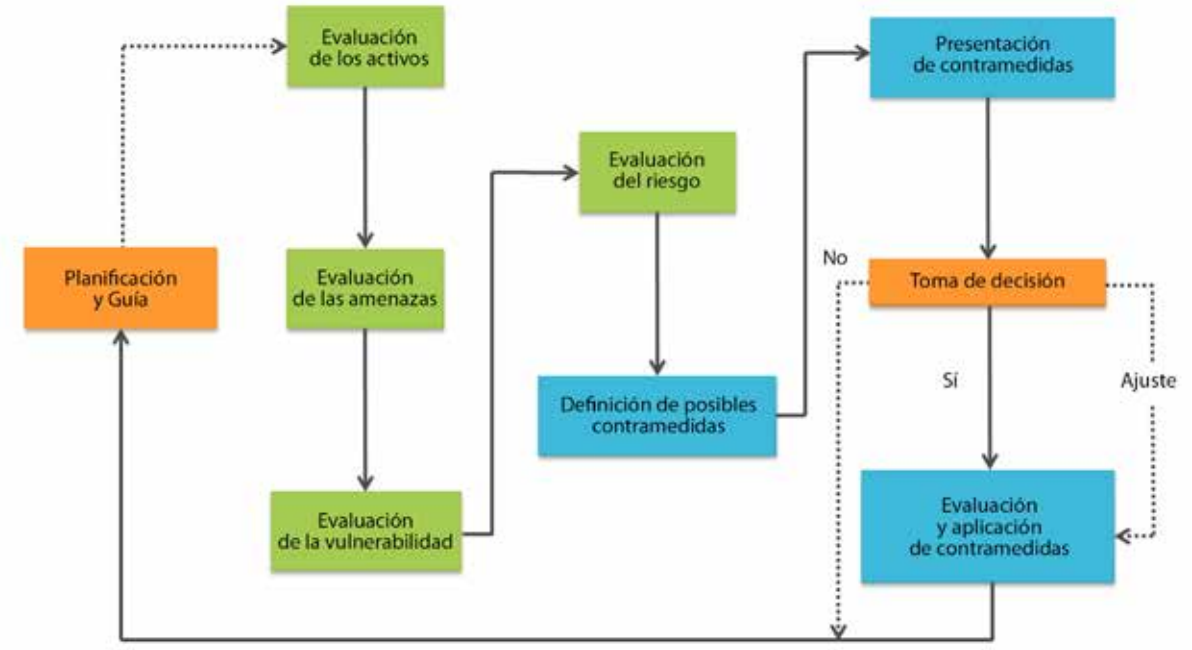
- identificación de las estructuras de la red que necesitan protección (puente, túnel, paso, etc.);
- lista clara y completa de las amenazas a esta estructura;
- lista clara y completa de las contramedidas propuestas;
- cálculo claro y detallado de los costos estimados para la implementación de las medidas de prevención / protección;
- análisis de la relación costo-beneficio considerando incluso otros beneficios posibles (por ejemplo, la seguridad).

Con esta información básica el propietario de la infraestructura puede decidir de manera competente sobre las inversiones a realizar. La imagen de abajo representa los pasos del procedimiento básico para el análisis enfocado en la seguridad para cierta estructura que al final brinda al propietario respuestas a todos estos problemas antes mencionados.

Un ejemplo de la literatura abierta, que proporciona un enfoque interesante a nivel nacional, es el *"marco de cumplimiento de TRANSEC (Transmisión de Seguridad)"* producido por el Departamento de Transporte del Reino Unido. Este tiene como objetivo proteger a la población viajera, las instalaciones de transporte y a la gente que trabaja en la industria del transporte (sobre todo contra actos de terrorismo). El Marco de Cumplimiento de TRANSEC tiene objetivos de seguridad sobre varios modos de transporte, incluyendo las carreteras (transporte de mercancías peligrosas únicamente).

Los objetivos son:

- organizar un programa proactivo y reactivo de cumplimiento que vigila la actividad para mantener y, cuando sea necesario, mejorar las normas de seguridad; tomar medidas oportunas, en consonancia con el enfoque escalonado, donde se identifican las deficiencias;



Análisis básico enfocado en la seguridad

- participar con la industria en todos los niveles para influir en su pensamiento estratégico y táctico para que la seguridad forme parte de la planificación de negocios y de la toma de decisiones;
- fomentar que la industria tome propiedad y responsabilidad de la seguridad y adapte en consecuencia sus actividades de aseguramiento de la calidad.

Alemania realiza investigación en el campo de la seguridad de la infraestructura carretera a nivel nacional (dentro del *"Programa Nacional de Investigación de la Seguridad"*): proyectos SKRIBT y SKRIBT +. Además, se encuentran disponibles los resultados de diversos proyectos de investigación en proyectos a nivel europeo como SERON, SECMAN. Los enlaces para estos proyectos están disponibles en el siguiente capítulo *"Recursos sobre seguridad vial"*.

A continuación se describen las referencias y breves descripciones de algunas herramientas utilizadas en los Estados Unidos para la evaluación de riesgo y para el diseño de contramedidas.

Ray, James C., Medidas de priorización de mitigación de amenazas terroristas en puentes, Revista de Ingeniería de Puentes, ASCE/SEI, Vol. 12, número 2, marzo/abril de 2007.

Este artículo describe un método basado en el riesgo para priorizar las estrategias de mitigación en un puente, haciendo coincidir cada componente en la estructura con riesgos específicos de terrorismo. Los resultados se miden frente al impacto de las medidas de mitigación y sus costos para ayudar a los propietarios a identificar una protección eficaz. La Administración Federal de Carreteras de los Estados Unidos ha adoptado este proceso y el Departamento de Seguridad Nacional para la evaluación de puentes estratégicos.

Informe de la NCHRP 645, Puentes en carreteras a prueba de explosivos Directrices de Diseño y Detalles, Consejo de Transporte e Investigación, Washington, D.C., 2010.

Este informe describe la respuesta de las columnas de puente de concreto sujetos a cargas de explosión, las directrices de diseño y detalle de las columnas de puentes sobre carreteras sometidos a las cargas y los resultados de experimentos para validar modelos para estas columnas. Los resultados

se adoptaron como una especificación indicativa en los Estados Unidos, en el Código de Factores de Diseño Oficiales de Carga y Resistencia de la Asociación Americana de Carreteras y Transporte. Los ejemplos del diseño demuestran cómo la metodología puede utilizarse para diseñar columnas más resistentes y evaluar diseños existentes comparados con un conjunto razonable de normas.

Informe de la NCHRP 525, volumen 15, Costos de protección de activos: Una guía de todos los peligros para agencias de transporte, Junta de Investigación en el Transporte, Washington, DC, 2009, www.trb.org.

CAPTOOL, guía del usuario para CAPTA, USDOT Centro Volpe, de la Administración Federal de Carreteras del Departamento de Transporte de los Estados Unidos[4]. Esta guía se actualizará con la nueva versión de CAPTA.

Estos dos documentos (CAPTA y CAPTOOL) describen un método para que las agencias de transporte gestionen el riesgo, utilizando atributos accionados en consecuencia para evaluar decisiones sobre financiamiento de alto nivel para múltiples activos expuestos a múltiples peligros. El informe detalla la metodología y CAPTOOL es una guía de usuario desarrollada por la Administración Federal de Carreteras para facilitar el uso de la herramienta. Se trata de una herramienta basada en el costo que reconoce límites a la financiación del transporte y la necesidad de equilibrar las decisiones de inversión entre muchos factores concurrentes, incluyendo las amenazas terroristas. Ambos documentos están disponibles y útiles en su forma actual y están bajo revisión, se espera que estén listos en el año 2015.

Encontrar literatura francesa sobre enfoques metodológicos para la seguridad no es un ejercicio fácil en general. La seguridad del transporte por carretera en particular no escapa a esta regla general. De hecho, el gobierno de Francia tiene una fuerte cultura de defensa nacional secreta. Por lo tanto, cuando existen guías metodológicas, a menudo se clasifican de *"defensa confidencial"* y, por consiguiente, sólo personas autorizadas tienen acceso a ellas. Por la misma razón, no son tantos los libros sobre el tema.

Los documentos administrativos franceses acerca de la seguridad del transporte comenzaron a publicarse en 2004, con la transposición francesa de las directivas europeas n° 2004/111/CE sobre *Transporte de mercancías peligrosas por carretera* y n° 2005/65/CE sobre B*uques internacionales y seguridad portuaria* (ISPS).

En consecuencia, puede encontrar asesoría autorizado acerca de la seguridad del transporte de mercancías peligrosas por carretera en la circular n° 2005-62 del 07 de octubre de 2005 y en particular, la guía elaborada por una asociación interprofesional, publicada como anexo[5] de la misma. Sobre la evaluación de seguridad de los puertos e instalaciones correspondientes, se puede encontrar asesoría en la circular de 2004[6], con más detalles en el anexo de una ley del 22 de abril de 2008[7].

Después, llegó el momento de la aplicación en Francia de una ley sobre "sectores de interés vital" (ley 2006-212 de 23 de febrero de 2006)[8], un concepto francés que más tarde inspiró

[4] *http://www.fhwa.dot.gov/security/emergencymgmt/profcapacitybldg/documents.cfm fhwa.dot.gov*

[5] *http://www.bulletin-officiel.developpement-durable.gouv.fr/fiches/BO200520/A0200044.htm*

[6] Circular del 29 de marzo de 2004 relativa a la implementación de medidas de fortalecimiento de la seguridad de los IP *http://www.upem.org/textes/Circ040329Surete.pdf*

[7] Ley del 22 de abril de 2008 que define el establecimiento de las evaluaciones y los planes de seguridad portuaria

[8] *http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000018767437)*

incluso a la Unión Europea para desarrollar su propia Directiva 2008/114/CE del 08 de diciembre de 2008 en la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección[9].

La Agencia del gobierno francés SGDSN (Secretaria General de la Defensa y la Seguridad Nacional) publicó a una guía para el desarrollo de planes de seguridad del operador y otros documentos útiles, pero clasificados. La protección de infraestructuras críticas se ha reanudado por medio de la instrucción interministerial n ° 6600[10]. Las infraestructuras viales se consideran como uno de los 12 sectores vitales tratados en este mecanismo.

Cualquiera que sea el campo deseado, el principio rector del método francés es aún sobre lo mismo: evaluación de la amenaza, resistencia y medidas de reducción de riesgo, planificación (organización, procedimientos, formación), detección y alerta, acción y rehabilitación, retroalimentación.

PROGRAMAS DE SEGURIDAD Y PROTECCIÓN

Se necesitan soluciones rentables de seguridad. Hay una gran superposición entre seguridad y protección (a menudo no son claros los límites) que puede utilizarse para fortalecer a ambas. Es más fácil para los dueños implementar soluciones de seguridad rentables donde existen sinergias con la protección. Los propietarios y operadores deben tener acceso a las metodologías y herramientas para aprovechar esta sinergia. Existe la necesidad de identificar objetos críticos y/o tramos carreteros y llevar a cabo análisis de vulnerabilidad con respecto a los escenarios de amenaza correspondientes y de evaluar la efectividad de las medidas de seguridad. ¿Son análogos desde el punto de vista de los programas la seguridad vial y los problemas de seguridad? Para la seguridad vial, si hay una reducción en las victimas de las carreteras a partir de una acción, entonces hay una compensación demostrable y amplia información que lo respalda. Es diferente para la seguridad con poca base de datos y bajo número de incidentes que hacen que intervenciones parezcan subjetivas y demasiado caras.

Hay una gran superposición entre seguridad y protección que puede utilizarse para fortalecer a ambas.

Un ejemplo: la tecnología de túneles en la carretera está desarrollado en cuanto a la protección. Es posible que los accidentes en túneles se relacionen con la protección o la seguridad (por ejemplo, incendio o terrorismo) y que las instalaciones estructurales y operacionales de seguridad se utilicen para evitar y mitigar tanto los eventos relacionados con la protección y con la seguridad. Existe un marco legal para la seguridad en túneles. Podrían utilizarse medidas adicionales como sistemas de detección innovadores para determinados puentes o túneles vulnerables o críticos y para la detección de vehículos, personas y objetos sospechosos con un enfoque en la prevención.

Sólo algunas medidas de seguridad son rentables cuando se enfocan estrictamente en aspectos de seguridad. Deben considerarse medidas con reducción potencial de riesgo

[9] *http://www.legifrance.gouv.fr/Eli/decret/2006/2/23/2006-212/Jo/texte*
http://EUR-Lex.Europa.eu/legal-Content/en/All/;ELX_SESSIONID=rT5PJ3MLYvJBx9ClVSpCgCb7rPqnvJk3dmGpxLs3vtZsp9sSmgTG!-870916461?uri=CELEX:32008L0114.
Consulte la publicación en Seguridad y Defensa Europea, enero de 2009
http://www.european-security.com/index.php?id=5845

[10] *http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf*

relevante y beneficios adicionales (por ejemplo, impactos en múltiples escenarios en seguridad). Proyectos europeos nacionales demostraron que el uso de *Sistemas de gestión de riesgos en tiempo real en túneles* (sistemas de detección existentes más sistemas de detección innovadores nuevos) que permiten la visualización del nivel de riesgo al operador del túnel en el centro de control en tiempo real y un experto en el sistema que sugiere medidas preventivas o de mitigación en caso de niveles de riesgo en *«amarillo»* o *«rojo»*

Los Sistemas de Transporte Inteligentes (ITS) integran tecnologías para vigilar el comportamiento del tráfico (por ejemplo, Bluetooth, teléfonos móviles y reconocimiento de placas de circulación) y están diseñados para mejorar los flujos de tráfico y la seguridad vial. A veces estos sistemas de vigilancia se pueden utilizar específicamente para propósitos de seguridad[11]. Por ejemplo, los ITS pueden utilizarse en situaciones de emergencia para apoyar a los equipos de gestión de crisis. Se pueden adoptar también para fines de aplicación. La tecnología de vehículos conectados tiene un gran potencial para la conducción pública, pero también introduce un nuevo conjunto de amenazas. La intención maliciosa, incluyendo los ataques cibernéticos, requerirá la atención concertada de los diseñadores y operadores de sistemas.

APLICACIÓN DE LOS CONOCIMIENTOS EN SEGURIDAD MEDIANTE EL DISEÑO

Después de una extensa investigación en las infraestructuras y los actos de terrorismo, un número creciente de ingenieros consultores y científicos tiene los conocimientos para diseñar estructuras a prueba de actos de terrorismo.

Algunas medidas de protección podrían costar menos de 1% del presupuesto total del proyecto; sin embargo, los códigos de diseño no requieren acciones de protección y los propietarios generalmente no los solicitan. Los principios generales y las especificaciones existentes pueden consultarse para el diseño de la seguridad y existe información considerable sobre las medidas de protección y el diseño de protección fuera de especificaciones. Ciertamente, hay espacio para el desarrollo de códigos y prácticas de mejora de la seguridad y la necesidad de que la Asociación Mundial de la Carretera pueda jugar un papel importante en el intercambio de información internacional. Los siguientes son algunos puntos claves del taller de la fuerza de tarea de seguridad de la Asociación Mundial de la Carretera, en relación a la seguridad mediante diseño.

Algunas medidas de protección son relativamente baratas y fáciles de implementar. Esto es particularmente cierto cuando los principios de la seguridad ya se incluyen desde las fases de diseño conceptual y preliminar.

Hay algunas medidas sencillas de seguridad de protección. Mantener a la gente lejos de los componentes críticos. Planificar con antelación el control de acceso (por ejemplo, bloquear las escotillas, etc.). Proporcionar independencia (por ejemplo de las columnas). Ningún sistema es impenetrable (por ejemplo, la gente puede escalar puentes) y se debe decidir el alcance del control de acceso que es razonable implementar. Garantizar el enlace de dispositivos y sensores de vigilancia a una fuerza de respuesta adecuada, con un concepto de operaciones de respuesta.

[11] Los aspectos de la privacidad de los datos necesitan ser tomados en cuenta al considerar medidas de seguridad; en algunos países (por ejemplo, Alemania) la protección del derecho a la intimidad hace más difícil la acción a activos seguros.

Como cabría esperar, una proporción considerable de las amenazas terroristas internacionales se ha dirigido contra puentes colgantes y otras estructuras icónicas (es decir, los más visibles), aunque un gran porcentaje de ataques reales ha sido dirigido en los puentes más comunes. Cables de puente, torres, columnas y vigas pueden ser vulnerables debido a su exposición directa a la explosión y a los efectos de grandes incendios. En este entorno de amenaza, pulgadas de aislamiento hacen la diferencia.

Las medidas de protección se pueden clasificar:

- por tipo: estructural, operacional y organizacional;
- por efecto: preventivo – antes del incidente, atenuante – incidente, reconstructivo – incidente posterior al incidente.

Para los nuevos diseños, existe la oportunidad de centrarse en el comportamiento del sistema mejorado, para mejorar activos - el nivel de redundancia y para implementar medidas independientes para componentes vulnerables. La solidez tiene valor para todos los peligros y hay oportunidad de tomar ventaja de los beneficios de la mitigación para más que solo la seguridad.

El diseño de puentes para seguridad no está tan desarrollado como para el diseño de edificios. Aun así, hay muchas oportunidades de utilizar las lecciones de la industria de la construcción para influenciar el diseño de seguridad en el transporte.

MODERNIZACIÓN DE LA INFRAESTRUCTURA EXISTENTE

Cuesta más adaptar la infraestructura existente para que incluya medidas que hacerlo desde el principio, sin embargo, se necesita una lista de posibles medidas de adaptación, incluyendo beneficios, requisitos de mantenimiento y prácticas de buen diseño. Las medidas deben ser robustas, seguras y proporcionales. Deben proporcionar relación calidad-precio, no deben comprometer la inspección ni el mantenimiento, deben ser ambientalmente apropiadas y encajar con la imagen deseada por la autoridad competente.

Los conceptos clave para su consideración son redundancia, recuperación, endurecimiento estructural y alta independencia. Se recomienda emplear un simple conjunto de medidas, estas medidas deben ser complementarias al plan de respuesta. Hay un requisito para las soluciones de bajo presupuesto, con seguridad encajar en las prácticas de negocio principales. Los términos *"protección"* o *"mitigación"* pueden ser aceptados más fácilmente que el término "seguridad". Se deben identificar las cláusulas modelo basadas en las buenas prácticas para la aplicación en los contratos.

La protección física incluye cercas, mallas, barreras para accidentes de tránsito, puertas de acceso de vehículos, puertas de seguridad y acceso con llave, bolardos (Grado[12] PAS, CWA o AIT, no clasificadas y bolardos de seguridad), gaviones, muros de contención y zanjas, cámaras con análisis, cerraduras, sistemas de detección de incidentes y seguros cibernéticos.

[12] PAS = Especificación públicamente disponible n publicada por la Institución de Estándares Británica. CWA =Taller sobre el Acuerdo del Comité Europeo de Normalización. AIT = Taller sobre el Acuerdo Internacional.

La redundancia proporciona resistencia y es de vital importancia para eliminar los puntos únicos de falla o para reducir la vulnerabilidad al ataque de estos componentes críticos. Hay diferencias entre la independencia para edificios y puentes. Con frecuencia, para los puentes no hay sistemas redundantes, por lo tanto, la pérdida repentina podría causar un colapso progresivo. Un dueño de un activo debe endurecer los componentes críticos cuando el aislamiento adecuado no es posible.

Están disponibles varias herramientas de planificación y diseño. Algunos ejemplos se enumeran en la siguiente sección de este documento.

Es necesario impedir el acceso a las áreas internas como a las vigas tubulares y a las vigas curvadas y evitar la colocación de un dispositivo explosivo contra los elementos críticos (por ejemplo, bridas, cables y rodamientos). Tiene que haber medios para detectar si un área protegida ha sido violada de manera ilegal. Los rodamientos se pueden proteger con malla o valla y pequeños depósitos de servicios. Se pueden usar cubiertas sólidas para los candados. Se pueden crear zonas estériles usando cámaras de vigilancia con análisis de video o incidentes láser o sistemas de detección de intrusión y alarmas. Estos sistemas deben ser vigilados en la Sala de Control. Es importante evitar que vehículos sin revisar se estacionen bajo el puente o al lado de los muelles.

Las medidas blandas (patrullas locales, signos, enlace con la población local) pueden ser beneficiosas. Será necesaria la vigilancia especial de las infraestructuras críticas y es posible que se requiera una respuesta armada. Puede haber beneficios adicionales de reducción en otros delitos (por ejemplo robo de metales, delincuencia general, prevención de intrusión y vandalismo).

En la modificación a menudo es necesaria la implementación de redundancia, con enfoque en las medidas de mitigación de explosiones que pueden suponer amenazas múltiples.

La respuesta a la amenaza debe incluir una serie de medidas tales como cámaras (CCTV) y sistemas de detección de incidentes o de intrusión (IDS). Estos y otras medidas de detección y seguridad física deben integrarse para dar tiempo a la respuesta de la policía. Es necesario proteger elementos críticos tales como columnas, torres, cables, vigas y rodamientos. La pregunta que se tiene que hacer *"¿Cuál es una respuesta proporcionada para un activo de propiedad pública?"* Los temas principales a considerar son el tamaño del activo, importancia económica, relación con otras infraestructuras, ubicación, atributos específicos del sitio y las complejidades de los acuerdos de la propiedad y uso de la tierra. En muchos casos, el dueño del camino no controla la tierra debajo de sus activos. Hay una necesidad de un concepto claro de operaciones (ConOps) para todas las funciones de seguridad.

RECURSOS SOBRE SEGURIDAD DE LAS INFRAESTRUTURAS

Algunas referencias para abrir documentos de interés para el contenido del artículo antecedente.

[1] Informe de la NCHRP 525, volumen 15, *Costos de protección de activos: Una guía de todos los peligros para agencias de transporte*, Junta de Investigación sobre el Transporte, Washington, DC, 2009, *www.trb.org*

[2] CAPTOOL, Guía del usuario para CAPTA, USDOT Centro Volpe, de la Administración Federal de Carreteras del Departamento de Transporte de los Estados Unidos *http://www.fhwa.dot.gov/security/emergencymgmt/profcapacitybldg/documents.cfm fhwa.dot.gov*. Esta guía se actualizará con la nueva versión de CAPTA.

[3] Ray, James C., *Medidas de priorización de mitigación de amenazas terroristas en puentes*, Revista de Ingeniería de Puentes, ASCE/SEI, Vol. 12, número 2, marzo/abril de 2007. 12, No. 2, pp. 140-146).

[4] Informe de la NCHRP 645, Puentes de carretera resistentes a las explosiones. *Directrices de Diseño y Detalles*, Programa Nacional de Cooperación en la Investigación de Carreteras, Consejo de Transporte e Investigación, Washington, D.C., 2010.

[5] Marco de Cumplimiento TRANSEC (Reino Unido) *http://WebArchive.nationalarchives.gov.uk/20110504004554/http:/DFT.gov.uk/PGR/Security/abou t/transeccomframe*

[6] Proyecto europeo SERON (seguridad de redes de transporte vial) relativo a la identificación y designación de infraestructuras críticas europeas y a la evaluación de la necesidad de mejorar su protección *www.seron-project.eu*

[7] SKRIBT: dos programas alemanes para la evaluación de seguridad de la infraestructura (sólo en alemán) *http://www.skribt.org/*

[8] ESIMAS Programa alemán de investigación para el monitoreo en tiempo real de túneles de carretera *http://www.esimas.de/*

[9] SECMAN: Procesos de gestión de riesgos de seguridad para la infraestructura carretera *http://www.secman-Project.eu/*

[10] *AllTraIn: Guía de todo peligro para la infraestructura de transporte http://www.alltrain-Project.eu/*

[11] Keeny, Ralph L. 2005. *Valores modelo para el análisis de la lucha contra el terrorismo*. Durham: Fuqua School of Business, Universidad de Duke.

[12] Lewis, Ted G. 2006. *Protección de infraestructuras críticas en seguridad nacional (defensa de una nación en red)*. New Jersey: John Wiley & Sons, Inc.

[13] Martin, Gus. 2003. *Entender el terrorismo (retos, perspectivas y problemas)*. California: SAGE Publications, Inc.

[14] Mussington, David. 2002. Conceptos para mejorar la protección de infraestructuras críticas, como relacionar Y2K con investigación y desarrollo CIP. Santa Mónica: RAND.

[15] Radvanovsky, Robert. 2006. Infraestructuras críticas (seguridad nacional y preparación para emergencias). Nueva York: Taylor & Francis Group.

[16] Auerswald, Felipe., Branscomb, M. Lewis, La Porte, Todd M. de Michel-Kerjan, Erwann. 2005. *El reto de la protección de infraestructuras críticas. Centro de gestión de riesgos y procesos de decisión*, The Wharton School de Pennsylvania. Disponible en: *http://opim.wharton.upenn.edu/Risk/downloads/05-11-EMK.pdf*

[17] Burke, Ronald J. 2005. *Terrorismo internacional y las amenazas a la seguridad: implicaciones para las organizaciones y la administración. Prevención y manejo de desastres*, 14: 5. Disponible en: *http://www.emeraldinsight.com.nukweb.nuk.uni-lj.si/Insight/viewPDF.jsp?Filename=html/Output/Published/EmeraldAbstractOnlyArticle/Pdf/0730140502.pdf*

[18] Coaffee, J. in Wood, David M. 2006. *La seguridad viene a casa: Replanteamiento de la escala y la resistencia de la construcción en la respuesta urbana global al riesgo de ataques terroristas*.

[19] SAGE publicaciones, David Davies Memorial Institute para Estudios Internacionales

[20] Dall'Asta L., Barrat Alain., Barthelemy Marc en Vespignani Alessandro. 2006. *Vulnerabilidad de redes ponderadas*. Revista de Estadísticas en Mecánica: Teoría y experimento, abril de 2006 disponible en: *http://hal.archives-ouvertes.fr/ccsd-00021128/en*

[21] Fletcher, David R. 2002. *El papel de la tecnología geoespacial en protección de infraestructuras críticas de transporte: Una agenda de investigación*. Consorcio Nacional de teledetección en el transporte, ESTADOS UNIDOS Departamento de transporte. Disponible en: *http://www.ncgia.ucsb. edu/ncrst/Research.html*

[22] Latora Vito en Massimo Marchiori. 2006. Vulnerabilidad y protección de infraestructuras críticas. Disponible en: *http://arxiv.org/PS_cache/cond-mat/pdf/0407/0407491v1.pdf*

[23] Luiijf Eric A.M., Burger Helen H. en Marieke Klaver H.A. 2003. *Protección de infraestructuras críticas en los Países Bajos: Un análisis rápido*. Disponible en: *http://www.crypto.rub.de/ imperia/md/content/lectures/kritis/bpp_13_cip_luiijf_burger_klaver.pdf*

[24] Luego, Siaw K. en Loosemore, Martin. 2006. *Prevención del terrorismo, preparación y respuesta en las instalaciones construidas*. Sydney, Facultad del Entorno Construido, de la Universidad de Nueva Gales del Sur. Disponible en: *http://www.emeraldinsight.com.nukweb.nuk.uni-lj.si/Insight/viewPDF.jsp? Filename=html/Output/Published/EmeraldAbstractOnlyArticle/Pdf/0690240501.pdf*

[25] Alain Coursaget, SGNSN. 2010 en la revista francesa "Sécurité & Stratégie" n ° 4 de noviembre de 2010 y marzo de 2011 sobre la seguridad de actividades críticas *http://www.ladocumentation-francaise.fr/Ouvrages/1390900000002-la-Protection-des- Installations-vitales*

[26] OECD *Seguridad de los contenedores intermodales de transporte https://books.google.fr/books?id=tTXHR0UOUtEC&pg=PA97&dq=s%C3%BBret%C3%A9+des+transp orts+routiers&hl=fr&sa=X&ei=zCX4VM- aFoyrUd7JgJgN&ved=0CDoQ6AEwAQ#v=onepage&q=s%C3%BBret%C3%A9%20des%20transports%20routiers&f=false http://ebiz.turpin-distribution.com/products/191057-container-transport-security-across- modes.aspx*

[27] TRB y resiliencia: Un resumen de las actividades de la Junta de Investigación del Transporte *http://www.trb.org/main/blurbs/166648.aspx*,
CUMPLIMIENTO DE TRANSEC (REINO UNIDO)
El marco se ha archivado en los archivos nacionales en *http://webarchive.nationalarchives.gov.uk/20110504004554/* o *http://dft.gov.uk/pgr/security/about/transeccomframe*
La página de política actual, que detalla los resultados del Departamento de Seguridad *https://www.gov.uk/government/policies/managing-the-risk-to-transport-networks-from-terrorism-and-other-crimes* hace referencia al marco de cumplimiento que se archivó en 2011.
Se puede encontrar información más reciente de todos los modos de transporte en: *https://www.gov.uk/government/policies/managing-the-risk-to-transport-networks-from-terrorism-and-other-crimes/supporting-pages/land-transport-security*

Asociación mundial de la Carretera (AIPCR)
Tour Pascal B, 19e étage
92055 La Défense cedex, FRANCE
Número Internacional Normalizado para Libros (ISBN) 978-2-84060-364-1

Portada © Jurewicz, Fotolia