www.piarc.org
2019R12ES

SEGURIDAD DE LA INFRAESTRUCTURA VIAL

GRUPO DE ESTUDIO C.1. *SEGURIDAD DE LA INFRAESTRUCTURA*

WORLD ROAD ASSOCIATION
MONDIALE DE LA ROUTE
AIPCR PIARC

SOBRE LA ASOCIACIÓN MUNDIAL DE LA CARRETERA

La Asociación Mundial de la Carretera (AIPCR) es una organización sin fines de lucro establecida en 1909 para mejorar la cooperación internacional y fomentar el progreso en el ámbito de las carreteras y el transporte por carretera.

El estudio objeto del presente informe se definió en el Plan Estratégico de la AIPCR de 2016-2019 aprobado por el Consejo de la Asociación Mundial de la Carretera, integrado por representantes de los gobiernos nacionales miembros. Los miembros del Comité Técnico responsable de este informe fueron nominados por los gobiernos nacionales miembros debido a sus competencias especiales.

Las opiniones, resultados, conclusiones y recomendaciones expresadas en esta publicación son las de los autores y no reflejan necesariamente los puntos de vista de sus entidades o agencias matrices.

Este informe está disponible en la página web de la Asociación Mundial de la Carretera: http://www.piarc.org

Asociación Mundial de la Carretera (PIARC)
Arche Sud 5° niveau
92055 La Défense CEDEX, FRANCE

Número Internacional Normalizado para Libros (ISBN): 978-2-84060-526-3

Portada © Adobe Stock

SEGURIDAD DE LA INFRAESTRUCTURA VIAL

GRUPO DE ESTUDIO C.1. *SEGURIDAD DE LA INFRAESTRUCTURA*

AUTORES/ AGRADECIMIENTOS

Este informe ha sido elaborado por el Grupo de Estudio C.1 “Seguridad de la Infraestructura” de la Asociación Mundial de la Carretera, PIARC. La información incluida en este informe es correcta según el conocimiento de los autores, por lo que no aceptan responsabilidad por cualquier error u omisión.

El Grupo de Estudio C.1 fue presidido por Saverio PALCHETTI (Italia), mientras los miembros Philippe CHANARD (Francia), y Luz Angélica GRADILLA HERNÁNDEZ (México) fueron los secretarios de habla francesa e hispana, respectivamente.

Los otros miembros (M) y miembros corresponsales (MC) del Grupo de Estudio C.1, también colaboradores en la preparación de este informe, fueron desde el inicio del Grupo de Estudio los siguientes:

- *Johanne BANVILLE (Canadá -Quebec), (CM)*
- *Martha Elizabeth DE LA TORRE ROMERO (México), (CM)*
- *Asesor de Seguridad Gubernamental del Reino Unido, Centro para la Protección de la Infraestructura Nacional* (*Reino Unido*)*, (M)*
- *Vit HENDRYCH (República Checa), (M)*
- Petra HERRMANNOVA (*República Checa*), (M)
- Jürgen KRIEGER (*Alemania*), (M)
- Flavius PAVAL (*Rumania*), (M)
- Bine PENGAL (*Eslovenia*), (M)
- Ulli VIELHABER (*Austria*), (M)

Federica CAPUZZO, Giuseppe CARTOLANO (Italia) y Selcuk NISANCIOGLU (Alemania) se unieron al Grupo de Estudio, nombrados formalmente como miembros asociados (MA).

Los revisores de este informe fueron , Asesor de Seguridad Gubernamental del Reino Unido, *Centre for the Protection of National Infrastructure* (CPNI) (Reino Unido) para la versión en inglés, en colaboración con Alexandra LUCK (Reino Unido), Philippe CHANARD (Francia) para la versión en francés y Luz Angélica GRADILLA HERNANDEZ (México) para la versión en español, quién también realizó la traducción al español.

Sabato FUSCO de C.A.V. S.p.A (Italia) y Gianni CUOZZO de ASPISEC S.r.l. (Italia), participaron como expertos externos en el panel que se llevó a cabo en la última reunión, en Liubliana, el 20 de septiembre, 2018.

Jean-Francois CORTÉ (Francia) y Kirsten GRAF-LANDMANN (Alemania) fueron respectivamente el Coordinador Estratégico del Tema C “Seguridad” y la Asistente Técnica del Coordinador.

Marina GAITA y Daniela PASTORE, de la Secretaría del Comité Nacional Italiano PIARC, supervisaron la versión en inglés, así como la traducción al francés y al español.

RESUMEN EJECUTIVO

2019R12ES

SEGURIDAD DE LA INFRAESTRUCTURA VIAL

Al Grupo de Estudio (GE) C.1 de la PIARC se le asignó la tarea de enfocarse en:

- proveer un documento de alto nivel, que contribuyera a aumentar el conocimiento y la toma de conciencia entre los miembros de la PIARC sobre los temas de seguridad pública en el transporte, y particularmente en el transporte carretero;
- resaltar los temas clave, mantener la meta de dos años del Grupo de Estudio y dejar detalles de las complejidades para una fase futura del trabajo;
- analizar estudios de caso;
- recolectar mejores prácticas y metodologías efectivas para la administración de riesgos de seguridad pública.

Por lo tanto, el GE C.1 decidió concentrarse en "la seguridad de la infraestructura, de los bienes y de las personas transportadas". Dicha decisión se tomó con base en la experiencia de que, a pesar de la ocurrencia de incidentes que toman ventaja de la distribución y el diseño de la infraestructura carretera, cuyo objetivo es causar daño en áreas utilizadas por peatones, algunas Administraciones de Carreteras (de aquí en adelante referidas como AC) todavía están renuentes a responsabilizarse de embeber o integrar la seguridad pública, de manera cotidiana, en las etapas de diseño, construcción, operación y mantenimiento de su infraestructura.

Los participantes del GE C.1 PIARC fueron, principalmente, miembros de instituciones/asociaciones técnicas sobre carreteras o AC, y personas que trabajaron como administradores/operadores carreteros. Lo que representó un desafío, ya que el conocimiento sobre temas de seguridad pública dentro de dichas áreas puede variar significativamente y puede depender del país en el que los individuos trabajen

Este informe tiene como objetivo:

1) aumentar el conocimiento y la toma de conciencia, así como motivar a las AC para que tomen un rol más activo en la seguridad de su infraestructura, y
2) proveer de antecedentes teóricos concretos y de una metodología que ejemplifique cómo se puede embeber o integrar la seguridad pública.

Por lo tanto, se establecen:

- diferentes factores de la seguridad de la infraestructura
- consideraciones clave para la realización de una evaluación de riesgos de seguridad pública, con respecto a la resiliencia de los activos de la red carretera;
- ejemplos prácticos del proceso de evaluación del riesgo;
- recomendaciones para los dueños o administradores de la infraestructura carretera.

Como fue el caso del anterior Grupo de Estudio 2, PIARC (2014-2015), el GE C.1 desea nuevamente resaltar el problema de la confidencialidad en relación con la bibliografía, las referencias, así como el nivel de detalle de la información que puede incluirse en este tipo de documento. Ambas son limitantes del resultado que puede generarse para la comunidad de la PIARC.

Sin embargo, el GE C.1 cree que este informe cumplirá su misión de aumentar el conocimiento y toma de conciencia sobre los temas de seguridad pública en la comunidad de la PIARC y comunicará un mensaje clave: *"La capacidad de planificación, mitigación y prevención de la seguridad pública debe convertirse en una parte vital de la estructura organizativa de las AC modernas".*


SECURITY
VIRUS

INDICE

1. INTRODUCCIÓN

En la última década, han aumentado los ataques directos e intencionados contra los usuarios de la infraestructura y/o carga, con la intención explícita de interrumpir los flujos de transporte, dañar a los pasajeros y otros miembros del público, con un fin político o para obtener beneficios económicos a través de chantajes al país [1].

En 2016, una vez concluido el trabajo del anterior Grupo de Estudio 2 **[1]**, la PIARC le asignó a este Grupo de Estudio C.1 el tema de la seguridad de la infraestructura para la próxima misión de dos años. Durante este tiempo, varios eventos trágicos han tenido lugar en Europa y en el mundo, destacando la evolución de las nuevas amenazas a la infraestructura, los espacios públicos y la movilidad [2]. Algunos incidentes involuntarios también ocurrieron con las mismas consecuencias.

Este documento se ha preparado para mejorar el conocimiento y la toma de conciencia de una AC moderna respecto de estos problemas de seguridad pública, así como para facilitar su desarrollo y la implementación exitosa de enfoques personalizados para la gestión de los desafíos clave sobre seguridad pública. Los consejos que se incluyen en este documento están basados en las buenas prácticas alrededor del mundo y pueden ser utilizados por las AC que trabajan por cuenta propia o, idealmente, en colaboración con otras administraciones, propietarios de infraestructura, operadores y administradores – la mejor práctica común en el contexto de la PIARC.

Este informe está compuesto por once capítulos y siete apéndices:

El Capítulo 1 “Introducción",

El Capítulo 2, "Comprensión del tema" ofrece una descripción general del contexto de la seguridad de la infraestructura y la teoría, así como de la terminología específica utilizada en esta área.

El Capítulo 3, "El enfoque con mentalidad de seguridad pública", establece la necesidad y la aplicación rutinaria de medidas de seguridad apropiadas y adaptadas para disuadir y/o interrumpir conductas o actividades hostiles, maliciosas, fraudulentas y delictivas. Este enfoque es esencial para desarrollar un proceso sólido que permita abordar las cuestiones de seguridad pública.

El Capítulo 4, “Gestión de los riesgos de seguridad pública en la infraestructura carretera” describe la metodología para que una AC identifique la naturaleza y el nivel de los riesgos de seguridad que tiene su infraestructura.

---

[1] En este período, los ataques aéreos a las Torres Gemelas y la consiguiente catástrofe en Nueva York, el 11 de septiembre de 2001, fueron para muchos un punto de inflexión en el tema de la seguridad de la infraestructura.

[2] Vea como referencia los dos artículos propuestos en las reuniones de este Grupo de Trabajo. por Saverio Palchetti: “Introducción al terrorismo y la seguridad carretera” [2]; "Actualización desde principios de 2017: un informe periodístico" [3]. Se muestra que los actores políticos no estatales (asimétricos), en forma de cuerpos territoriales, han podido causar un daño enorme o un precio alto en términos de vidas humanas con relativamente pocos medios. Ver también [14] [15], ya que los artículos antes mencionadas fueron presentados también en algunas conferencias.

El Capítulo 5, "Desarrollo de medidas para mitigación los riesgos de seguridad pública", se centra en la mitigación de tres amenazas principales: vehículo hostil, ataque cibernético e infraestructura inteligente.

El Capítulo 6, “Resiliencia”, trata sobre la preparación y gestión de eventos no planificados e imprevistos con altas incertidumbres.
El Capítulo 7, “Estudios de caso”, proporciona escenarios de algunos tipos de ataques hostiles y otras acciones maliciosas.

El Capítulo 8, “Recomendaciones para las administraciones de carreteras”, establece las acciones clave que deben considerar las AC para responder ante las amenazas a la seguridad.

El Capítulo 9, “Conclusiones”.

El Capítulo 10, “Glosario y siglas”.

El Capítulo 11, “Referencias”.

2. COMPRENSIÓN DEL TEMA

2.1. EL CONTEXTO DE LA SEGURIDAD PÚBLICA

Existen numerosas consideraciones de seguridad pública en la gestión de la infraestructura, que surgen de su importancia estratégica, sus diferentes usos y su proximidad; y, por lo tanto, el acceso que puede proporcionar a otros activos y espacios públicos. Los desafíos pueden incluir todo, desde, pero no limitado a:

- la protección de personas muy importantes - VIP,
- la protección de espacios públicos, donde se congrega un número significativo de personas,
- la protección de activos clave de infraestructura;
- protección de los edificios que pueden ser un blanco debido a quién es el dueño u ocupación;
- la protección de activos de terceros que brindan servicios vitales para el funcionamiento de las sociedades modernas: por ejemplo, energía, comunicación y agua, y
- el suministro de transporte seguro de carga y pasajeros, en todos los modos de transporte (carretero, ferroviario, marítimo y aéreo).

En el contexto de la infraestructura, la movilidad es la capacidad de mover o moverse con facilidad y libertad; y, como tal, puede tener impactos económicos y sociales significativos. Una buena red de infraestructura, al facilitar el movimiento de bienes y personas, mejora el comercio y aumenta las posibilidades de que las personas no sólo alcancen una gama de oportunidades de educación, trabajo y atención médica, sino que también viajen por razones sociales. Por lo tanto, una interrupción significativa en parte de la red de la infraestructura puede tener consecuencias de gran alcance para los individuos, las comunidades, las empresas y, en última instancia, la economía de un área.

De todos los modos de transporte, el carretero y la red de carreteras de la que depende, es sin duda el más extendido en todo el mundo y, por lo tanto, tiene un papel muy importante en el suministro, el mantenimiento y la mejora de la movilidad.

El alcance del impacto de la pérdida o daño de una parte de dicha red carretera dependerá de la cantidad de resiliencia que tenga la parte relevante de la infraestructura y de la red, la importancia estratégica del área afectada, así como la naturaleza y el grado de pérdida o daño causado.

La escala y cobertura de la red carretera conlleva a que siempre sea susceptible de vandalismo y robo, así como verse afectada por actos como manifestaciones y desorden público. Además, su importancia estratégica y valor simbólico, la presencia de activos importantes como puentes y túneles donde se pueden causar daños significativos, y su proximidad a áreas donde hay un gran número de personas, también la convierte en un blanco atractivo para individuos o grupos extremistas. Otras partes de la infraestructura de transporte enfrentan desafíos similares por las mismas razones.

Además, la red carretera y la industria automotriz se encuentran al comienzo de un período de cambios significativos, a medida que se buscan soluciones tecnológicas innovadoras para mejorar la seguridad vial, el nivel de servicio, la sostenibilidad y la resistencia de la infraestructura. La forma en que se administran las redes y en que se utiliza el espacio carretero está evolucionando, con un mayor uso de la tecnología para monitorear las condiciones de la red y para administrar activamente el tráfico vehicular.

En la mayoría de los países, hasta hace poco, la protección de la movilidad de personas y bienes contra este tipo de amenazas estaba en el dominio de las fuerzas policiales, los servicios de

inteligencia, las aduanas y los servicios responsables del control de los bienes transportados, y no se percibía como una responsabilidad de quienes gestionan y operan la infraestructura. Sin embargo, las partes que poseen, son responsables o gestionan la infraestructura, tienen un papel cada vez más importante que desempeñar, en particular en relación con la mitigación y la planificación de incidentes.

La naturaleza cambiante del entorno de amenazas y el número creciente de vulnerabilidades potenciales, que surgen a través del uso cada vez mayor de las tecnologías digitales, incluyendo los sistemas ciber-físicos, conlleva a que más AC que nunca antes requieran considerar la seguridad de: sus activos construidos, los servicios que ofrecen, las personas y comunidades, y, los datos o información que poseen. Este es el caso, en particular, de los centros de control de túneles y de tráfico, que están embebidos en las redes de comunicación de TI, a través de diferentes interfaces. Los sistemas informáticos utilizados para la supervisión y el control deben protegerse adecuadamente contra el creciente riesgo de ciberataques.

La incorporación y gestión de la seguridad pública como parte de las actividades normales requiere recursos en forma de inversión financiera, pero lo más importante es la introducción de la gobernanza, la obligación y la responsabilidad en materia de seguridad pública, las nuevas políticas y procesos, así como la capacitación del personal, la concientización y los comportamientos orientados a la seguridad.

Además, es importante un enfoque colaborativo entre el gobierno, los propietarios de la infraestructura, los administradores y los operadores, reconociendo que los ataques pueden tener lugar utilizando, o facilitados por, más de un modo de transporte y cualquier otro medio que están bajo la responsabilidad de diferentes organizaciones.

2.2. SEGURIDAD VIAL (*SAFETY*) VS SEGURIDAD PÚBLICA (*SECURITY*)

La seguridad vial (*safety*), en el contexto del transporte, se define como la protección de la infraestructura de transporte contra eventos aleatorios, no intencionales, como accidentes, y es un tema cubierto con una serie de estándares a nivel mundial.

La seguridad pública (*security*) puede definirse como el estado relativo de estar libres de amenazas o daños causados por actos intencionales, no deseados, hostiles o maliciosos, incluidos el sabotaje y el espionaje.

En francés se tienen dos términos correspondientes: "sécurité" y "sûreté", pero en muchos idiomas sólo hay una palabra para la seguridad vial (*safety*) y la seguridad pública (*security)*. En alemán, por ejemplo, la palabra es "sicherheit", en español es "seguridad", y en italiano es "sicurezza".

Existe un traslape considerable entre los métodos de la seguridad vial y la seguridad pública, aunque el enfoque es diferente y, en algunos casos, los requerimientos de ambos pueden estar en conflicto. Teniendo esto en cuenta, es importante comprender las diferencias que existen entre los dos métodos: a la seguridad vial le atañe principalmente proteger al medio ambiente del sistema, mientras que a la seguridad pública le concierne proteger al sistema del medio ambiente. Esta diferencia de opinión explica uno de los contrastes clave entre los dos métodos - desde la perspectiva de la seguridad vial, la amenaza para el medio ambiente es el sistema y los sistemas son estáticos. Por el contrario, en el ámbito de la seguridad pública, la amenaza para el sistema

proviene del medio ambiente y éste último es dinámico. Esta importante diferencia de perspectiva es uno de los principales obstáculos para la integración de la seguridad vial y la seguridad pública.

Con los sistemas modernos que utilizan tecnología moderna, la seguridad vial y la seguridad pública están estrechamente entrelazadas y las clasificaciones de seguridad vial carecen potencialmente de sentido, a menos que estén acompañadas de algún tipo de evaluación de seguridad pública. De hecho, si un sistema moderno no es seguro (*secure*) o no está protegido, no debe considerarse seguro (*safe*). En última instancia, la industria de la seguridad vial necesita estar en una posición en la que si un sistema se considera seguro (*safe)*, entonces debería estar seguro (*secure*) o protegido por defecto.

La comprensión de la relación entre ambos tipos de seguridad es relevante en el contexto de la infraestructura carretera. Los sistemas de control y monitoreo para la seguridad vial se implementan para detectar las condiciones peligrosas y tomar medidas para prevenir peligros: típicamente, cerrar un túnel, un puente o una sección de una carretera, con el fin de evacuar a las personas. Por lo general, se proporcionan varios niveles de seguridad vial en los esquemas generales de protección de una estructura. Mientras que los sistemas de seguridad pública se refieren a la capacidad para proporcionar la confianza suficiente de que las personas y los sistemas no autorizados no pueden acceder a la estructura o infraestructura ni a las funciones del sistema para alterar o robar *software* o datos. Todo ello garantizando el acceso a personas o sistemas autorizados.

La protección o seguridad pública a menudo puede contribuir a la seguridad (*safety*) de la infraestructura, por ejemplo, la construcción de una seguridad pública adecuada en vehículos conectados y autónomos será crítico para que continúen operando de manera segura (*safely*), pero también puede ser contrario a ella. Mientras que puede ser deseable apagar un vehículo comprometido, que se mueve a través de la red, desde una perspectiva de la seguridad pública, se deben tener en cuenta las posibles implicaciones de la seguridad vial para los ocupantes y otros usuarios de las carreteras, así como para las personas y los activos en el entorno circundante.

En un túnel es necesario permitir la evacuación de conductores y pasajeros en el menor tiempo posible mediante salidas de emergencia. Al mismo tiempo, también es necesario tomar medidas para evitar que estas salidas se utilicen para acceder a la infraestructura para realizar acciones maliciosas como las que causan daños o incidentes/accidentes.

Hasta hace poco, las disciplinas de ingeniería de seguridad vial y diseño de la seguridad pública se encontraban efectivamente en caminos separados, pero paralelos. Los estándares de seguridad vial y las prácticas de trabajo de ingeniería asociadas están maduras y bien establecidas, basadas en décadas de aprendizaje. Por otro lado, el diseño de la seguridad pública es un campo mucho más nuevo y tiene sus raíces en los enfoques de tipo militar aplicados al mundo civil.

Otro aspecto es que los riesgos de seguridad vial están menos sujetos a cambios que los riesgos de seguridad pública. La seguridad vial puede estar totalmente regulada por las leyes nacionales, mientras que la seguridad pública necesita una estrategia corporativa, un enfoque con mentalidad de seguridad. La incorporación y gestión de la seguridad pública como parte de las actividades normales requiere recursos en forma de inversión financiera, pero lo más importante es la introducción de la gobernanza, la rendición de cuentas y la responsabilidad en materia de

seguridad, las nuevas políticas y procesos, así como la capacitación del personal, la concientización y los comportamientos con mentalidad de seguridad.

Es comprensible que la seguridad pública pueda considerarse como un costo adicional a la seguridad vial, tanto en términos financieros como de tiempo, que ya se ven amenazadas por el mantenimiento de extensas redes de carreteras y activos asociados que pueden incluir infraestructura compleja como túneles y puentes. En esta perspectiva, un primer acercamiento a las medidas de seguridad pública puede obtenerse mediante un uso inteligente de las medidas de seguridad vial, que ya se han implementado (por ejemplo, en la recopilación y procesamiento de datos en los centros de control).

En caso de un incidente, el hecho de no comprender tanto la gama de riesgos de seguridad pública existentes como la implementación de las medidas apropiadas y adaptadas para mitigar aquellos riesgos que son inaceptablemente altos, los usuarios de la infraestructura pueden verse afectados y las áreas circundantes, así como la infraestructura en sí misma y los numerosos servicios que dependen de ella. También pueden ocasionar daños financieros y de reputación a la AC, además de tener un impacto social y económico más amplio.

2.3. El concepto de resiliencia

El hecho de que ocurran incidentes, ya sean naturales, accidentales o malintencionados, es inevitable y, en algunos casos, impredecible.

Un enfoque adecuado para la gestión de los riesgos de seguridad pública debe considerar qué tan críticas son las diferentes partes de la infraestructura para mantener la prestación de servicios y otras actividades que son esenciales para conservar el bienestar económico y social de las comunidades, regiones o potencialmente de un país en su conjunto.

La velocidad a la que se lleve a cabo la recuperación dependerá de los planes que se implementen de antemano, su ejecución en el momento del incidente y la honestidad con la que se realizan las revisiones posteriores.

Por lo tanto, además del enfoque tradicional de análisis de riesgos, los enfoques basados en el concepto de resiliencia a menudo se utilizan para eventos no planificados e imprevistos, con grandes incertidumbres. Paralelamente a las consideraciones tradicionales de análisis de riesgos, también se deben tener en cuenta las actividades de la planificación y preparación ante los eventos, así como la fase muy importante de recuperación de la infraestructura carretera, es decir, hasta que se restablezca el rendimiento total del sistema.

Más adelante en el informe, se explican con más detalle los conceptos de la resiliencia y de la gestión de la resiliencia en la infraestructura carretera.

2.4. Las tecnologías digitales en la Ingeniería Civil

El uso de las tecnologías digitales a lo largo del ciclo de vida de los activos se convertirá en un contribuyente cada vez más importante para el cumplimiento de los objetivos fiscales, funcionales, de sostenibilidad y de crecimiento. La implementación del estándar de Modelado de Información para la Construcción (BIM, por sus siglas en inglés) **[4]** ya es habitual en el diseño y la construcción de grandes proyectos de infraestructura, en algunos países. Este concepto se abordará más adelante y en las recomendaciones finales (ver capítulo 7). Al usar una combinación de sensores y

actuadores, estos sistemas pueden capturar datos en tiempo real sobre el uso y la condición de los activos para lograr beneficios tales como: aumentos en la eficiencia energética y una mejor gestión del ciclo de vida de los activos. Estos sistemas ya se pueden encontrar en cierta infraestructura de transporte, de servicios públicos y de otro tipo. A largo plazo, estos interactuarán como ambientes ciber-físicos integrados, por ejemplo, en el desarrollo de comunidades inteligentes.

Comprometer los sistemas ciber-físicos puede dañar, o comprometer, los activos físicos y, por lo tanto, dañar potencialmente a los ciudadanos. Además, los ataques ciber-físicos son más baratos y menos riesgosos para los atacantes, no están limitados por la distancia y son más fáciles de alinear y coordinar entre ellos.

El mayor uso y dependencia de estos sistemas y tecnologías de información, comunicaciones y operaciones, en el medio construido, significa que existe una necesidad real de abordar los problemas de vulnerabilidad inherentes y, por lo tanto, las implicaciones de seguridad pública que surgen. Estas implicaciones de seguridad pública pueden estar relacionadas con la infraestructura en sí misma, los entornos a través de los cuales pasa, los servicios que facilita la infraestructura, los individuos y las comunidades, así como los datos e información.

3. EL ENFOQUE CON MENTALIDAD DE SEGURIDAD PÚBLICA

Para que la seguridad pública se convierta en una práctica habitual, es esencial que sea capaz de actuar como facilitador en lugar de ser percibida o utilizada como un obstáculo para la adopción de otras buenas prácticas, operaciones diarias, tecnologías o innovación.

Un enfoque con mentalidad de seguridad pública se define como la comprensión de la necesidad y la aplicación rutinaria de medidas de seguridad pública apropiadas y adaptadas para disuadir y/o interrumpir conductas o actividades hostiles, maliciosas, fraudulentas y criminales[3]. Por lo tanto, las AC necesitan entender las amenazas y los problemas de vulnerabilidad claves, así como la naturaleza de los controles necesarios para administrar los riesgos resultantes, llevándolos a un nivel que sea tolerable.

Las amenazas incluyen el terrorismo, las acciones hostiles por parte de los estados nacionales, el espionaje comercial, el crimen organizado, los activistas, los actores solitarios, los hackers y el personal malintencionado. Los actores de amenazas asociados con estos pueden tratar de hacer uso de las vulnerabilidades para: comprometer el valor, la longevidad y el uso continuo de los activos y/o servicios de la organización; causar daño, herir, angustiar o comprometer al personal de la organización u otros usuarios del activo o servicio; obtener, interrumpir o corromper datos, información y/o sistemas; y/o causar daño a la reputación.

Es esencial aplicar contramedidas adecuadas para cada uno de los riesgos potenciales identificados, ya que las medidas son realistas, apropiadas, rentables y acordes con el apetito de riesgo de la organización. Una organización siempre tendrá que asumir un nivel de riesgo, pero la capacidad que tenga para hacerlo dependerá del impacto que una violación o incidente de seguridad pueda tener en la organización y en las partes interesadas de la misma, que resulte en la pérdida, el daño o la falla de un activo.

Además, para que sean efectivas, las medidas de mitigación de riesgos de seguridad pública deben ser holísticas e incluir:

- *la gobernanza* con líneas claras de responsabilidad y compromiso;
- *la seguridad del personal* – teniendo en cuenta la competencia en materia de seguridad del personal, los requisitos de detección y verificación de la seguridad pública, la inducción, la capacitación y la desmovilización;
- *la seguridad física* – proporciona el nivel necesario de protección física de los activos críticos u otros sitios de interés para personas que tengan intenciones maliciosas, así como en ubicaciones donde se almacenan datos e información confidenciales;
- *la ciberseguridad* – incluye la provisión de suficiente seguridad en torno a los sistemas en donde se recopilan, procesan y almacenan datos e información, así como en las interconexiones e interacciones entre ellos, así como la garantía de la seguridad adecuada, en particular, en los sistemas ciber-físicos relacionados con la seguridad vial.

[3] Probablemente nunca ocurra un ataque terrorista perturbador, sin embargo, un enfoque orientado a la seguridad pública, con el que se cultive una mentalidad y cultura apropiadas, es capaz de proporcionar una mayor capacidad para proteger los activos de un accidente o de un incidente menor malicioso.

Además, tanto el personal como los miembros de cualquier cadena de suministro deben conocer y comprender las políticas de seguridad pública vigentes y ser capaces de implementarlas de manera simple y eficiente – si son demasiado onerosas, existe el peligro real de que, con el tiempo, las medidas puestas en marcha para gestionar los riesgos de seguridad pública sean ignoradas o burladas.

Mediante la integración de la seguridad del personal, física y cibernética con la seguridad de la información, la buena gobernanza, la responsabilidad y la rendición de cuentas, es posible crear un enfoque de la seguridad de la red de infraestructura carretera que ofrezca:

- *seguridad (safety)* – evitar la creación de situaciones dañinas que pueden provocar lesiones o la muerte, o daños ambientales no intencionales;
- *autenticidad* – garantizar que las entradas y salidas sean auténticas y que no se hayan producido alteraciones;
- *disponibilidad (incluida la confiabilidad)* – garantizar la accesibilidad y disponibilidad de la infraestructura carretera de manera adecuada y oportuna;
- *confidencialidad* – garantizar el control del acceso y la prevención del acceso no autorizado tanto al activo físico como a la información;
- *integridad* – mantener la consistencia, coherencia y configuración de la infraestructura y los sistemas carreteros;
- *posesión* – evitar el control no autorizado, la manipulación o la interferencia en las instalaciones y los servicios;
- *resiliencia* – garantizar la capacidad de transformar, renovar y recuperar el servicio de manera oportuna, en respuesta a eventos adversos; y
- *servicio* – garantizar la disponibilidad y el servicio, a lo largo del tiempo, de activos, datos, información y sistemas.

En PAS 1192-5 **[5]** está disponible más información sobre el enfoque de seguridad pública, en particular en relación con el diseño, la construcción, la operación y el mantenimiento de activos, dicha información se puede descargar de forma gratuita desde el sitio web del *British Standards Institute.*

4. GESTIÓN DE LOS RIESGOS DE SEGURIDAD PÚBLICA EN LA INFRAESTRUCTURA CARRETERA

El desarrollo de un enfoque conjunto, apropiado y adaptado para gestionar los riesgos de seguridad de la infraestructura se basa en[4]:

- *Establecer el contexto (estratégico, organizativo).*
- *Identificar los riesgos (amenazas, vulnerabilidades, criticidades) (sección 4.1) mediante:*
  - *el entendimiento del alcance de las amenazas existentes y la capacidad de los diferentes actores de amenazas, tanto actualmente como a lo largo de la vida útil de los activos de infraestructura;*
  - *comprensión de las vulnerabilidades y criticidades actuales y en evolución, que los diferentes actores de amenazas pueden tratar de aprovechar;*
- *Valorar los riesgos (probabilidad, consecuencias) (secciones, 4.1, 4.3 y 4.4), la naturaleza de las consecuencias que los actores de amenazas podrían provocar al aprovechar las vulnerabilidades y la probabilidad de que un actor de amenazas logre con éxito sacar provecho de una vulnerabilidad o varias vulnerabilidades para generar un impacto.*
- *Evaluar riesgos (aceptabilidad de la tolerancia). Comprender el apetito de riesgo de una organización individual- su capacidad para aceptar el riesgo - y, cuando se está desarrollando un enfoque colaborativo, el apetito de riesgo de las organizaciones colectivas.*
- *Entender la interdependencia con otros sectores (energía, agua, comunicación).*
- *Atender los riesgos (evitar, compartir, aprovechar, aceptar, usar) mediante el desarrollo y la evaluación de la gama de medidas de mitigación de riesgos potenciales; determinar qué medidas de mitigación, si las hay, se pondrán en marcha; desarrollar los medios por los cuales esas medidas de mitigación pueden ser implementadas consistentemente así como desarrollar procesos efectivos de monitoreo, auditoría y revisión.*

4.1. AMENAZAS

Las amenazas a la seguridad pública se pueden dividir en aquellas que:

- *tienen la capacidad de causar daño o interrupciones en la construcción, operación o mantenimiento de la infraestructura física y dañar al personal que ahí labora;*
- *podrían dañar o interrumpir los sistemas operativos de la infraestructura y la información asociada (la infraestructura de los Sistemas Inteligentes de Transporte).*

Las amenazas también pueden ser involuntarias, no dirigidas o imprevistas, por ejemplo:

- *pandemias;*
- *incidentes relacionados con materiales peligrosos;*
- *colisiones de tránsito en la carretera;*
- *afectación a otros modos de transporte debido a una interrupción;*
- *la interferencia de las señales de navegación causadas por factores naturales;*
- *infección a un Sistema Inteligente de Transporte a través de un malware.*

Además del funcionamiento normal de las redes carreteras, que se centra principalmente en aspectos de preservación, mantenimiento, reparación, rehabilitación y modernización, surgirán desafíos futuros para los propietarios y operadores de la infraestructura carretera. Estos incluyen:

- ***infraestructura envejecida**, que se encuentren en buen estado de conservación (especialmente puentes y otras obras de ingeniería),*

[4] HB167:2006: Security Risk Management, Standards Australia/Standards New Zealand, ISBN 0 7337 7899 2 **[6]**

- ***el cambio climático y los fenómenos meteorológicos extremos*** *(p. ej., lluvias intensas, tormentas, olas de calor),*
- ***desastres naturales*** *(p. ej., deslizamientos de tierra, inundaciones, daños por tormentas, incendios forestales, terremotos).*

El nivel potencial de impacto dependerá de qué tan crítico sea el activo, el sistema o la información en cuestión.

A continuación, en la **Tabla 1** se presentan algunos de los tipos de ataques potenciales por parte de diferentes actores de amenazas, así como el rango de posibles consecuencias para la infraestructura de las AC y los usuarios de la carretera. También deberían considerarse las consecuencias más amplias para otros miembros del público, empresas y otros servicios.

En esta sección distinguimos:

- ***Amenazas físicas intencionales*** (p. ej., ataques terroristas con explosiones, incendios, impactos mecánicos, contaminación, accidentes severos con o sin la participación de mercancías peligrosas),
- ***Amenazas cibernéticas y ciber-físicas*** (p. ej., a centros de control de túneles y tráfico).

Amenaza	Tipo de ataque	Medios de ataque	Evento inicial	Consecuencias para la infraestructura y los usuarios
TERRORISMO - ACCIÓN HOSTIL POR UN ESTADO-NACIÓN - CRIMINALIDAD - ACCIÓN MALICIOSA POR OTRO TIPO DE ACTOR DE AMENAZAS	**EXPLOSIÓN**	Radioactiva	Dispositivo de dispersión radiológica (RDD, por sus siglas en inglés) – bomba sucia	Dispersión alfa, evacuación del área, perímetro de zona roja, descontaminación
		Convencional	Explosión pequeña	Exceso de presión causada por una onda expansiva, dispersión potencial; mayor afectación dentro de los túneles y sobre puentes
			Explosión mediana	
			Explosión mayor	
	FUEGO	Sin liberación de material peligroso	Fuego de un vehículo (5 MW)	Generación de calor y humo.
			Fuego de un camión (30 MW)	
			Fuego mayor (100 MW)	Destrucción de equipo, efectos en los usuarios
		Con liberación de material peligroso	Fuego mayor (>100 MW)	Liberación de gases tóxicos (plásticos)
	IMPACTO MECÁNICO	Colisión	Impacto vehicular dentro de una infraestructura	Daños o destrucción de la pared del túnel o del portal.
			Impacto vehicular hacia una infraestructura	Daños en pilares del puente, elementos estructurales, cables.
		Proyectiles	Impacto de un proyectil sobre una infraestructura	Daños o destrucción causada por un proyectil explosivo o por los fragmentos de una explosión.
	CONTAMINACIÓN	Radioactiva	Se arroja material radioactivo	Impacto en el usuario y sobre los servicios de rescate, mayor afectación en los sistemas de ventilación, túneles, área urbana.
		Biológica	Virus	
			Bacteria	
			Rickettsia	
			Esporas	
		Química	Se arrojan sustancias químicas	
	CIBERNÉTICO	Interna y externa (en internet, www)	Infiltración con *malware*	Interrupción de sistemas de control y monitoreo; en los equipos; propagación de la sensación de inseguridad entre la población.
			Substracción de información a través del secuestro (*ransomware*)	Interrupción y el cese del servicio; desalojo y efectos en cascada.
			Manipulación directa	Incremento de riesgo de accidentes; mayor afectación en: centros de control de tráfico, túneles y puentes, vehículos modernos, carreteras inteligentes.

Tabla 1: Amenazas de seguridad pública y sus posibles consecuencias

4.1.1. Amenazas físicas llevadas a cabo por el hombre

En la actualidad, el terrorismo es de hecho uno de los factores motivacionales más debatidos para los actos violentos hacia otras personas. Sin embargo, no todo ataque al transporte y/u otra infraestructura está relacionado con el terrorismo.

Hoy en día, después de los trágicos eventos de los años recientes con numerosas víctimas, gracias a las medidas preventivas adoptadas por muchos gobiernos en todo el mundo, la mayoría de los terroristas sólo pueden utilizar medios al alcance de la mano (vehículos como un arma, un cilindro de gas o drones básicos, cuchillos u otras armas en un vehículo). A pesar de ello, hoy en día siguen siendo una amenaza clave, ya que las organizaciones terroristas siguen activas en algunos territorios nacionales.

Además del terrorismo y los ciberataques, el daño o la interrupción de la construcción, operación o mantenimiento de la infraestructura carretera pueden provocarse a partir de:

- *ataques maliciosos;*
- *robo de equipo;*
- *materiales peligrosos;*
- *afectación a otros modos de transporte debido a una interrupción;*
- *interrupción de los sistemas de navegación global;*
- *protestas civiles y huelgas.*

Un **ataque malicioso** puede ocurrir a través de una variedad de amenazas externas e internas. Éstas incluyen daños causados por *malware*, hackers o personas descontentas. Es probable que el resultado de un ataque, durante la construcción, operación y mantenimiento de la red carretera, se centre en daños físicos o sabotaje a la infraestructura, planta o equipo, o bloqueo a los usuarios de la carretera.

Dependiendo del **tipo de equipo**, el robo puede impactar directamente en las operaciones del tráfico vehicular y en la capacidad de una autoridad para construir, mantener y mejorar la infraestructura de transporte, así como el costo para ello. También puede influir directamente en la seguridad vial de los usuarios de la carretera y en la capacidad de una autoridad para gestionar el comportamiento del tráfico y mejorar la capacidad de una red.

La diseminación de materiales peligrosos (sólidos, líquidos y gases que pueden ser inflamables, corrosivos o tóxicos), que con frecuencia se transportan por carretera. También se usan para la construcción y administración de carreteras, y pueden almacenarse, procesarse o usarse en áreas adyacentes a la red de carreteras (o en las proximidades). Un incidente que involucre materiales peligrosos puede provocar el cierre de la carretera o daños a la misma y a sus sistemas de soporte.

El bloqueo (*jamming*), o la interferencia, de las **señales de navegación** pueden ser causados por actos o ataques maliciosos y esto puede dar lugar a la pérdida de precisión de la información de ubicación, el fallo de los sistemas de navegación a bordo de los vehículos y/o la pérdida de señales precisas para los sistemas de toda la zona.

Es más probable que **las protestas civiles y las huelgas** surjan de la inestabilidad social y la desobediencia civil. Algunas veces, éstas se dan en respuesta a la construcción de activos que son sensibles por razones ambientales, sociales, económicas o políticas. Las mismas tienen el potencial de interrumpir o retrasar las operaciones y pueden ser costosas de gestionar.

Además, la red carretera contiene una gama de **activos de servicios públicos de terceros**, como telecomunicaciones, cables de electricidad, tuberías de gas y agua, etc., que pueden convertirse en objetivos de un ataque. Si bien no forman parte de la infraestructura carretera en sí misma, un ataque afectaría la red carretera en la que están enterrados.
Otros tipos de ataques intencionales son:

- *intimidación, insultos, fraude, interrupción del servicio público;*
- *desinformación (rumores, engaños, publicidad maliciosa, divulgación de datos confidenciales);*
- *vandalismo, daño intencional (en vehículos, equipos o edificios);*
- *tráfico ilícito de mercancías, tráfico de personas, secuestro;*
- *robo de cualquier tipo, piratería (carga, equipo, materiales que se tienen en el sitio, etc.);*
- *colisiones intencionales de vehículos y choques destructivos intencionales;*
- *ataque a edificios operativos (garajes y bodegas, generadores, almacén de fluidos); y*
- *ataque a sistemas de información (centros operativos, lugares de almacenamiento, sistemas de peajes de autopistas).*

Además, se puede esperar que el entorno general de las amenazas parezca moverse: [5]

- *de fuentes conocidas a más desconocidas,*
- *de físico a cibernético y/o ciber-físico,*
- *de lo esperado a lo inesperado, y*
- *de menos a más severo.*

4.1.1.1 Vehículos hostiles

Las amenazas van desde vandalismo hasta ataques sofisticados o agresivos, llevados a cabo por determinados delincuentes o terroristas, dándose dos casos en los cuales se usa:

- un vehículo que entrega una bomba, conocido como un dispositivo explosivo improvisado instalado en un vehículo (VBIED, por sus siglas en inglés),
- un vehículo que se usa como arma para chocar contra la infraestructura y dañarla o para herir o matar a personas (VAAW, por sus siglas en inglés).

Dispositivo explosivo improvisado instalado en un vehículo (VBIED).

Parte de la infraestructura de la AC, por ejemplo, un puente o túnel, puede ser el objetivo de este tipo de ataque. Sin embargo, cuando el ataque se dirige contra un activo de terceros o una comunidad, es muy probable que la red de carreteras se utilice como un medio para facilitar dicho ataque y pueda sufrir daños si el ataque tiene éxito, pero no es el objetivo en sí.

Los efectos de un VBIED incluyen la explosión, la bola de fuego, la fragmentación primaria y secundaria, así como el choque en tierra. La separación de explosiones (la distancia entre el explosivo y el activo) es el factor más importante para determinar el alcance del daño que puede causarse y, por lo tanto, es importante maximizar esta distancia.

Hay cinco principales tipos de ataque cuando se usa un VBIED:

- **estacionado:** un VBIED puede estacionarse cerca de un activo que es el objetivo del terrorista. Los efectos de la explosión son mucho mayores cuando el VBIED está cerca del activo.

[5] Contestabile, J.; Radow, L.: Resilience Thinking and Future Research: Beyond Quick Fixes; TR News Número 311, Septiembre-Octubre 2017, pp. 33-39.

- **invasión:** un vehículo hostil puede aprovechar los huecos en la protección perimetral, o seguir a un vehículo legítimo a través de un Punto de Control de Acceso de Vehículos (VACP, por sus siglas en inglés) de una sola capa. Alternativamente, antes de un ataque se puede manipular una barrera vehicular de seguridad para abrirla posteriormente con el vehículo hostil.
- **penetración:** un vehículo puede ser utilizado para debilitar y/o destruir un edificio o perímetro físico. Un ataque de penetración podría provocar que un dispositivo explosivo improvisado (IED, por sus siglas en inglés) detonara dentro de una estructura debilitada.
- **engaño:** un vehículo hostil puede ser modificado para replicar un vehículo legítimo (es decir, un vehículo "caballo de Troya"), ya que un vehículo de la antigua flota o el/los ocupante(s) de un vehículo pueden usar un pretexto para obtener acceso al sitio.
- **coacción:** un oficial de seguridad podría verse obligado a abrir un punto de control de acceso del vehículo (VACP) o un conductor legítimo podría verse obligado a llevar un IED dentro de su vehículo a una ubicación vulnerable.

Otros métodos de ataque con un VBIED pueden ser una combinación de los anteriores para acercar un VBIED al objetivo de un terrorista; esto se conoce como un ataque por capas.

Vehículo como arma (VAAW)

Un vehículo por sí mismo puede ser utilizado con intenciones hostiles para violar un perímetro, chocar fuertemente contra la infraestructura y dañarla, o como un arma para herir o matar a personas. Esto se conoce como un ataque de "vehículo como arma". En años recientes, el VAAW ha sido utilizado por terroristas para atacar lugares muy concurridos. Una amplia gama de vehículos puede causar importantes pérdidas de vidas y lesiones graves.

4.1.1.2 Centros de gestión de tráfico

Los Centros de Gestión de Tráfico (CGT) representan una parte vital de la actual gestión del tráfico vehicular. Son los nodos y puntos de conexión de la información y pueden controlar eficazmente los flujos de transporte en las carreteras. El mal funcionamiento de un CGT puede causar serias interrupciones en el transporte y, por lo tanto, no es de extrañar que se reconozcan a los CGT como un riesgo para la seguridad pública en las redes de transporte en todo el mundo.

Hay una serie de amenazas a un CGT que deben tenerse en cuenta al tratar de garantizar su protección y resiliencia frente a un posible ataque. Teniendo en cuenta que el daño principal que se puede hacer, con los medios disponibles, es a través del software de información, lo más probable es que el objetivo final de un atacante sea interrumpir la gestión del transporte. En general, podemos distinguir dos tipos de posibles ataques al CGT:

- *Ataque físico,* y
- *Al software o ciberataque*.

La mayoría de las AC se enfocan naturalmente en proteger el sistema de un ataque al software o ciberataque, y no en la seguridad física del edificio en sí. Como en otros capítulos de este informe se analizan más a fondo las amenazas y las contramedidas de los ataques cibernéticos, en este momento no abordaremos más esta cuestión. Aquí nos centramos en la protección física del edificio.

Cuando hablamos de un ataque físico, tenemos en mente un ataque directo y violento con medios físicos, que se lleva a cabo para acceder a los componentes de software del CGT. Podemos distinguir cuatro escenarios posibles de un ataque físico a un CGT o a sus componentes/equipos:

- **La intrusión física** y toma de control físico del CGT, incluyendo del equipo que se va a aprovechar para un ataque cibernético en la segunda fase del ataque.
- **Atacar y tomar el control de las líneas o cables eléctricos y de otro tipo**, que permiten el funcionamiento del CGT, fuera del perímetro de un CGT - es decir, tomar el control del CGT desde el exterior y desconectar el centro.
- **Ataque físico con explosivos y otras armas** con el objetivo de destruir o dañar el CGT, junto con su equipo para ponerlo fuera de servicio.
- **Vandalismo (intrusión física y/o daño al equipo)** con el objetivo de dañar el equipo del centro sin tener como objetivo interrumpir los flujos de tráfico vehicular.

Intrusión física

Exploremos la opción de un ataque de dos fases en el CGT con el objetivo final de interrumpir los flujos del tráfico vehicular a través del equipo del CGT. La primera fase de un ataque probablemente se llevaría a cabo como una intrusión típica en el edificio y en las instalaciones internas. Como los CGT generalmente funcionan las 24 horas del día, los 7 días de la semana, el momento más adecuado para una intrusión sería en la noche, cuando hay menos personas en el edificio. Normalmente, para este tipo de edificios, no hay protección física especial, por lo que una intrusión nocturna no exigiría un alto grado de fuerza física para ingresar al edificio. Un equipo muy versado también sabría cómo desactivar las cámaras de seguridad y el sistema de alarma, por lo que ningún equipo de respuesta de una compañía de seguridad podría intervenir en principio. La segunda fase de tal intrusión consistiría en tomar el control del sistema de información en el CGT y empezar a reprogramar ciertas características del sistema de gestión de tráfico vehicular. Si se buscara un beneficio económico, en forma de chantaje, probablemente habría una llamada para pedir rescate, posteriormente.

Atacar y tomar el control de las líneas/cables eléctricos y de otro tipo.

Aquí se presenta otro tipo de ataque físico, que también puede ser un ataque en dos fases. El objetivo principal de este ataque es tomar el control del sistema de gestión del tráfico vehicular desde el exterior del CGT y, al mismo tiempo, cortar físicamente la alimentación y las conexiones del CGT. La primera fase de tal ataque probablemente se llevaría a cabo como una operación encubierta de mantenimiento, en algún lugar del perímetro exterior del CGT. Los atacantes primero necesitarían tener acceso a un mapa detallado de los cables eléctricos, ópticos y otros cables/líneas que van hacia el CGT o salen de éste, y luego determinar la ubicación correcta donde se necesitarían cortar o interceptar. Dado que las conexiones suelen ser subterráneas, la operación implicaría probablemente la utilización de equipos de construcción y maquinaria más pesada para crear una "zona de trabajo" temporal con el fin de no atraer demasiado la atención del público. Necesitarían un equipo de hardware y software muy bueno para poder conectarse al sistema desde el exterior del CGT (donde sea posible) y tomar el control del mismo. En la segunda fase cortarían la energía y las conexiones al CGT, y luego hackearían el sistema ellos mismos. Este tipo de ataque probablemente también implicaría un chantaje con fines de lucro.

Ataque físico con explosivos y otras armas.

Este es un "ataque de una fase" y se lleva a cabo con la intención de dañar al CGT tanto como sea posible, por lo menos para dejarlo fuera de servicio por algún tiempo. El equipo de asalto probablemente llegue por la noche cuando haya menos personas en el edificio y se requiera menos fuerza para ingresar y tomar el control de las instalaciones del CGT. En este caso, se centrarían en infligir el mayor daño posible al equipo del CGT. Probablemente se centrarían en destruir el hardware pero, en el peor de los escenarios, podrían decidir instalar explosivos para destruir físicamente el edificio y derribarlo. Posiblemente, su intención principal sería ganar suficiente tiempo antes de que se avise a la policía sobre la situación, con el fin de colocar los explosivos y escapar, permitiendo que la explosión se active de forma remota. Este ataque también puede combinarse con una petición de rescate, una vez que se hayan instalado los explosivos.

Vandalismo (intrusión física y/o daño al equipo).

Este tipo de ataque físico es tal vez el más probable, pero tiene las consecuencias menos severas. Suele ser realizado por individuos más jóvenes o grupos más pequeños que no tienen una agenda más seria con esta acción. Los actos de vandalismo probablemente también se llevarán a cabo durante la noche y, en casos menos graves, sólo afectarán al exterior de los perímetros del CGT, dañando el equipo exterior sin obstaculizar realmente el propio sistema de gestión del tráfico vehicular. Por otro lado, en un caso más grave, podrían orientarse hacia el equipamiento interior del CGT. En esas circunstancias, también incluiría la intrusión en el edificio y, a continuación, el daño o el robo de piezas de equipo. Dado que el CGT funciona las 24 horas del día, los 7 días de la semana, casi no hay posibilidad de que el edificio esté totalmente vacío y es probable que el personal llame a la policía o a los servicios de seguridad con bastante rapidez, en caso de que se produzca un ataque no encubierto. Por lo tanto, es probable que la situación se resuelva rápidamente y no suponga una amenaza adicional para el entorno cercano o para la gestión del tráfico vehicular. En el vandalismo generalmente no hay demanda de rescate de ningún tipo, por lo que se puede esperar que las consecuencias económicas sean mínimas en comparación con otros tipos de ataques físicos mencionados anteriormente.

4.1.2. Ciberamenazas y amenazas ciber-físicas

La información detallada sobre los ataques de ciberseguridad no está disponible debido a la renuencia de las organizaciones a proporcionar información que se considera sensible para su reputación. Algunos esfuerzos de investigación sobre ataques de ciberseguridad a los transportes se han llevado a cabo desde principios de los años ochenta. En el trabajo del Proyecto Chariot de la Unión Europea[6] sobre monitoreo de la seguridad de las redes, se enumeran algunos ataques de ciberseguridad a los transportes que muestran cómo están en constante crecimiento, mostrando una descripción de tipologías, metodologías y daños.

A continuación, se enumeran las principales amenazas y los actores de amenazas que dan lugar a los ciberataques, donde los actores pueden ser desde "script kiddies" hasta hackers privados

[6] Chariot Project – Cognitive Heterogeneous Architecture for Industrial IoT - Deliverable 1.4 CHARIOT Design Method and Support Tools, with funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 780075, ver https://www.chariotproject.eu

altamente profesionales y Estados extranjeros hostiles, en particular servicios de inteligencia, que involucran a hackers en el espionaje patrocinado por el Estado o el sabotaje a través del ciberespacio:

- *Los hackers y el cibervandalismo*: los hackers pueden dividirse de manera burda en dos grupos. Los hackers con motivación política que tendrán como blanco el contenido de los sitios web o intentarán impedir el acceso a ciertas páginas o contenidos, y los hackers cibervandálicos que no tienen objetivos políticos. Este último grupo está motivado por la necesidad de poner a prueba los límites de su capacidad, de lograr la autocomplacencia sabiendo que lograron su objetivo;
- *Atacante desde el interior:* los empleados descontentos siguen siendo la mayor fuente de ataques dirigidos contra los sistemas de control de la infraestructura. Tienen un acceso más fácil a los objetos protegidos que los atacantes externos y, con frecuencia, conocen los mecanismos de protección utilizados o tienen acceso directo a los códigos fuente. La amenaza interna se extiende a los empleados de los proveedores de servicios y de sistemas;
- *Cibersabotaje*: está dirigido contra la integridad y disponibilidad de los sistemas y procesos críticos de las TI (Tecnologías de la Información). Esto conduce a la destrucción o al daño masivo del equipo técnico o de la información almacenada;
- *Ciberterrorismo:* tanto los grupos terroristas como los individuos radicalizados pueden perseguir sus objetivos políticos e ideológicos a través del ciberespacio, para llamar la atención sobre sus ideales y valores;
- *Ciberdelincuencia:* los delincuentes cibernéticos actúan individualmente o en grupos y pueden estar muy bien organizados y equipados, aunque otros pueden ser considerablemente menos sofisticados. Sus actividades ilegales en el ciberespacio están orientadas a obtener beneficios económicos. Por lo general, los delincuentes cibernéticos no cometen ataques selectivos contra los sistemas de control de la infraestructura. Los intereses de estos atacantes se centran principalmente en acceder ilegalmente a los datos del usuario (cuentas de banco, tarjetas de crédito). [7]

La amenaza cibernética es una amenaza transversal en el mundo de la infraestructura carretera porque no se puede circunscribir fácilmente. Las amenazas se pueden agrupar en dos grandes grupos:

- *amenazas a los operadores del sistema;*
- *amenazas a la infraestructura.*

4.1.2.1. Amenazas a los operadores del sistema.

En este caso, la amenaza pasa por una fase de recolección de información, por ejemplo, para entender quién dentro de una organización está autorizado para acceder y gestionar el ERP o, lo que es más preocupante, quién tiene las autorizaciones de acceso al SIEM de los sistemas SCADA/ICS.

Una vez que se ha recopilado suficiente información, los atacantes pasan a la parte de recolección de las identidades y permisos de acceso. Esta operación se puede llevar a cabo utilizando diversas "herramientas de ingeniería social" que están dirigidas a personal clave.

[7] El 12 de mayo, 2017, un gran ataque ciber-físico inició con *WannaCry*, el cual infectó a cerca de 230,000 computadoras (la mayoría viejas y no actualizadas) en 150 países y se pidieron pagos de rescate. Esto muestra que los ataques no dirigidos o no selectivos con software malicioso pueden afectar las operaciones significativamente.

Las herramientas para facilitar estas acciones están fácilmente disponibles en línea y están presentes en distribuciones dedicadas a la seguridad informática como "SET" (*Social Engineering Toolkit,* herramientas de Ingeniería Social). Los empleados de los centros de control de túneles están regularmente en contacto con los fabricantes/proveedores de servicios externos para eliminar el mal funcionamiento y los errores. Sin embargo, es un proceso importante validar las llamadas de terceros, ya que un actor de amenazas buscará aprovechar las características humanas tales como el ser servicial, la confianza, el miedo o el respeto a la autoridad. Por esta razón, se recomienda que los empleados reciban capacitación sobre los riesgos relacionados con la Ingeniería Social. También vale la pena considerar la realización de ejercicios de simulación y auditar las políticas y procesos relacionados con la minimización del riesgo de la "Ingeniería Social". Sin embargo, la ejecución de auditorías en las que los empleados son seleccionados como blanco de ataques sin su conocimiento debe ser cuidadosamente sopesada y discutida con el comité de representantes del personal. Un ataque "exitoso" puede ser también una violación a la confianza.

Después de recopilar las identidades y permisos de acceso necesarias, un atacante puede actuar como un administrador del sistema, obteniendo la capacidad de realizar operaciones "de confianza" que los sistemas normales de seguridad informática no pueden controlar ni filtrar. Estos tipos de ataques son los menos sofisticados, pero también los más comunes.

4.1.2.2. Amenazas a la infraestructura.

Llevar a cabo un ciberataque a la infraestructura es más complejo y, por lo tanto, en la actualidad es una forma de ataque menos generalizada, aunque es probable que el uso cada vez mayor de los peajes electrónicos y los datos personales asociados de los usuarios hagan que esta forma de ataque resulte más atractiva para una serie de actores de la amenaza. Los ataques se llevan a cabo directamente en dispositivos a través de *firmware* o mediante el uso de SCADA/ICS.

Este tipo de ataques se han hecho posibles debido a que el software de control y/o el Kernel de administración de los dispositivos industriales a menudo tienen un rendimiento deficiente y/o están mal escritos. El enfoque utilizado por los proveedores se basa en llevar a cabo actualizaciones de sus sistemas una vez que se hayan instalado. Es fácil entender cómo este tipo de enfoque puede poner en riesgo a la infraestructura.

Hoy en día, gracias a herramientas como "Shodan", es posible realizar análisis y establecer qué tipo de dispositivos se están utilizando. La araña web del buscador también tiene la capacidad de recuperar información sobre el nivel de actualizaciones de dichos dispositivos. Si esta información está en manos de atacantes con una capacidad significativa, puede ser utilizada para crear ataques personalizados a la infraestructura con efectos devastadores **[18].**

4.1.2.3. Amenazas a las carreteras inteligentes

El sector del transporte está evolucionando rápidamente y los vehículos automotores ya han pasado de ser un simple modo de transporte a convertirse en un centro de información móvil. La telemática, las redes a bordo de los vehículos, así como las tecnologías inalámbricas para el acceso de vehículos y la recepción de emisiones digitales multi-estándar están ahora integradas en los vehículos automotores. Sin embargo, estas características conllevan nuevos riesgos.

En las carreteras inteligentes, la infraestructura moderna debe permitir la comunicación simultánea entre los automóviles y la infraestructura para recopilar y analizar datos, facilitar el movimiento del tráfico vehicular y aumentar el nivel tanto de la seguridad vial como de la seguridad pública. Los paneles electrónicos, las señales viales y los bolardos retráctiles ya facilitan soluciones avanzadas de gestión de tráfico vehicular para fines de seguridad vial y regulación del tránsito. Los requisitos técnicos específicos de estos sistemas deben garantizar altos niveles de ciberseguridad.

Un aspecto relacionado de gran importancia es el de la privacidad y la autorización para procesar datos personales con fines específicos declarados, regulados en la Unión Europea por el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés). El principio regulador es que sólo se permite trabajar con datos personales si la persona interesada ha dado su consentimiento para uno o más fines específicos. Por lo tanto, existe una gran preocupación entre las AC europeas por el robo de datos personales, ya que conlleva consecuencias penales muy graves. Es probable que los hackers tengan como blanco a los titulares de tarjetas de pago automático, a las imágenes tomadas por cámaras y los datos de las matrículas vehiculares, a las casetas de peaje y las bases de datos de los pagos de peaje, así como a los centros de control y, en el futuro, a los propietarios y conductores de los vehículos autónomos.

4.2. VULNERABILIDAD

Una vulnerabilidad en el contexto de la seguridad pública en la red carretera se define como una debilidad en la infraestructura carretera, en los sistemas operativos o en el personal que puede ser aprovechada por una o más amenazas.
Las vulnerabilidades asociadas a la construcción, operación o mantenimiento de la red de carreteras se relacionan con su escala y la facilidad para:

- obstruir o interferir con la logística, las instalaciones y la maquinaria, las rutas de suministro, y el personal, con el fin de interrumpir el movimiento de personas y bienes, y la cadena de suministro;
- causar daño a equipos tales como cámaras y sensores que proporcionan información sobre la condición o el uso del activo de la carretera;
- causar daño a la infraestructura de carreteras y autopistas, nueva o existente.

Las vulnerabilidades que afectan las operaciones de la red de autopistas se refieren al cableado, el equipo, los sensores y los sistemas de procesamiento asociados que podrían ser atacados:

- de forma remota, a través de internet o la conectividad inalámbrica;
- a través de aberturas físicas de los sistemas como resultado de daños, ya sea accidentales o deliberados, interferencia o manipulación; y/o
- por personal con acceso de administrador.

4.3. CONSECUENCIAS

Las consecuencias de los riesgos de seguridad pública pueden expresarse generalmente como una medida de la pérdida financiera, la influencia de los grupos de interés o comunidades, los daños a la reputación, la pérdida de capacidad operativa o los efectos sobre la salud y la seguridad pública.

La siguiente lista general de posibles consecuencias debe tenerse en cuenta al evaluar las amenazas y vulnerabilidades de la seguridad pública:

- los daños a las personas (agresiones verbales, ataques físicos, secuestro);
- los daños a la propiedad (robo, paquetes sospechosos, vandalismo, choques voluntarios, ataques a la integridad de los edificios operativos y a los sistemas de información);
- los daños a los bienes inmateriales (daños a la reputación, pérdida de la moral en el personal, disminución de la capacidad para reclutar y retener al personal);
- los daños causados por un déficit de gestión (nivel insuficiente de "capacitación en seguridad pública", fracaso de la organización y de los procedimientos de protección, déficit estructural o sensibilización en materia de seguridad pública) [8].

En el ámbito de la infraestructura del transporte por carretera, el daño directo a la infraestructura, la pérdida de vidas o el daño a la integridad física de los usuarios, así como las consecuencias indirectas y macroeconómicas se suelen utilizar para determinar las consecuencias globales.

Los costos directos de un evento normalmente pueden ser determinados con suficiente precisión por los respectivos propietarios y operadores. Aquí se tienen en cuenta los costos de reparación durante la rehabilitación, los costos de las soluciones temporales que puedan requerirse, los costos de instalación de la obra, etc.

La cuantificación de las consecuencias para la vida y la integridad física de los usuarios puede llevarse a cabo cualitativamente sobre la base de evaluaciones de expertos basadas en escenarios o cuantitativamente utilizando métodos de análisis de riesgos. En el caso de los túneles de carretera europeos, los Estados miembros desarrollaron procedimientos de análisis de riesgos como parte de la implementación de la Directiva 2004/54/CE, que también podrían utilizarse para los riesgos de seguridad pública con ciertas restricciones. Como resultado, se obtienen las curvas F-N (consecuencias con probabilidad de ocurrencia asociada) o los valores de expectativa de riesgo, que en principio también pueden ser monetizados.

La determinación de las consecuencias macroeconómicas de los riesgos para la seguridad pública puede hacerse cualitativamente con base en el juicio de expertos, semicuantitativamente mediante la determinación de indicadores adecuados o cuantitativamente utilizando modelos de tráfico que constituyan un puente entre la oferta y la demanda del transporte.

En aplicaciones prácticas, puede ser muy difícil evaluar con precisión el alcance de las consecuencias de un riesgo de seguridad pública. Esto se aplica en particular a los eventos con baja probabilidad y grandes consecuencias (eventos LFHC o "cisnes negros"), cuya naturaleza es de gran complejidad e incertidumbre (véase la sección 3.4) y que se encuentran fuera de la experiencia común. El "problema" se ve exacerbado por las muy diferentes opiniones sobre la naturaleza del riesgo y sus consecuencias, que existen en la mayoría de las organizaciones.

4.4. PROBABILIDAD

Los procesos tradicionales para la toma de decisiones buscan el punto óptimo y las funciones para predecir un estado futuro basado en los planes para las condiciones de ese estado. Este enfoque conduce a resultados óptimos para el futuro previsto, pero su aplicabilidad puede ser limitada en el caso de grandes incertidumbres (como las amenazas de seguridad pública).

[8] IFIE (Institut Français de l'Intelligence Economique) Bernard Besson et Jean-Claude Possin.

Al abordar la incertidumbre cuantificable (riesgo), este método puede extenderse a varios estados posibles, que se caracterizan con sus respectivas probabilidades de ocurrencia. Sin embargo, a medida que aumenta la incertidumbre ya no es posible caracterizar la distribución (es decir, la probabilidad de ocurrencia). En tales situaciones, la solución óptima puede diseñarse para un mundo cuya existencia es incierta, pero que luego puede funcionar mal para otros mundos plausibles, aunque no analizados.

La aceptación de la incertidumbre requiere, por lo tanto, centrarse en la robustez. Un proceso de toma de decisiones robusto implica la selección de un proyecto o plan que cumpla con los objetivos deseados para una variedad de escenarios futuros plausibles. En el cual, se consideran en primer lugar los puntos débiles de un plan para una serie de posibles variables. Se identifican una serie de escenarios futuros plausibles y se evalúa el desempeño de cada plan bajo cada escenario plausible. Como resultado, se pueden determinar qué planes son robustos para los escenarios considerados probables o importantes.

La evaluación de la probabilidad de que ocurra una amenaza de seguridad pública está asociada con un alto grado de incertidumbre. La estimación puede basarse en información de tendencias y eventos; de fuentes tales como informes policiales, informes nacionales de noticias, informes internos de eventos, análisis de auditorías y evaluaciones comparativas con otras organizaciones. Sobre esta base, se puede llevar a cabo un proceso más robusto para la toma de decisiones.

4.5. RIESGO

El riesgo se entiende como el producto de la probabilidad (de que se produzca una amenaza) y las consecuencias (esperadas/calculadas) si se produce la amenaza. Las consecuencias también pueden diferenciarse en consecuencias directas (es decir, víctimas mortales y daños estructurales a la infraestructura) e indirectas (es decir, costos económicos, tiempo de viaje adicional, etc.) [9].

[9] La descripción detallada se puede encontrar en SERON *"Security of Road Transport Networks"*, proyecto de la Unión Europea **[8]** y en HB 167:2006 Security risk management handbook **[6]**

5. DESARROLLO DE MEDIDAS PARA MITIGAR LOS RIESGOS DE SEGURIDAD PÚBLICA

Una vez que se entienden los riesgos de seguridad pública, es necesario desarrollar y evaluar una serie de medidas potenciales de mitigación de riesgos para abordar cualquier riesgo que exceda el apetito de riesgo de la AC. Esto se hace considerando[10] :

- el costo de la medida de mitigación y su implementación;
- la reducción del riesgo que podría lograrse;
- el impacto previsto en el costo;
- otros impactos que la medida de mitigación podría tener en el activo (que podrían incluir la facilidad de uso, eficiencia y apariencia);
- el potencial de la medida para crear más vulnerabilidades; y
- si la medida aporta otros beneficios de negocio.

5.1. MITIGACIÓN DE UN ATAQUE CON VEHÍCULO HOSTIL

Las amenazas de los vehículos automotores se pueden mitigar mediante la instalación de medidas físicas (incluyendo las que se integran con el paisaje interurbano o urbano) que pueden ser pasivas (estáticas) o activas (controladas por la seguridad pública). Estas medidas se pueden instalar de forma permanente o temporal; deben cumplir con los estándares apropiados en términos del desempeño en caso de un impacto vehicular, diseño e instalación. La naturaleza y el alcance de la mitigación dependerán de la evaluación de riesgos y de los requisitos operativos específicos de cada sitio o evento.

Mitigación de vehículos hostiles (HVM) y barreras de seguridad contra vehículos (VSB)

La HVM (por las siglas en inglés de *Hostile Vehicle Mitigation*) utiliza una combinación de medidas para reducir la velocidad de los vehículos potencialmente hostiles y las barreras de seguridad contra los vehículos para detener el avance de vehículos hostiles. Hay una variedad de opciones de HVM y VSB (por las siglas en inglés de *Vehicle Security Barriers*) para ayudar a reducir o mitigar la amenaza de los vehículos, éstas incluyen:

- la exclusión total del tráfico vehicular de un área, utilizando las VSB
- la exclusión parcial del tráfico vehicular con VSB, pero con la detección de todos los vehículos que ingresan al área (con un VACP adecuado, preferiblemente dos capas de VSB activo para evitar el seguimiento de las personas)
- la inclusión del tráfico/flujo libre dentro de un área, pero con todos los activos críticos/vulnerables protegidos con VSB dentro de esa área
- barreras temporales/suplementarias instaladas en momentos de mayor amenaza o cuando hay un evento que requiere seguridad en la zona.

La gama de VSB incluye:

- bolardos o postes de protección (retráctiles activos y estáticos pasivos)
- portones o puertas de acceso
- jardineras y mobiliario urbano reforzado, como las bancas.

Las opciones de paisajismo incluyen:

[10] Para obtener más detalles sobre las amenazas potenciales para la infraestructura de transporte, puede descargar las hojas de datos de peligros que son el resultado del proyecto europeo “AllTraIn” (http://www.alltrain-project.eu/results), consulte en particular las hojas sobre medidas de mitigación **[9].**

- zanjas, terraplenes y bermas.

La mejor forma de HVM es la exclusión total del tráfico vehicular de un área, la cual debe ser ejecutada por las VSB debidamente clasificadas y correctamente instaladas. Un despliegue de VSB que restringe el tráfico (vehículos, peatones o ambos) puede requerir una autorización específica de la autoridad policial.

La instalación de un sistema VSB estático, a una distancia de separación adecuada de un sitio, anulará los estilos de ataque de engaño y coacción. También puede mitigar la manipulación y el seguimiento, que son formas de ataque de intrusión.

Si se requiere acceso frecuente de vehículos a un sitio, entonces se deben considerar las soluciones activas. Las barreras manuales requieren recursos significativos en términos de personal. Las barreras automatizadas requieren tanto un mantenimiento proactivo como procedimientos de llamada reactivos. Éstas soluciones son generalmente más caras y menos seguras que un sistema de barrera de seguridad estática, por las razones expuestas anteriormente.

Si los vehículos acceden ocasionalmente a los sitios, entonces puede ser más rentable utilizar sistemas de barreras desmontables de la base (por ejemplo, un bolardo con zócalos) en lugar de instalar sistemas activos totalmente automatizados.

Opciones temporales

Las VSB temporales pueden incluir unidades de pared modulares y barreras móviles en la carretera (por ejemplo, "New Jersey") para proporcionar soluciones montadas en superficie (por gravedad/independientes) o soluciones fijas. Se pueden alquilar de forma temporal. Después de una evaluación de riesgos apropiada, se puede considerar el uso de vehículos como barrera, como posible mitigación contra un ataque con vehículo como arma (VAW). Este despliegue puede afectar a la seguridad vial de un evento y, por lo tanto, también se debe considerar el acceso de emergencia, las tasas de flujo de la multitud, las rutas de evacuación y tanto la seguridad vial como la seguridad pública de los conductores de los vehículos automotores.

Esquemas de barrera de contingencia

El alquiler repetido de barreras temporales es costoso; por lo tanto, los sitios deben considerar un esquema de barrera de contingencia. En general, estos son las VSB en forma de portones preinstalados en las áreas relevantes, que pueden cerrarse justo antes del evento o zócalos de base preinstalados en los que se colocan las VSB pasivas o activas. Esto evita la pérdida de disponibilidad de carriles durante la instalación de barreras temporales en los días o noches anteriores a un evento, lo que puede beneficiar a las comunidades y a las autoridades de transporte.

Estándares y pruebas

En muchos países existen estándares específicos y metodologías apropiadas para la evaluación de las VSB, a través de estándares de prueba de impacto; por ejemplo, considerando una gama de vehículos de prueba que van desde automóviles de 1.5 toneladas, pasando por vehículos 4x4 de 2.5 toneladas, furgonetas de 3.5 toneladas, camiones de 7.2/7.5 toneladas hasta camiones de 30 toneladas.

Los resultados de las pruebas se clasifican en función de la distancia de penetración del vehículo más allá de las VSB. Esta distancia de penetración es crucial, particularmente cuando los sitios

tienen una separación limitada entre la VSB y el activo a proteger. Las barreras temporales tienden a desplazarse más que las VSB instaladas permanentemente, ya que no tienen el beneficio de una base estructural.

No todos los sitios requieren protección contra las amenazas más grandes o más rápidas de vehículos hostiles, ya que la topografía local o la evaluación de las amenazas pueden descartarlas.

Un experto en seguridad puede evaluar las velocidades máximas de impacto, llevando a cabo una evaluación de la dinámica del vehículo; ésta debe utilizarse para determinar las VSB más adecuadas y/o cuantificar los riesgos residuales.

5.2. MITIGACIÓN DE CIBERATAQUES Y ATAQUES CIBER-FÍSICOS

Un ciberataque es un ataque a sistemas informáticos con fines maliciosos. Se dirige a diferentes dispositivos informáticos: computadoras o servidores, aislados o en redes, conectados o no a Internet, equipos periféricos como impresoras, o dispositivos de comunicación como teléfonos móviles, teléfonos inteligentes o tabletas. Existen cuatro tipos de riesgos cibernéticos con diversas consecuencias, que afectan directa o indirectamente a las personas, las administraciones y las empresas:

- la ciberdelincuencia;
- el daño a la reputación;
- el espionaje, y;
- el sabotaje.

Al abordar el problema de la ciberseguridad, es necesario considerar todo el enfoque de la seguridad de las TI (Tecnologías de Información) como un proceso coherente de calificación, ejecución y verificación continua. Todavía se conoce muy poco el riesgo y el enfoque que se prefiere muchas veces es el tradicional, es decir, instalar contramedidas "físicas" como los *firewalls* y los sistemas de protección de los puntos finales.

Aunque estos sistemas pueden ser útiles, no pueden garantizar el nivel más básico de seguridad, ya que las amenazas han evolucionado en los últimos años.

El equipo de adquisiciones de la organización debe tener en cuenta la seguridad informática y de la información, ya que tendrá que establecer requisitos estrictos sobre la calidad del *firmware* y el protocolo del dispositivo que se comprará. También se debe solicitar una garantía sobre el soporte postventa de los dispositivos. En los casos más sensibles, será necesario realizar una verificación previa a través de estructuras internas especializadas o *ad hoc* de la calidad del *sortware* del dispositivo y luego estructurar un "análisis mapa-dinamo" o un mapa crítico, ya que se puede causar un efecto de dinamo en la infraestructura crítica interna.

Con respecto a las "carreteras inteligentes", se pueden perseguir cuatro objetivos principales:

a. el control de tráfico vehicular
b. la mejora de la seguridad vial
c. la gestión de la movilidad
d. el control de la infraestructura

Los siguientes actores deben ser considerados:

- Las administraciones de carreteras (infraestructura y transporte): las tecnologías inteligentes para la infraestructura y el transporte ofrecen nuevas oportunidades en términos de seguridad vial, eficiencia y protección ambiental, pero los ciberataques y el robo de datos son una nueva frontera de riesgos que deben considerarse en las especificaciones de la licitación, la fase de diseño y la fase de implementación;
- Los conductores y los pasajeros: son el principal grupo objetivo de las soluciones de transporte inteligente;
- Los fabricantes automotrices: las nuevas oportunidades tecnológicas están transformando sus productos con dispositivos aún más complejos, con más componentes electrónicos en su interior, capaces de conectarse a otros dispositivos a través de Internet y creando nuevos desafíos en términos de la seguridad vial, la ciberseguridad y la privacidad;
- Los proveedores de equipos y servicios: se ven afectados por una demanda cada vez mayor de soluciones a prueba de ataques cibernéticos.

6. RESILIENCIA

Los propietarios y operadores de la infraestructura carretera tienen un interés clave en garantizar que los activos y los servicios de la infraestructura de transporte funcionen de manera continua y segura. Este interés ha llevado a un enfoque específico en el concepto de resiliencia. Además del enfoque tradicional de gestión de riesgos descrito anteriormente, los conceptos de resiliencia y gestión de resiliencia se utilizan a menudo en el caso de eventos no planificados o imprevistos con altas incertidumbres.

En general, la gestión de riesgos y de la resiliencia se basa en enfoques similares para:

- evitar consecuencias negativas de los eventos que ocurren;
- revisar los sistemas para detectar debilidades, e
- identificar las actividades que podrían mitigar y/o resolver dichas debilidades.

En el análisis y la evaluación de riesgos convencionales, se utiliza comúnmente un marco conservador basado en la dureza del sistema (protección del sistema, mecanismos a prueba de fallas y/o medidas de respuesta) para protegerlo contra eventos adversos.

Con el fin de juzgar los resultados de los eventos peligrosos, el análisis de la resiliencia busca proporcionar un marco con la capacidad de reducir los daños y, al mismo tiempo, ayudar al sistema a recuperar su máximo rendimiento de la manera más rápida y eficiente posible. Por lo tanto, el análisis de la resiliencia difiere del análisis tradicional de riesgos al considerar la recuperación del sistema después de un evento, una vez que se ha producido el daño. Además de considerar el declive del sistema después de un evento, la resiliencia tiene plenamente en cuenta la preparación, la recuperación y la respuesta posterior al evento. La consideración de estos aspectos es especialmente importante para gestionar la resiliencia de la infraestructura o de las redes carreteras frente a amenazas complejas con altas incertidumbres[11]. El escenario del Apéndice 1.7 - Un accidente en una autopista - muestra un buen ejemplo de tales consideraciones, que van más allá de la mera protección de la infraestructura de transporte.

Como se describe en el capítulo 4.1 de este informe, los propietarios y operadores deben gestionar un espectro muy amplio de posibles amenazas. Éstas, por separado y en combinación, pueden tener un impacto significativo en la disponibilidad de las redes carreteras. Los propietarios y operadores deben enfrentar estos desafíos clave para garantizar un funcionamiento confiable de sus redes carreteras, la movilidad y las cadenas de suministro. También está claro que las interdependencias con otros modos de transporte, así como los efectos en cascada, deben considerarse como parte de un enfoque integral de la resiliencia ante todos los peligros.

Dependiendo del escenario de amenaza considerado, se deben asumir incertidumbres o incluso incertidumbres profundas que dificultan la aplicación de un enfoque tradicional de gestión de riesgos[12]. Una forma adecuada de abordar los desafíos ya mencionados es el enfoque metodológico de la resiliencia o de gestión de la resiliencia. Para el campo de la ingeniería, la resiliencia se puede definir de la siguiente manera:

---

[11] Aven, T., Krohn, BS (2014): A new perspective on how to understand, assess and manage risk and the unforseen. Reliab. Anal. 31(4), 515-522.

[12] Walker Warren E. Walker; Robert J. Lempert; Jan H. Kwakkel: Uncertainty In Model-Based Decision Support

La resiliencia es la capacidad de repeler, prepararse, tomar en cuenta, absorber, recuperarse y adaptarse cada vez con más éxito a eventos adversos reales o potenciales. Esos eventos son catástrofes o procesos de cambio con consecuencias catastróficas que pueden tener causas humanas, técnicas o naturales[13] .

Esta definición muestra que el concepto de resiliencia es, en comparación con la gestión tradicional de riesgos, un enfoque integral y genérico para todos los peligros, que comienza mucho antes de los posibles eventos (preparar, prevenir, proteger) y, en particular, también incluye la fase posterior a la ocurrencia del evento (responder, recuperar). La resiliencia de los sistemas técnicos también se describe a menudo en el ciclo de resiliencia de cinco fases que se muestra en la **Figura 1.**[13]

Figura 1: El ciclo de resiliencia
Fuente: Edwards 2009, ilustración propia del autor

Para ilustrar los elementos de la resiliencia, se puede definir una curva de rendimiento del sistema (**Figura 2**). Se observa una caída importante en el rendimiento cuando se produce un evento extremo inesperado o imprevisto. Sobre la base de la robustez de un sistema, la capacidad de absorción del sistema se ve afectada y el rendimiento que queda puede llegar a ser inferior al que normalmente se esperaría. Después de la ocurrencia de un evento extremo, el rol de la capacidad de adaptación se puede reconocer en función de la cantidad de tiempo que lleva la recuperación del sistema.

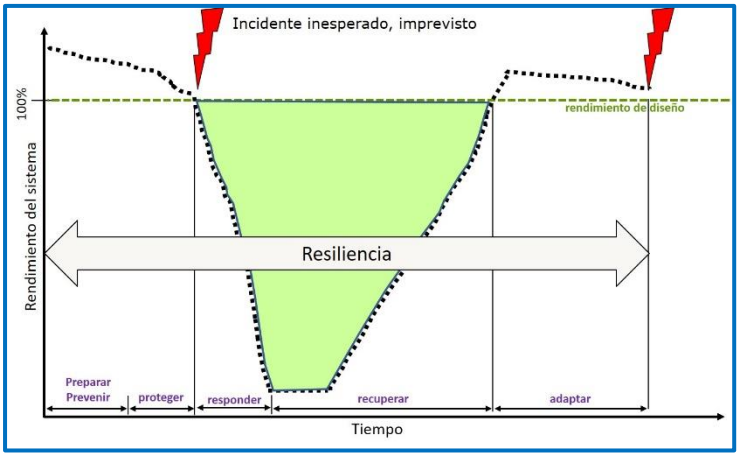


Figura 2: Elementos de la resiliencia
Fuente: (basado en Michel Bruneau y Andrei Reinhorn, 2006) [14]

[13] Scharte, Benjamin/Hiller, Daniel/Leismann, Tobias/Thoma, Klaus (2014): Introduction - Thoma, Klaus (Hrsg.): Resilien Tech. Resilience by Design: Strategy for the technology issues of the future (acatech STUDY). München: Herbert Utz Verlag, 17.

[14] Krieger, J.: PIARC International Seminar on climate change adaptation, risk and disaster management for roads and road organizations, Havana, Cuba, 2017.

El objetivo clave del enfoque holístico de la resiliencia es tener en cuenta todas las fases que se muestran en la Figura 2. Por lo tanto, es importante considerar la infraestructura carretera a nivel de objeto (un puente específico, un túnel específico), así como parte de toda la red (nivel de red) y establecer un vínculo útil entre ambos niveles.

Ya se han hecho aplicaciones prácticas de este enfoque, un ejemplo es el marco de resiliencia desarrollado por la Agencia de Transporte de Nueva Zelanda[15], que es aplicable en todo el sistema de transporte terrestre (carretera y ferrocarril) y que permite tener en cuenta varias escalas (activo/red/región). Para medir la resiliencia, el marco se centra en dos dimensiones -técnica y organizativa- y en principios técnicos (robustez, redundancia, es seguro en caso de falla) y organizativos (preparación para el cambio, liderazgo y cultura, redes). El marco implica una determinación inicial del contexto para la evaluación de la resiliencia, seguida de una evaluación detallada de las medidas de resiliencia; éstas medidas pueden agregarse y ponderarse según sea necesario.

El concepto de resiliencia y la forma en que puede definirse, medirse y mejorarse en todo el sistema de transporte puede ayudar a garantizar que los activos y servicios de la infraestructura de transporte funcionen de forma continua y segura. Este es un cambio cultural, conforme la organización vea la seguridad pública como un trabajo de tiempo completo e incorpore las mejores prácticas de seguridad pública en las operaciones diarias[16]. En comparación con la ciberseguridad, la resiliencia cibernética requiere que la organización piense de manera diferente y sea más ágil en el manejo de los ataques.

La sección 8 de este informe contiene recomendaciones que se aplican a todas las fases del ciclo de resiliencia. Las secciones 8.1 "Mejora del conocimiento y la toma de conciencia" y 8.6 "Cooperación con otros servicios" se ocupan de la planificación y preparación de organizaciones para eventos inesperados o imprevistos, mientras que la sección 8.2 "Mejora de la resiliencia" ofrece indicaciones concretas para mejorar la resiliencia en todas las fases del ciclo de vida de la infraestructura de transporte. Las secciones 8.4 "Seguridad pública en el diseño" y 8.5 "Seguridad pública en el mantenimiento" tratan de las medidas para planificar, preparar y proteger la infraestructura.

[15] Hughes, JF; K Healy, K.: Measuring the resilience of transport infrastructure, NZ Transport Agency reporte de investigación 546, contracted research organisation – AECOM New Zealand Ltd, Febrero 2014

[16] https://www.forbes.com/sites/forbestechcouncil/2017/06/06/cybersecurity-is-dead/#3d1ad0c40121 (última descarga: 13.02.2018)

7. ESTUDIOS DE CASO

El entrenamiento basado en escenarios de ataques u otras acciones maliciosas es un medio práctico para prepararse ante un eventual ataque real. Se utilizan ampliamente en todo el espectro de servicios de seguridad, personal e instituciones para una variedad de tipos de amenazas y blancos.

No existe una regla o metodología universal sobre cómo diseñar un escenario debido a la gran variedad de peligros y amenazas para los cuales se pueden preparar los escenarios. Por lo general, un escenario trata de abordar e incluir información sobre: qué, dónde y por qué ocurrió, quiénes fueron los perpetradores, cuáles son las consecuencias, las víctimas, la respuesta de los servicios de emergencia, etc. Posteriormente, puede incluir otras preguntas e información muy detalladas, específicamente adaptadas a una situación particular de seguridad pública.

Por lo tanto, es aconsejable que los escenarios sean elaborados por personal calificado que conozca el tema o por actores clave que también estén familiarizados con una situación de seguridad pública más amplia (geopolítica) y más reciente alrededor del mundo.

Los escenarios proponen siete acciones agresivas realistas, elegidas entre dos familias generales de actos maliciosos hacia la infraestructura (véase la **Tabla 2** a continuación):

A) terrorismo, ataques físicos, ciberataques;

B) vandalismo, robos, conducta antisocial.

Estos sirven como ejemplos de cómo preparar y luego analizar un escenario para planificar y preparar de la mejor manera posible las actividades y medidas de mitigación/prevención, y pueden proporcionar orientación para abordar cuestiones de seguridad pública como:

1. el conocimiento y la toma de conciencia sobre las amenazas y los daños (ver sección 8.1.): las amenazas pueden ser ataques con explosivos, fuego, impacto mecánico, contaminación y de tipo cibernético (ver **Tabla 1)** o simplemente actos maliciosos más comunes (humillaciones, insultos). Es útil saber cómo se prepara un atentado terrorista y cómo se comportan los perpetradores justo antes de la acción, lo que permite a las personas cercanas a la acción tratar de identificar comportamientos sospechosos y denunciarlos;

2. la resiliencia de (infra)estructuras y sistemas (ver sección 8.2): un ataque simulado muestra la fragilidad del activo y es útil para evaluar las reglas básicas de la preparación, prevención, protección, respuesta y recuperación;

3. la protección otorgada por la ciberseguridad (ver sección 8.3): es probable que sea especialmente importante para los centros de gestión del tráfico vehicular;

4. la protección en el diseño de infraestructura (ver sección 8.4) y en el mantenimiento (ver sección 8.5): demostrar la utilidad de garantizar medidas físicas asociadas con las medidas adoptadas contra los ciberataques;

5. la cooperación con las fuerzas policiales y las autoridades aduaneras, así como la coordinación con las partes interesadas en la red carretera (ver sección 8.6): los servicios de seguridad pública, prestados por un gobierno, son responsables de controlar a las personas y los bienes. Tienen importantes herramientas de seguridad pública y prerrogativas. Los administradores

carreteros con sus propios sistemas y centros de gestión de tráfico son, y seguirán siendo, los socios privilegiados para la seguridad pública;

6. la designación de un asesor de seguridad pública (ver la sección 8.7): muchas organizaciones tienen ahora en cuenta los problemas de la seguridad pública y cuentan con un asesor de seguridad pública entre su personal.

En los apéndices de este informe se proponen los siguientes escenarios de acciones maliciosas:

Apéndice 1.1.: Escenario de la explosión de una bomba sucia en un área urbana.

Apéndice 1.2.: Escenario de un ataque ciber-físico a un centro de control de túneles.

Apéndice 1.3.: Escenario de un vehículo utilizado como arma.

Apéndice 1.4.: Escenario de vandalismo y actos maliciosos en la operación de una carretera.

Apéndice 1.5.: Escenario de robo de carga.

Apéndice 1.6.: Escenario de transporte de materiales peligrosos.

Apéndice 1.7.: Escenario de un accidente en una autopista.

DOS FAMILIAS DE ACTOS MALICIOSOS	
A/ TERRORISMO – ATAQUES FÍSICOS – ATAQUES CIBERNÉTICOS	**B/ VANDALISMO – ROBOS – CONDUCTA ANTISOCIAL**
Acto 1: Explosión de una bomba sucia en un área urbana **Apéndice 1.1** **Acto 2: Ataque ciber-físico a un centro de control de túneles** **Apéndice 1.2** **Acto 3: Utilización de un vehículo como arma** **Apéndice 1.3**	**Acto 4: Vandalismo y actos maliciosos en la operación de una carretera.** **Apéndice 1.4** **Acto 5: Robo de carga.** **Apéndice 1.5** **Acto 6: actos maliciosos contra un camión con materiales peligrosos** **Apéndice 1.6** **Acto 7: actos maliciosos que provocan un accidente carretero** **Apéndice 1.7**

TABLA 2: Dos familias de actos maliciosos contra la infraestructura

8. RECOMENDACIONES PARA LAS ADMINISTRACIONES DE CARRETERAS

8.1. MEJORA DEL CONOCIMIENTO Y LA TOMA DE CONCIENCIA

En la mayoría de los países, la responsabilidad de la seguridad pública recae en la administración de emergencias del Estado o en los Ministerios del Interior u organismos subordinados. Esto contribuye al hecho de que la percepción de los propietarios y operadores de la infraestructura carretera tienda a "la seguridad pública no es un asunto de las AC".

Si bien las AC pueden no ser directamente responsables del monitoreo de la seguridad de la infraestructura, las AC desempeñan un papel en el control del acceso a los componentes críticos y en la coordinación con los organismos encargados de hacer cumplir la ley para garantizar una respuesta rápida a los incidentes, llevar a cabo evaluaciones de los riesgos y la vulnerabilidad de la infraestructura, así como tomar medidas para mitigar el impacto. de dichos riesgos y vulnerabilidades. Por lo tanto, las AC tienen un papel importante que desempeñar en la seguridad de la infraestructura.

Para crear una mayor conciencia de seguridad pública dentro de las AC, se debe considerar, entre otras cosas, lo siguiente [17]: :

- La seguridad pública no es una actividad ocasional llevada a cabo sólo por ciertas personas en el marco de las auditorías de seguridad pública. La seguridad pública sólo puede crearse dentro del marco de la responsabilidad distribuida. Los empleados de las AC están muy bien posicionados y saben (intuitivamente) lo que es normal y lo que es inusual. Ellos hacen una contribución vital para proteger a los empleados, la información, los datos y las instalaciones. Los empleados deben entender que son una parte integral de la solución de la seguridad pública;
- La comunicación y el tratamiento de la seguridad pública son tan importantes como las actividades físicas para aumentar dicha seguridad. Debido a la poca frecuencia de los incidentes de seguridad pública, la creación de una conciencia sobre la seguridad y el mantenimiento de la vigilancia es un desafío particular. Por lo tanto, se necesitan esfuerzos especiales para integrar la conciencia sobre la seguridad en la cultura de las AC;
- Otro factor de éxito para crear conciencia sobre la seguridad pública es el apoyo al Programa de Concientización sobre la Seguridad Pública por parte de todos los niveles de gestión. Por lo tanto, los gerentes deben comunicar activamente que la conciencia de seguridad es una habilidad importante de la AC.

El establecimiento de una conciencia de seguridad pública en las AC para todo tipo de amenazas es un reto importante. Los enfoques para integrar la concientización en materia de seguridad pública en las operaciones rutinarias de las AC y en la capacitación deberían incluir los siguientes aspectos[18]:

- Los administradores deberían tener en cuenta la conciencia de seguridad pública en todas sus áreas y transmitirla a los empleados de la siguiente manera:
  - platicar sobre la seguridad pública en todas las ocasiones; por ejemplo, usar el eslogan "la seguridad pública es asunto de todos" o "si ve algo, diga algo" en todas las reuniones;
  - destacar el tema de la seguridad pública en reuniones periódicas, por ejemplo, en las instrucciones para la integración de la seguridad pública en la vida laboral cotidiana.
- Dialogar sobre la seguridad pública a nivel de unidades organizativas:

[17] Incorporating Transportation Security Awareness into Routine State DOT Operations and Training, NCHRP Report 794, Transportation Research Board, Washington D.C., 2014.

    - los supervisores pueden dialogar rutinariamente con los empleados sobre "las cosas fuera de balance" y la importancia de tomar conciencia sobre la seguridad pública;
    - las sesiones pueden incluir temas de seguridad pública para "resaltar las cosas que hay que buscar" o para enfocarse en cómo reportar personas u objetos inusuales o sospechosos.
- Integración del conocimiento y la concientización sobre la seguridad pública en los cursos de capacitación (existentes):
    - el conocimiento y la concientización sobre la seguridad pública puede incorporarse en cursos de capacitación para empleados nuevos o ya existentes. Se pueden integrar módulos cortos sobre la sensibilización en materia de seguridad pública en los cursos de capacitación existentes;
    - la concientización sobre la seguridad pública puede incluirse en cursos de capacitación específicos para cada objeto, si es necesario. Por ejemplo, la integración en la formación de inspectores de puentes y túneles.
- Integración de informes de concientización sobre seguridad pública en la comunicación interna regular de la agencia y en ocasiones especiales:
    - los boletines informativos y correos electrónicos de la agencia pueden utilizarse para enviar recordatorios y consejos de seguridad pública;
    - los carteles, volantes, etc., para empleados con información y mensajes claros sobre seguridad pública, bien comunicados, pueden distribuirse dentro de la agencia;
    - se pueden agregar, ocasionalmente, informes de concientización a los informes de inspección y otros documentos relevantes.

Al igual que en el caso de la concientización en materia de seguridad vial, el establecimiento de la concientización en materia de seguridad pública puede aumentar significativamente la eficacia de las AC en su conjunto. El conocimiento y la toma de conciencia sobre la seguridad pública es la piedra angular de una cultura de seguridad en la que la seguridad pública es una parte integral de la rutina diaria. La clave del éxito es que todos los empleados en todos los niveles comprendan la importancia de la seguridad pública en su trabajo diario y asuman la responsabilidad de identificar los riesgos de seguridad pública existentes, así como las medidas adecuadas para abordar los problemas de seguridad pública reales y potenciales.

8.2. MEJORA DE LA RESILIENCIA

Como ya se explicó anteriormente (sección 6), la resiliencia representa un enfoque muy completo para hacer frente a incidentes no planificados o imprevistos, que va más allá de la gestión tradicional de riesgos. Además de la mera protección de la infraestructura, la planificación y la preparación, así como la fase de recuperación después de un evento - que es particularmente relevante por la magnitud de las consecuencias (macroeconómicas) -, son de particular importancia en este caso.

Desde el punto de vista de la mejora de la resiliencia de las organizaciones y/o la infraestructura, debe considerarse la preparación y planificación ante posibles eventos, incluyendo la fase de recuperación, además de una evaluación del riesgo basada en la probabilidad de ocurrencia y en las consecuencias.

Para el caso de los sistemas de control de tráfico vehicular en carreteras, se puede recomendar en primer lugar un análisis de la criticidad. En donde se determinan y evalúan los efectos de la falla de elementos de infraestructura individuales (por ejemplo, un puente o un túnel) en la funcionalidad

y el rendimiento de la red, por lo que la criticidad puede entenderse aquí como una variable independiente de la amenaza.

Dicho análisis puede estimarse o determinarse cualitativamente sobre la base de un sistema de puntos, semicuantitativamente mediante la determinación de indicadores de criticidad o cuantitativamente utilizando modelos de transporte que establecen un vínculo entre la oferta y la demanda de transporte. Aquí también se puede concebir una combinación o un enfoque por niveles[18]. El resultado es una compilación de los elementos o secciones de infraestructura "importantes" de una red, que puede utilizarse como una base para los siguientes pasos.

Basándose en estos análisis, el siguiente paso puede ser la planificación y preparación, ante eventos no planificados o imprevistos, para procesos y/o elementos clasificados como críticos. Sobre la base del análisis de amenazas y escenarios de amenazas, se pueden mencionar los siguientes pasos que se deben llevar a cabo antes de que ocurra un evento:

- Planificar para reducir las consecuencias antes de que ocurra un evento;
- Planificar para prevenir/mitigar las consecuencias durante un evento;
- Planificar para prevenir/mitigar las consecuencias después de un evento.

Para los elementos y/o secciones de una red clasificados como críticos, se puede recomendar la preparación de planes de respuesta ante emergencias y peligros, con el fin de prevenir o mitigar las consecuencias durante un incidente. Estos planes deberían abarcar todas las medidas de seguridad vial, tales como las instalaciones de seguridad vial, la gestión del tráfico vehicular, la capacitación de propietarios y operadores, los servicios de emergencia, la gestión de incidentes, la información al usuario, así como la comunicación en caso de que ocurra un incidente entre las autoridades competentes y los servicios de emergencia como la policía, los bomberos, incluyendo los servicios de rescate. Para los túneles en redes transeuropeas de transporte, los planes de emergencia y prevención de peligros son obligatorios, de conformidad con la Directiva del Parlamento Europeo y del Consejo 2004/54/EC sobre la seguridad vial de los túneles de carretera. Dicha directiva también ofrece una buena base para considerar aspectos específicos de seguridad pública[19] .

En preparación para la fase de recuperación de elementos críticos de la red carretera después de los eventos, se pueden utilizar las siguientes decisiones y tareas clave, mismas que se pueden tomar o llevar a cabo antes de un evento[20]:

- Identificación de los elementos relevantes de la red (por ejemplo, identificación de puentes y túneles importantes):
  - criticidad;
  - vulnerabilidad;
  - riesgos.
- Reparación o reemplazo:
  - criterios de reparación y sustitución;
  - sistema de clasificación de daños;
  - evaluación del sitio.

[18] European Research Project - Security of Road Transport Networks, http://www.seron-project.eu/ **[8]**

[19] A Guide to Emergency Response Planning at State Transportation Agencies, NCHRP Reporte 525, Volumen 16, Transportation Research Board, Washington D.C., 2010.

[20] A Pre-Event Recovery Planning Guide for Transportation, NCHRP Reporte 753, Transportation Research Board, Washington D.C., 2013.

- La gestión del tráfico vehicular:
  - Disponibilidad y rendimiento de rutas alternativas, incluida la gestión del sitio;
  - Disponibilidad de sistemas temporales (por ejemplo, puentes temporales);
  - Mantenimiento de existencias e inventario.
- Demolición:
  - Preparación de memorándums de entendimiento y/o contratos;
  - Disponibilidad de equipos especiales.
- Planeación y diseño:
  - Enfoques y decisiones de planificación;
  - Planificación preliminar y especificaciones técnicas.
- Contratos de construcción:
  - Precalificación de contratistas;
  - Procedimiento de adjudicación.

- Métodos y procedimientos de construcción:
  - Procesos innovadores para hacer construcciones nuevas en forma acelerada
- Gestión de proyectos:
  - Precalificación de la gestión de proyectos y supervisión de obra.
- Permisos/Aprobaciones:
  - Requisitos y regulaciones europeas/nacionales;
  - Uso de suelo;
  - Compatibilidad ambiental.
- Financiamiento:
  - Utilización de los fondos del presupuesto para nuevas construcciones o mantenimiento;
  - Presupuestos para desastres.

Dado que no pueden descartarse los daños y la pérdida de elementos de la infraestructura carretera debido a eventos no planificados o imprevistos, a pesar de las amplias medidas de planificación y protección, la mejora de las medidas de resiliencia para una rápida recuperación en caso de un incidente es de particular importancia. Entre otras cosas, se utilizan métodos de ingeniería de resiliencia; en los que, además de las funciones para la operación normal, también se aborda el comportamiento durante el evento y la rápida puesta en funcionamiento de nueva cuenta.

Para los puentes con vanos pequeños o medianos, es particularmente importante la provisión y almacenamiento de puentes temporales que permiten una restauración rápida en caso de un incidente, incluso si el rendimiento es limitado. En el caso de los túneles, se puede aumentar su resiliencia, por ejemplo, equipando túneles de doble tubo para que en caso de necesitar que el tráfico fluya en sentido contrario, en un mismo tubo del túnel, pueda circular con seguridad vial.

Las explicaciones anteriores muestran que el concepto genérico y holístico de resiliencia permite una consideración más allá de la gestión tradicional de riesgos, en la que sólo se considera la reducción de la probabilidad de ocurrencia y/o las consecuencias de los eventos, y, por lo tanto, representa un enfoque más integral.

8.3. MEJORA DE LA CIBERSEGURIDAD

Existen procedimientos para proporcionar un enfoque estandarizado a las evaluaciones de vulnerabilidad, con el fin de verificar el nivel de ciberseguridad de una AC. La ventaja más obvia de tal evaluación es la capacidad de identificar las exposiciones de seguridad antes de que lo hagan los atacantes potenciales. Al completar evaluaciones continuas, es fácil identificar posibles problemas

de seguridad que puedan estar presentes en la red, tanto desde una perspectiva interna como externa. La detección temprana presenta la oportunidad de abordar los problemas antes de que los atacantes puedan aprovechar alguna debilidad, que podría causar graves daños a los activos de la empresa y posiblemente a su reputación.

Por lo tanto, debe entenderse que ya no puede aplicarse en el mundo actual el enfoque tradicional de las licitaciones destinadas a obtener el costo más bajo posible y que incluyen una única verificación de los requisitos funcionales, ya que dicho enfoque expondría la infraestructura a una autorización ineficaz de los dispositivos y, por lo tanto, pondría en riesgo la seguridad de los mismos dentro de la infraestructura. El enfoque tradicional está fomentando la mala configuración y los factores de "falla por diseño" que pueden conllevar grandes riesgos, en un mundo en el que la amenaza terrorista se desplazará cada vez más hacia este frente. Esto debe tenerse en cuenta en un mundo cada vez más hiperconectado y, por lo tanto, debemos hacer que la ley se adapte a la tecnología y su uso, y no al revés.

De cara al futuro, la nueva banda telefónica 5G será capaz de ofrecer un enorme potencial en aplicaciones para el control remoto de infraestructura carretera. La característica más interesante es la posibilidad de usar un número casi ilimitado de terminales conectables, con la única limitante de la cantidad de datos transmisibles. Por ejemplo, se pueden monitorear unas decenas de miles de puntos de detección con una frecuencia de muestreo muy superior a la que ofrece la actual banda 4G LTE. El límite está constituido por la modesta cantidad de datos transmisibles y por el hecho de que las imágenes no pueden transmitirse, sino únicamente información resumida. Además, el problema del uso extensivo de datos en 5G aumentará el perímetro de ataque, ya que siempre habrá más dispositivos conectados a una alta velocidad binaria y, por lo tanto, más datos que pueden verse comprometidos.

8.3.1. Proceso de evaluación de la vulnerabilidad

Una Evaluación de la Vulnerabilidad (EV) es un examen sistemático de un sistema o producto de información para determinar la idoneidad de las medidas de seguridad, identificar las deficiencias de seguridad, proporcionar datos para predecir la eficacia de las medidas de seguridad propuestas y confirmar la idoneidad de dichas medidas tras su implementación. La EV permite obtener una lista de las vulnerabilidades más identificables (vulnerabilidades de software, contraseñas predeterminadas, etc.) para resolver los problemas, priorizándolos y estructurando las acciones correctivas en un plazo relativamente corto.

La EV brevemente descrita se refiere a la metodología NIST SP 800-53A [10]. La mayoría de los procedimientos de prueba para evaluar el estado genérico de la ciberseguridad son viables de realizar con formularios (ver más abajo). Se utilizan herramientas específicas y actividades manuales para identificar fallas en la protección.

El propósito final de las herramientas de verificación es la lista de vulnerabilidades encontradas. Para cada uno de ellas, proporciona información como la tipología, una descripción del problema, el impacto que genera, el componente afectado y cualquier referencia a las clasificaciones. Para cada vulnerabilidad se deben proponer medidas y posibles soluciones.

Las principales actividades a realizar son:

- evaluación del comportamiento;
- identificación de las exposiciones;

- ocuparse de las exposiciones.

El proceso operativo típico es:

- análisis preliminar: escuchar las necesidades y demandas de la administración anfitriona, obtener información sobre las estructuras lógicas y virtuales, así como examinar cualquier informe anterior;
- presentación de la propuesta: después de realizar el análisis preliminar, presentar propuestas con enfoques operativos;
- desarrollo del proyecto: una vez que el administrador anfitrión ha elegido una propuesta, se establece el entorno de desarrollo del proyecto personalizado;
- realización del proyecto: llevar a cabo el proyecto, informar e involucrar a la administración anfitriona en las fases de ejecución;
- primera versión: proponer una primera versión del servicio/producto solicitado en un entorno seguro, para no exponer la estructura a ninguna vulnerabilidad, sino para recibir realimentación del anfitrión.
- segunda versión: proponer una segunda versión preliminar, basada en la retroalimentación del anfitrión;
- entrega y servicio postventa: entrega del servicio/producto y los planes en concordancia con el anfitrión, así como del servicio postventa.

8.3.2. Pruebas de penetración

El alcance de una penetración es:

- determinar si un usuario malintencionado puede obtener acceso no autorizado a activos que afectan la seguridad fundamental del sistema, archivos, registros y/o datos de titulares de tarjetas, y cómo puede obtener dicho acceso; y
- confirmar que se cuenta con los controles aplicables, como el alcance, la gestión de vulnerabilidades, la metodología y la segmentación, requeridos en el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS , por sus siglas en inglés).

Existen tres tipos de pruebas de penetración: caja negra, caja blanca y caja gris. En una evaluación de caja negra, la entidad anfitriona no proporciona ninguna información antes del inicio de la prueba. En una evaluación de caja blanca, la entidad puede proporcionar al examinador de penetración detalles completos de la red y las aplicaciones. Una evaluación de caja gris es un enfoque intermedio, llevado a cabo con la estructura del código interno o la lógica de programación del producto de software.

El alcance de una prueba de penetración, tal como se define en el marco estándar de NIST, debe incluir todo el perímetro CDE y cualquier sistema crítico que pueda afectar la seguridad de la CDE.

8.3.3. Proceso de evaluación del riesgo

Las evaluaciones de riesgos pueden llevarse a cabo con eficacia en varias etapas del ciclo de vida del desarrollo del sistema para aumentar el nivel de confianza con respecto a los controles de seguridad empleados dentro de un sistema de información o inherentes a éste. El objetivo es identificar por adelantado la arquitectura de seguridad de la información y los controles de seguridad, así como garantizar que el diseño y las pruebas del sistema validen la implementación de dichos controles.

Las fases de un proceso formalizado de evaluación de riesgos de seguridad pública son:

- identificar la misión de la organización, la gobernanza y las políticas, los perfiles de reputación;

- identificar los activos/componentes que contribuyen a la prestación de todos los servicios de la organización;
- realizar un análisis de riesgos basado en un análisis de impacto y probabilidad;
- definir un plan de acción basado en los riesgos priorizados;
- a partir de la evidencia del seguimiento formal, crear un seguimiento de las acciones correctivas para la mitigación del riesgo;
- proporcionar los requisitos de resiliencia que apoyarían la prestación de los servicios críticos en todas las operaciones de los Estados (por ejemplo, bajo coacción/ataque, durante la recuperación, durante las operaciones normales).

Las evaluaciones de seguridad pública deben realizarse periódicamente (probablemente anualmente) para abordar e incorporar cualquier cambio en la oferta de servicios, nuevos clientes, nuevo entorno, etc., que pueda introducir nuevos riesgos de seguridad que deban abordarse. La evaluación de riesgos debería incluir también al personal, a los contratistas y a toda la cadena de suministro.

Al mismo tiempo, en el caso de los servicios específicos, el proceso de evaluación de riesgos incluye los siguientes controles técnicos periódicos:

- La Evaluación de la Vulnerabilidad (EV) cada 3 meses
- Prueba de Penetración (PP) cada 6 meses.

La Evaluación de la Vulnerabilidad y la Prueba de Penetración deben realizarse con frecuencia, ya que permiten que una AC obtenga una lista de sus vulnerabilidades más identificables y que estructure las acciones correctivas en un período de tiempo relativamente corto. Una vez que los eventos de riesgo son evaluados como de mediana o alta criticidad, una organización debería comenzar la planificación e implementación de la mitigación de dichos riesgos.

La etapa de mitigación de riesgos implica el desarrollo de planes de mitigación diseñados para gestionar, eliminar o reducir el riesgo a un nivel aceptable. Una vez que un plan es implementado, se monitorea continuamente para evaluar su eficacia, con la intención de revisar la línea de acción si es necesario.

Las opciones para el manejo de la mitigación de riesgos incluyen:

- Asumir/Aceptar: reconocer la existencia de un riesgo en particular y tomar la decisión deliberada de aceptarlo sin realizar esfuerzos especiales para controlarlo;
- Evitar: ajustar los requisitos o restricciones del programa para eliminar o reducir el riesgo. Este ajuste podría acomodarse mediante un cambio en la financiación, el programa de actividades o los requisitos técnicos;
- Controlar: implementar acciones para minimizar el impacto o la probabilidad del riesgo;
- Transferir: reasignar el compromiso, la responsabilidad y la autoridad de la organización a otro actor que esté dispuesto a aceptar el riesgo;
- Vigilar/Monitorear: monitorear el entorno para detectar cambios que afecten la naturaleza y/o el impacto del riesgo.

Cada una de estas opciones requiere el desarrollo de un plan que sea implementado y monitoreado para su efectividad.

Se elaboraron los siguientes dos cuestionarios; el primero, en el marco del proyecto de investigación Ciber-Seguro (Cyber-Safe) [11], donde se identificaron las medidas técnicas, organizativas y de personal para los centros de control de túneles (**Tabla 3**), y el segundo es parte de una investigación para concesionarios de autopistas (**Tabla 4**).

En el proyecto Ciber-Seguro se investigó la seguridad informática de los centros de control de tráfico, de túneles y del transporte público alemanes. El objetivo era desarrollar medidas que permitan a los operadores aumentar la seguridad de las TI. Como primer paso en la evaluación de la seguridad, se desarrolló la siguiente lista de verificación que podría proporcionar una primera visión general del nivel de seguridad del personal. En dicha lista se pide que se evalúen las afirmaciones con base en una valoración personal, en una escala que va desde "plenamente aplicable" hasta "no se aplica en absoluto" o la respuesta puede dejarse en blanco.

TABLA 3: Cuestionario del proyecto de investigación Ciber-Seguro [11]

1. Control de la tecnología
1.1 ¿El acceso a todos los sistemas de información es a través de una combinación de usuario y contraseña? 1.2 Las contraseñas deben contener al menos 8 caracteres e incluir letras mayúsculas y minúsculas, caracteres especiales y números. 1.3 ¿Se cambian las contraseñas regularmente (al menos cada 6 meses)? 1.4 ¿Se anotan las contraseñas y/o se registran por escrito? 1.5 ¿La comunicación entre el nivel de control y los objetos a nivel de campo está encriptada y autenticada? 1.6 ¿Tienen que cumplir los contratistas con un nivel básico de seguridad de las TI? 1.7 ¿Todos los sistemas de las TI con acceso remoto son monitoreados constantemente por el centro de control y pueden ser bloqueados en cualquier momento? 1.8 ¿Todos los sistemas de las TI con acceso remoto tienen programas antivirus actualizados? 1.9 ¿El sistema del centro de control está conectado a internet?
2. Comunicaciones internas
2.1 ¿Existe una separación física entre el sistema del centro de control y las comunicaciones internas del centro? 2.2 ¿El intercambio de datos entre el sistema del centro de control y las comunicaciones internas se realiza conforme a las reglas de seguridad? 2.3 ¿Están conectados los dispositivos privados (computadoras portátiles, teléfonos inteligentes - incluso para recarga -, memorias USB, etc.) a las computadoras de servicio? 2.4 ¿Hay una Red Inalámbrica de Área Local (WLAN, por sus siglas en inglés)? 2.5 ¿Las computadoras de trabajo también se utilizan para fines privados?
3. Control del acceso al centro
3.1 ¿El acceso al centro de control y a las instalaciones está garantizado por los sistemas de videovigilancia y de alarma contra robos? 3.2 ¿Están documentados todos los accesos a los edificios mencionados en la pregunta anterior? 3.3 ¿Se verifica periódicamente la eficacia de los sistemas de control de acceso (al menos cada 6 meses)? 3.4 ¿Se monitorean internamente las salas vulnerables (por ejemplo, la sala de servidores, las instalaciones con áreas de trabajo)?
4. Organización y personal
4.1 En caso de un ataque a las TI o falla de las TI, ¿están disponibles los planes de contingencia apropiados? 4.2 ¿Ya está completamente implementado el catálogo básico de seguridad de las TI? 4.3 ¿Se cuenta con un administrador de seguridad de las TI? 4.4 ¿Se capacita regularmente a los empleados sobre la seguridad de la TI? 4.5 ¿Es adecuada la capacitación de los empleados? 4.6 ¿Los empleados conocen los peligros de las redes sociales?
5. Evaluaciones del personal
5.1 En su opinión, ¿la seguridad de las TI del centro de control es en general alta?
6. Retroalimentación sobre la lista de verificación
Nos encantaría que nos pudiera dar sugerencias sobre esta lista de verificación.

TABLA 4: Cuestionario para evaluar el estado actual de la ciberseguridad en una AC

		SÍ	NO	Parcial	Especificaciones y comentarios	Respuestas
1	**Infraestructura de Seguridad**					
1.1	¿Dispone de un Centro de Datos interno o externo a la red de su empresa?					
1.2	Si es externo, ¿es segura la conexión? ¿A través de qué canales y protocolos (SSH, SSL, IPSec)?					
1.3	¿Ha sufrido alguna vez ataques/accidentes de seguridad informática? ¿Cuánto tardó la reanudación? ¿Hubo pérdida de datos?					
1.4	¿Ha preparado medidas de seguridad de acceso a la red y a los sistemas informáticos?					
1.5	¿Se ha nombrado a un administrador de sistemas?					
2	**Gobernanza de la Seguridad**					
2.1	¿Dispone de un documento sobre las políticas de la empresa en materia de seguridad informática?					
2.2	¿Ha preparado procedimientos para la gestión de los accidentes de seguridad informática? ¿Se elaboró un Plan de Continuidad de Negocio y/o un Plan de Recuperación de Desastres?					
2.3	¿Ha realizado alguna vez simulacros de accidentes o situaciones de emergencia informática?					
2.4	¿Se llevan a cabo periódicamente actividades de auditoría para verificar el estado efectivo del cumplimiento de la seguridad y el control?					
2.5	¿Dispone de programas de capacitación, concientización y lecciones en el ámbito de la seguridad de las redes y de los sistemas informáticos?					
3	**Cumplimiento de la Normativa**					
3.1	¿Se está adaptando su empresa a la normativa general sobre Protección de Datos de la Unión Europea 2016/679?					
3.2	¿Se ha identificado la figura de RPD (Responsable de la Protección de Datos)?					
3.3	¿Se han realizado Planes de Evaluación de Seguridad y/o Evaluación de Riesgos?					
3.4	¿Se han implementado (o se están implementando) las nuevas Directivas NIS (EU) 2016/1148?					
3.5	¿Gestiona usted directamente los Sistemas Inteligentes de Transporte (ITS, por sus siglas en inglés)?					
4	**Seguridad Cibernética**					
4.1	¿Tiene una Estrategia de Seguridad Cibernética?					
4.2	¿Se ha llevado a cabo alguna vez una Evaluación de Vulnerabilidad y/o una Prueba de Penetración para evaluar el nivel de seguridad de las redes y los sistemas informáticos?					
4.3	¿Utiliza servicios de terceros (*outsourcing*) y, en particular, servicios en la nube (*cloud computing*)?					
4.4	¿Está equipado con un sistema IDS (siglas en inglés de Sistema de Detección de Intrusos)?					
4.5	¿Está equipado con un SOC (siglas en inglés de Centro de Operaciones de Seguridad)?					

8.4. SEGURIDAD PÚBLICA EN EL DISEÑO

El concepto de "seguridad pública en el diseño" se refiere a la toma de conciencia de los propietarios y administradores de la infraestructura sobre las amenazas y los riesgos de seguridad para su infraestructura. Se debería pensar sobre la protección de los activos desde las primeras fases de diseño de un nuevo edificio/infraestructura. Al igual que con cualquier otro tipo de obras, la incorporación de nuevas soluciones y adaptaciones en la fase de reconstrucción es – casi por regla general – más costosa que su incorporación en la fase de diseño. En la infraestructura más antigua no hay otra opción que implementar medidas de protección durante la reconstrucción; en la infraestructura de nueva construcción, sin embargo, se recomienda mucho que los diseñadores incorporen soluciones de seguridad pública desde el principio.

En este punto también debemos mencionar la evolución y el uso creciente del Modelado de Información para la Construcción (BIM) [4] en la planificación de nuevas construcciones y en las reconstrucciones. BIM se está convirtiendo poco a poco en un estándar para todos los nuevos proyectos de construcción y sus beneficios para facilitar el intercambio de información son evidentes. Sin embargo, hay que tener en cuenta algunos aspectos de seguridad pública debido a que la representación digital del edificio debe ser compartida para facilitar la comunicación entre los distintos actores que participan en el proceso de diseño.

A continuación, se enumeran algunos principios generales de resiliencia, que los propietarios y administradores de infraestructura deberían tener en cuenta al hablar con los diseñadores sobre la incorporación de medidas de seguridad pública en el plan de construcción[21]:

- **Principio de concepción proactiva**, para reducir o eliminar la vulnerabilidad;
- **Principio de mejora de la capacidad de adpatación** durante un evento;
- **Principio de añadir redundancias a un sistema informátivo** para reducir los efectos en términos de degradación de la integridad, en relación con la magnitud del evento crítico y mejorar la disponibilidad para redirigir el tráfico vehicular a través de uno o más componentes paralelos;
- **Principio de preparación de los componentes esenciales de seguridad**, para disponer de componentes de respaldo que reemplacen rápidamente el funcionamiento interrumpido.

Desde un punto de vista estrictamente estructural, algunos de los conceptos tomados de la ingeniería antisísmica son útiles. En general, es necesario aumentar la resistencia de la estructura de soporte permitiendo la deformación plástica (ductilidad), buscando la plasticidad de la sección, la construcción y la consiguiente reducción de la rigidez para redistribuir la demanda inesperada. Se trata de aprovechar la respuesta unitaria y de colaboración entre los diferentes elementos estructurales (todos para uno – uno para todos). En este sentido, los métodos de diseño en "capacidad" son útiles para aplicarse en secciones, elementos, conexiones, distinguiendo entre aquellos con comportamiento frágil o dúctil. También se debe tener precaución en términos de la "jerarquía de resistencias" con el objetivo de que es acoplen correctamente entre sí, logrando el comportamiento dúctil deseado, tanto local como global, para evitar colapsos locales mortales. [22]

---

[21] AASHTO Fundamental Capabilities of Effective All-Hazards Infrastructure Protection, Resilience, and Emergency Management for State Departments of Transportation. American Association of State Highway and Transportation Officials, Washington, 2015; página 8 **[16]**

[22] Prof. Franco BRAGA, Buildings in Seismic Area, Department of Structural Engineering, University of Rome - La Sapienza, 2016.

El propietario/gerente y el diseñador deben tener en cuenta que existen múltiples contramedidas que tienen diferentes roles. La mejor y más importante manera de empezar es tratar de prevenir o dificultar el acceso a la estructura. Todas las demás contramedidas, más allá de esa línea, tienen por objeto prevenir que se cometa un acto malicioso una vez que el autor ya se encuentre en las instalaciones o haya tenido acceso a un activo. Uno debe tratar de visualizar su activo vulnerable desde un punto de vista "militar", con múltiples líneas de defensa o "capas de seguridad" (**Figura 3**).

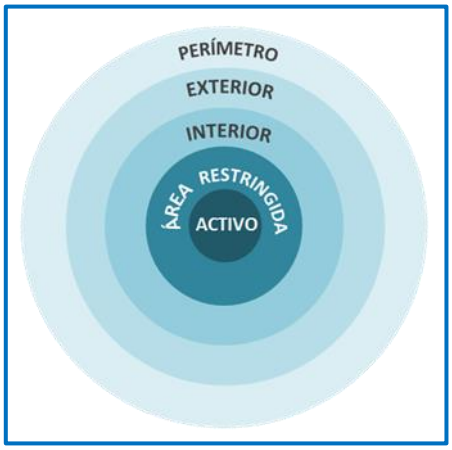


Figura 3: Capas de seguridad
Fuente: imagen rediseñada por el GE C.1 de acuerdo con[23]

La mayoría de las herramientas, que deben considerarse en la fase de implementación de la planificación como medio para evitar el acceso a la infraestructura e instalaciones vulnerables, sistemas de información y otras áreas, son contramedidas de seguridad física. A continuación, se presentan brevemente algunos de los grupos de contramedidas, pero se debe tener en cuenta que no se trata de una lista completa de las medidas que pueden usarse.

8.4.1. Señales [24]

Una cosa ha sido probada: ni las vallas ni las señales detendrán a un enemigo determinado. Sin embargo, las señales de seguridad pública pueden desempeñar un papel muy importante en la seguridad pública de las instalaciones de transporte, los derechos de paso y la infraestructura crítica. Son relativamente baratas y de bajo mantenimiento. El mantenimiento de un buen programa de señalización de seguridad pública también ayuda a crear un entorno de trabajo en el que la seguridad pública se perciba como algo serio. El uso efectivo de los letreros comienza con la creación de un plan que identifica cada letrero por tipo y leyenda, dicho plan también establece el emplazamiento para su colocación y la forma de instalación, por lo que es la base para la toma de decisiones. Las señales pueden utilizarse en todas las capas de seguridad (véase la Figura 3).

[23] Misma fuente; página 30.

[24] Ernest R. Frazier, Yuko J. Nakanishi and Mary Ann Lorimer: Security 101: A Physical Security Primer for Transportation Agencies. Surface Transportation Security, Volumen 14. National cooperative highway research program, Transportation research board, Washington, 2009; todo el texto tomado y adaptado de las páginas 27 y 30 **[17]**

8.4.2. Teléfonos de emergencia, alarmas y estaciones de asistencia[25]

Las cabinas telefónicas, los botones de alarma de pánico y los sistemas para la comunicación interna generalmente estaban conectados a estaciones centrales donde los despachadores o el personal de monitoreo que respondía a las llamadas de emergencia podían enviar personal de respuesta a la ubicación para ayudar. Hoy en día, la tecnología inalámbrica ha añadido nuevas dimensiones y capacidades para el uso de estos sistemas en relación a la seguridad pública. Un aspecto importante es que el despliegue de los sistemas de alerta o alarma de emergencia debe hacerse en función de las capacidades de respuesta estimadas, teniendo en cuenta la posible variación en el tiempo de respuesta y, cuando corresponda, las rutas y ubicaciones de los vehículos y equipo de la agencia. Se debe evitar una alarma de coacción o un sistema de comunicación de emergencia que quede sin respuesta. Estas medidas se usan generalmente en la capa de seguridad interior (ver **Figura 3**).

8.4.3. Controles con llave y cerraduras [26]

Las cerraduras son una medida básica de seguridad pública, ampliamente utilizadas para proteger a las instalaciones, las actividades, al personal y las propiedades. Pero aún el mecanismo de cerradura más costoso y bien construido puede abrirse si el adversario o el agresor tiene suficiente habilidad y tiempo. Las cerraduras más sofisticadas y resistentes a la manipulación, las cerraduras con cuatro o más tambores, algunos sistemas de núcleo intercambiables o los dispositivos de cierre en cajas fuertes o puertas pueden proporcionar un aumento apreciable de la dificultad, pero aun así están sujetos a verse comprometidas. Por lo tanto, las cerraduras deben considerarse, en el mejor de los casos, como elementos disuasorios y más razonablemente como un dispositivo de retardo que no restringe completamente la entrada a un área protegida. Estas medidas se utilizan generalmente en el área restringida de las capas de seguridad (véase la **Figura 3**).

8.4.4. Barreras de protección [27]

Las barreras de protección incluyen a las vallas, varios tipos de barreras y el diseño del paisaje. Todas estas medidas se utilizan habitualmente en el perímetro más exterior de las capas de seguridad (ver la **Figura 3**).

8.4.4.1. Vallas

Las vallas son un tipo de barrera protectora disponible para los diseñadores de seguridad pública. El uso principal de las vallas de seguridad es como factor de disuasión o retraso. Cuando las vallas se utilizan de esta manera, se aplican términos como línea perimetral y zona de acceso controlado. La línea perimetral es la línea de defensa más exterior de una zona protegida. Una zona de acceso controlado intenta limitar el acceso al área más inmediata que se está protegiendo.

---

[25] Ibídem; todo el texto tomado y adaptado de las páginas 30 y 31.

[26] Ibídem; todo el texto tomado y adaptado de las páginas 31y 32.

[27] Ibídem para los puntos 7.4.4., 7.4.4.1., 7.4.4.2. y 7.4.4.3.; todo el texto tomado y adaptado de las páginas 32-34.

8.4.4.2. Otras barreras

Otros tipos de barreras incluyen las barreras anticolisión para vehículos clasificadas como pasivas o activas. Las barreras pasivas son contramedidas fijas e incluyen bolardos (tubos de acero rellenos de hormigón), mobiliario urbano reforzado, muros de hormigón, jardineras y bermas. Las barreras activas se pueden mover o son retráctiles para de alguna manera permitir el paso cuando sea necesario. Tales barreras pueden incluir bolardos retráctiles, vigas para choques, sistemas de cuña giratoria o barricadas levadizas.

8.4.4.3. Diseño del paisaje

Las barreras naturales, como los árboles o el agua, pueden utilizarse para reducir las vulnerabilidades. Además, la planificación real del sitio para las áreas protegidas puede tener en cuenta la seguridad pública, con un diseño paisajístico que cumpla con el doble propósito de la estética y la función.

8.4.5. Iluminación de protección (lámparas y luminarias) [28]

Los profesionales de la seguridad pública, el personal de respuesta a emergencias y los expertos de la seguridad vial exaltan el valor de la luz manufacturada para proteger a las personas y a la propiedad de daños o riesgos irrazonables de lesiones. Aunque es relativamente barato en comparación con otras estrategias de seguridad pública, el alumbrado requiere un fuerte compromiso para su cuidado y mantenimiento continuo. Usada como una contramedida de seguridad pública durante horas de oscuridad, la iluminación de protección puede crear un entorno operativo que ofrezca una mejor seguridad que durante el día. Debido al acceso abierto en el medio ambiente, se deben examinar los posibles aspectos de la iluminación de doble uso, para su posible integración en las operaciones convencionales del transporte. Estas medidas se utilizan normalmente en el perímetro más alejando y en el exterior, pero también pueden aplicarse en las demás capas de seguridad interiores (véase la Figura 3).

8.4.6. Sistemas de detección de intrusos y alarmas [29]

La aplicación de la seguridad física básica que ofrecen los sistemas de alarma de detección de intrusos se relaciona principalmente con la detección de movimiento. Dichos sistemas son una contramedida importante en el kit de herramientas de planificación de la seguridad pública y su implementación suele llevarse a cabo con otras contramedidas de seguridad pública, como las barreras naturales y artificiales, los sistemas de control de acceso y otras tecnologías de sensores. Su propósito principal es trabajar como un multiplicador de fuerza para permitir un uso más eficiente del personal, ya que se reduce la cantidad de personal de seguridad necesario para patrullar o monitorear un área protegida. Suponiendo que haya una fuerza de respuesta cerca, los sistemas de alarma pueden eliminar la necesidad de contar con una fuerza de patrullas de seguridad dedicadas. Para que un sistema de alarma de detección de intrusos sea eficaz, debe haber tanto una capacidad de monitoreo activo o pasivo como una capacidad de respuesta del personal de

[28] Ibídem; todo el texto tomado y adaptado de las páginas 35 y 37.

[29] Ibídem; todo el texto tomado y adaptado de las páginas 38-40.

seguridad pública o de las fuerzas del orden público. Estas medidas se utilizan generalmente en el área restringida de las capas de seguridad (véase la **Figura 3**).

8.4.7. Sistemas electrónicos de control de acceso [30]

Los sistemas de control de acceso limitan o restringen el acceso de personal o vehículos hacia dentro o fuera de un área controlada. Hoy en día, la tecnología de tarjetas inteligentes y los sistemas biométricos son cada vez más frecuentes. No siempre es posible controlar los movimientos de las personas debido al entorno operativo abierto. El chequeo inadecuado de los usuarios del sistema puede crear un nivel insostenible de molestias que se traduzca en la pérdida de clientes. Los sistemas pueden ser autónomos para controlar el acceso a un único punto de entrada o en varias puertas, basados en computadora y capaces de controlar el acceso a cientos de puertas y gestionar miles de credenciales de identificación. Antes de implementar un sistema de control de acceso, las administraciones de carreteras deben tener una comprensión clara de las amenazas y vulnerabilidades que deben abordarse. Estas medidas se utilizan generalmente en el área restringida de las capas de seguridad (véase la **Figura 3**).

8.4.8. Sistemas de vigilancia y monitoreo [31]

En general, la videovigilancia CCTV es un sistema de una o más cámaras de vídeo conectadas en circuito o en bucle. Las cámaras proporcionan imágenes de entrada a un monitor de televisión para su visualización. Dependiendo de los objetivos de seguridad pública, el sistema de CCTV también puede incluir la capacidad de grabación y reproducción. La integración efectiva de videovigilancia CCTV en un programa de seguridad pública de la administración de transportes y carreteras exige que los planificadores tengan un alto nivel de comprensión conceptual de las capacidades de la tecnología para satisfacer los requisitos y necesidades de la organización. Los sistemas de vídeo no proporcionan ninguna forma de rechazo o demora al ataque, en respuesta a las tácticas o acciones del agresor. No representan ninguna barrera física, no controlan el acceso ni reducen la exposición a condiciones peligrosas. Sin embargo, la videovigilancia CCTV es la segunda herramienta de seguridad pública más importante, capaz de mejorar en gran medida el rendimiento y la capacidad de respuesta de las fuerzas de seguridad pública y de los sistemas de detección de intrusos. Al añadir la videovigilancia a estos sistemas, una administración de carreteras puede monitorear y evaluar de manera remota las condiciones de seguridad durante un incidente de seguridad pública. Estas medidas generalmente se utilizan en el interior y en el área restringida de las capas de seguridad (ver **Figura 3**).

8.4.9. Centros de gestión del tráfico

Hay algunas cosas que se pueden hacer para proteger físicamente un centro de gestión de tráfico (CGT) que no difieren de las medidas de protección de cualquier otro edificio importante en riesgo [12] [13]:

- estudiar y conocer (si es posible, controlar) los alrededores del CGT; es decir, las carreteras, cualquier característica especial del terreno, los edificios cercanos y/o las áreas residenciales, las conexiones de transporte, etc., para poder predecir desde qué dirección podría provenir el ataque;

---

[30] Ibídem; todo el texto tomado y adaptado de las páginas 41-44.

[31] Ibídem; todo el texto tomado y adaptado de las páginas 44-48.

- establecer un perímetro físico y defensivo alrededor del edificio (pero no evidente); es decir, no es necesario instalar una valla de seguridad muy alta y obvia, hay otras soluciones menos obvias. Elija el tipo de perímetro de seguridad adecuado con respecto a la ubicación del CGT y a la naturaleza de su entorno, la intención es guiar y canalizar físicamente los movimientos alrededor de las instalaciones;
- controlar estrictamente y de forma electrónica el acceso directo al edificio y dentro del mismo; todas las puertas del edificio deben estar aseguradas y el acceso debe ser controlado con cerraduras electrónicas, códigos de acceso y videovigilancia, si es necesario, debido a la ubicación del CGT, asegúrese de que haya guardias de seguridad armados para el control del acceso;
- conocer la ubicación y el paso de las líneas de suministro (eléctrico, óptico, de gas, de agua, etc.) para averiguar los puntos más débiles a los que podrían dirigirse;
- programar y controlar las entregas periódicas al CGT;
- educar al personal que trabaja en el CGT sobre los riesgos y protocolos de seguridad pública (incluidos los trabajadores de apoyo, para la limpieza y el mantenimiento, la cocina, el servicio y cualquier otra actividad que se realice en el edificio);
- realizar periódicamente simulacros de emergencia; no sólo para para la evacuación en caso de incendio, sino también para posibles escenarios de intrusión o ataque;
- establecer una conexión directa con la policía y/o el servicio de seguridad pública, así como planificar con ellos el sistema de seguridad pública del CGT.

8.5. SEGURIDAD PÚBLICA EN EL MANTENIMIENTO

La seguridad en el mantenimiento se refiere a que los propietarios/administradores tomen conciencia de las vulnerabilidades de seguridad pública cuando se realizan trabajos de mantenimiento. El concepto se puede ver desde dos perspectivas:

- concientización sobre la seguridad pública en los trabajos de mantenimiento físico y reconstrucción;
- concientización sobre la seguridad del personal durante el mantenimiento (cuando la protección de la infraestructura no está 100% asegurada).

8.5.1. Concientización sobre la seguridad pública en los trabajos de mantenimiento físico y reconstrucción

Esto está estrechamente relacionado con el concepto de "seguridad pública en el diseño" y significa que deben aplicarse los mismos principios en la planificación de los trabajos de mantenimiento y reconstrucción que en la fase de diseño de una nueva infraestructura. Exige un buen conocimiento del estado de la infraestructura por parte del propietario/administrador, que puede incluir nuevas soluciones de seguridad pública en los trabajos de mantenimiento y reconstrucción, así como mejorar la resiliencia de la infraestructura. Algunas de las medidas (en relación con las capas de seguridad - ver **Figura 3**) ya se presentaron en el capítulo anterior sobre seguridad en el diseño.

Como ya se mencionó, la implementación de soluciones de seguridad pública en la fase de mantenimiento y reconstrucción de la infraestructura suele ser más costosa que su incorporación en la fase de diseño, es decir, antes de la construcción. Por supuesto, en la infraestructura más antigua esto no es posible y tratamos de alentar a las personas responsables para que no consideren las medidas de seguridad pública únicamente desde una perspectiva financiera. Si un análisis de seguridad/vulnerabilidad muestra que se debe mejorar la seguridad de cierta infraestructura, entonces un buen propietario/administrador debe abordar seriamente esta necesidad e invertir los fondos necesarios para garantizar su protección.

8.5.2. Concientización sobre la seguridad del personal durante el mantenimiento.

Otro aspecto de la seguridad pública en el mantenimiento está relacionado con los protocolos de seguridad pública que ya están implementados durante el funcionamiento normal de la infraestructura (controles de seguridad del personal y de los visitantes, cerraduras, alarmas, áreas restringidas, etc.). Cada trabajo de mantenimiento y reconstrucción de la infraestructura supone una desviación de los procedimientos operativos normales, pero eso no debería disminuir el nivel de protección física de esa infraestructura. Es muy importante que los empleados comprendan que los protocolos de seguridad pública deben adaptarse de tal manera que permitan realizar el mantenimiento de rutina o la reconstrucción sin comprometer la protección de la infraestructura. A los empleados y a los trabajadores subcontratados (que trabajarán en la infraestructura) se les debe informar de antemano de los cambios en los protocolos de seguridad pública (si es necesario, se recomienda una capacitación especial).

Los protocolos de seguridad pública deben adaptarse para permitir el movimiento seguro de múltiples personas subcontratadas (trabajadores) y equipos, para acceder, estar dentro y salir de la zona en mantenimiento o reconstrucción. Además, en la infraestructura de transporte, también debería habilitarse, en la medida de lo posible, la circulación segura del tráfico. Esto significa que todas las barreras de protección física, vallas, barreras anticolisión, etc., deben ser desmanteladas cuidadosamente, de acuerdo con un plan predefinido y un calendario de desmontaje, reparación/reconstrucción y reemplazo (ver **Figura 3**). La protección debe proporcionarse en todo momento, si es necesario se deben subcontratar los servicios para controlar la seguridad pública en la obra. En una frase, la seguridad pública en el mantenimiento puede ralentizar la velocidad a la que se llevan a cabo los trabajos de mantenimiento o reconstrucción, pero proporciona protección continua a la infraestructura, es decir, a cualquier hora.

8.6. COOPERACIÓN CON OTROS SERVICIOS

Si bien la seguridad vial y la salud del personal son los ejes principales de la política vial de las administraciones de las carreteras locales y nacionales, así como de las agencias de carreteras, la concientización sobre las cuestiones de seguridad pública suele ser muy escasa, sobre todo en las administraciones públicas.

De hecho, las AC tienden a dejar la seguridad pública a las fuerzas policiales y a los servicios de inteligencia, pero los equipos locales están acostumbrados a cooperar con los servicios de emergencia y las fuerzas policiales cuando ocurren accidentes. Por consiguiente, debería establecerse o mejorarse la cooperación con las fuerzas policiales en materia de seguridad pública.

Por otro lado, la seguridad de la infraestructura es un tema de gran importancia que no sólo afecta a la propia infraestructura, sino también al tráfico vehicular y, en consecuencia, al transporte de personas y mercancías. Las personas que utilizan el sistema de transporte pueden ser personas ilegales, vándalos, delincuentes, terroristas; los vehículos pueden ser utilizados como armas hostiles y para el tráfico de personas ilegales, armas, explosivos u otros dispositivos para cometer actos malintencionados.

La presencia en las carreteras de los servicios que se encargan del control de camiones y mercancías (aduanas) es muy útil, ya que también tienen como objetivo los vehículos comerciales ligeros (<3.5 T), que son la fuente de numerosas infracciones. También debe establecerse o mejorarse la cooperación con los servicios encargados del control de los vehículos de transporte de mercancías, así como de las mercancías en sí mismas.

La cooperación con otros servicios podría incluir:

- el suministro de imágenes (en tiempo real o diferido, incluida la identificación de las matrículas) grabadas en los centros de gestión del tráfico vehicular;
- la realización de patrullajes en la infraestructura que podría ser un blanco, durante períodos sensibles (alto riesgo de acciones terroristas). Algunos patrullajes podrían llevarse a cabo de manera coordinada o conjunta con la policía;
- el desarrollo de medios de comunicación rápida (teléfonos móviles seguros, radiofrecuencias específicas, etc.);
- la participación de los servicios viales en la seguridad de la infraestructura y de los usuarios durante las operaciones de seguridad pública llevadas a cabo por la policía y/o las aduanas;
- la participación de los servicios viales en el establecimiento de nuevos equipos o medios de vigilancia de la seguridad de las infraestructuras y del transporte por carretera;
- el uso común de aviones no tripulados (drones) para la inspección detallada de la infraestructura y la vigilancia de los puntos sensibles (desde el punto de vista de la seguridad pública);
- la implementación de sistemas de control reforzados y automatizados en las puertas de peaje para la red de carreteras “cerradas” (de acceso controlado), tales como autopistas de peaje, puentes de peaje o túneles de peaje;
- la capacitación que incluya la ciberseguridad;
- simulacros de intervención;
- información para asesores/gerentes de seguridad pública en administraciones de carreteras (que se defina un contacto regular con los servicios de inteligencia, la policía y las aduanas; especialmente, a nivel local y nivel nacional).

Podría ser interesante para los servicios viales crear una red a nivel nacional de oficiales de seguridad pública local. Podrían elaborarse acuerdos o memorandos de entendimiento entre los servicios viales, las fuerzas policiales y los servicios aduaneros a partir de un marco nacional que se difundiría a nivel local.

8.7. ASESOR DE SEGURIDAD PÚBLICA

En una organización, el "gerente de seguridad pública" es el experto encargado de la seguridad pública, el programa de capacitación y la motivación del resto del personal (que no sea de seguridad pública) para participar en la gestión general de la seguridad pública. Muchas organizaciones tienen un asesor de seguridad pública cercano al gerente general. Para las AC, este tipo de asesor es cada vez más importante para promover activamente la postura de seguridad pública en los servicios.

El asesor de seguridad pública es el responsable de ayudar a prevenir los riesgos inherentes a las actividades de la AC con respecto a las características de la infraestructura, las personas, los bienes y el medio ambiente. Las principales actividades del asesor son:

- el desarrollo de un curso de capacitación sobre seguridad pública,
- informar al personal sobre las cuestiones de seguridad pública cuando sea pertinente;
- aumentar la seguridad pública mediante el análisis de escenarios con los gerentes y la redacción de procedimientos;
- seguir las directrices, como por ejemplo la Directiva Europea de Túneles 2445/2004/54/EC;

- consultar con las fuerzas policiales y los servicios de rescate, así como preparar ejercicios o simulacros comunes de seguridad vial y seguridad pública.

Se debería realizar una capacitación especial para los gerentes de seguridad de la infraestructura carretera.

Dentro del estándar PAS 1192-5 [5], se considera el cargo de un "administrador de seguridad pública para los activos construidos".

9. CONCLUSIONES

El presente Informe aborda un tema que por su propia naturaleza es complejo, contemplando la necesidad de una síntesis con una visión amplia e integrada, centrada en todos los fenómenos que amenazan el mundo del transporte carretero y su infraestructura, de los cuales no todos pueden ser representados en un documento público. Dos elementos deben destacarse como conclusiones, en relación con la seguridad física y la ciberseguridad.

Les recuerdo que, al inicio de la actividad de este Grupo de Estudio (2015-2016), la crisis terrorista estaba en su punto álgido, especialmente en Europa, con atentados en varias capitales y ciudades. Hoy en día, la amenaza Yihadista no puede considerarse agotada por su derrota militar en el territorio y hay razones para pensar con la perspectiva de su resiliencia y capacidad de adaptación. Junto a los llamados "lobos solitarios" hay extremistas "en busca de autoría" y células dormidas que pueden suponer una amenaza para el mundo de la infraestructura y el transporte. Además, debido también a la pérdida de territorio, es razonable pensar en el retorno de una amenaza generalizada en el mundo como la de Al Qaeda a principios de siglo (autor de la destrucción de las Torres Gemelas de Nueva York en 2001). Por su parte, Daesh podía inspirar o atacar directamente, llevando a cabo asesinatos y ataques selectivos. El "riesgo cero" tampoco existe para las AC. Considerando que una acción delictiva, tal y como se manifestó en los últimos atentados terroristas, está motivada por el deseo de llevarla a cabo por cualquier medio, se analizó la identidad de aquellas acciones accidentales vinculadas a eventos maliciosos e intencionados, como los terroristas, proporcionando algunas indicaciones preliminares para el diseño de estructuras y sistemas, incluyendo también características de resiliencia y robustez.

El segundo tema a considerar es la amenaza cibernética, una amenaza paradigmática de nuestros tiempos, porque además de mantener en sí misma un gran potencial de daño -especialmente cuando afecta a la infraestructura crítica y estratégica- también es transversal a todos los demás fenómenos de amenaza. Es un reto que involucra a todos. El crecimiento de la cultura de la seguridad cibernética afecta, más allá de cada gobierno, a cada ciudadano, cada uno de nosotros en todos los niveles del gobierno y de la gestión corporativa debemos contribuir a aumentar el nivel general de seguridad del ecosistema cibernético, incluso en el campo de las carreteras, especialmente con los avances tecnológicos en curso. Estamos presenciando un fuerte aumento de las acciones hostiles que van en detrimento de las administraciones públicas centrales y locales, así como de las entidades privadas, incluidos los operadores del sector del transporte. Un hacker selecciona objetivos de acuerdo con la vulnerabilidad encontrada, para que sea factible con capacidades técnicas reducidas y a bajo costo. La exposición de la infraestructura ha aumentado, ya que el Internet de las Cosas se está difundiendo y los equipos no están integrados en los sistemas operativos desarrollados a la medida, por lo que se utiliza el software de código abierto. Por lo tanto, es necesario desarrollar campañas adecuadas de capacitación digital en el mundo de las AC, de tal manera que se estimule la concientización y la implementación de los nuevos estándares para lograr altos niveles de seguridad de redes y sistemas.

El Informe propone recomendaciones que se consideran útiles para prevenir las amenazas actuales. En este contexto, con vistas a un nuevo ciclo de la PIARC 2020-2023, somos conscientes de que debe prestarse la debida atención al aspecto interdisciplinario de las amenazas y al hecho de que una AC debe considerarlas todas juntas. El tema de la seguridad pública es transversal y, por lo tanto, está incluido en la mayoría de los temas tratados por otros Comités Técnicos y Grupos de

Estudio de la PIARC. En el ciclo actual, como Grupo de Estudio "Seguridad de las Infraestructuras", se ha llevado a cabo una investigación preliminar sobre los informes ya publicados por la PIARC, pero por razones de tiempo no ha sido posible desarrollar correlaciones reales con otras actividades en curso. Por lo tanto, en los Informes de los distintos cuerpos técnicos antes mencionados que se publicarán al final de este ciclo no habrá capítulos relativos a la seguridad pública, ni en este Informe se cuenta con correlaciones explícitas, aunque muchas de ellas serán implícitas. Se trata de una cuestión importante que debe integrarse en el próximo ciclo y que generará contribuciones directas a cada uno de los cuerpos técnicos de la PIARC. De esta manera, se pueden crear las correlaciones necesarias para llenar los vacíos existentes e introducir una evolución relevante en términos de un enfoque holístico y sin silos, que son esenciales para una estrategia eficaz en la seguridad de la infraestructura carretera y del transporte.

10. GLOSARIO Y ACRÓNIMOS

Término	Definición	Fuente
Activo	Un artículo de valor o importancia. Los activos pueden incluir elementos físicos, cibernéticos (sistemas de información y comunicación), humanos o para la supervivencia (conocimiento y funciones críticas).	Proyecto SeRoN [8]
Administración de Carreteras (AC)	Una Administración de Carreteras es una institución pública o privada que es propietaria o concesionaria de una o varias redes de carreteras y/o autopistas, encargada de su gestión operativa y mantenimiento. El punto de vista de este informe es el de una AC que se preocupa diariamente de las cuestiones de seguridad pública y de la protección de sus activos.	PIARC GE C.1
Amenaza	Cualquier circunstancia o evento con el potencial de causar la pérdida de un activo o su daño. En el caso del terrorismo, la amenaza representa la intención y la capacidad, así como el atractivo de ese activo en relación con otros activos alternativos. En el caso de los peligros "naturales", la amenaza se refiere a la frecuencia histórica (o estimada) del fenómeno natural al que puede estar sujeto el activo. En ambos casos, a efectos del análisis de riesgos, la amenaza se define como la probabilidad de que ocurra el evento.	Proyecto SeRoN [8]
Análisis cuantitativo de riesgos	Un método de análisis de riesgos basado en cálculos numéricos.	PIARC
Análisis de consecuencias	Procedimiento sistemático para describir y/o calcular las consecuencias.	PIARC
Análisis de probabilidad	Procedimiento sistemático para describir y/o calcular la probabilidad de un evento futuro.	PIARC
Análisis de riesgos	Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis de riesgos proporciona la base para la evaluación de riesgos y la toma de decisiones sobre el tratamiento de los riesgos.	ISO Guía 73
Apetito del riesgo	La "cantidad y tipo de riesgo que una organización está dispuesta a perseguir, retener o asumir". El apetito de riesgo es el nivel de riesgo que una organización está dispuesta a aceptar para lograr sus objetivos, y antes de que se considere necesario actuar para reducir el riesgo. Representa un equilibrio entre los beneficios potenciales de la innovación y las amenazas que el cambio trae inevitablemente. En un sentido literal, definir tu apetito significa definir qué tan "hambriento" estás de riesgo.	ISO Guía 73
Ataque ciber-físico	Un ataque ciber-físico es un ciberataque que tiene como objetivo dañar o desactivar componentes físicos de la infraestructura carretera, como cámaras, luces, ventilación, etc.	PIARC GE C.1
Carreteras inteligentes	Una infraestructura moderna con comunicación simultánea entre automóviles y la estación, la recopilación y el análisis de datos, el aligeramiento del congestionamiento vial así como el aumento del nivel de la seguridad vial y la seguridad pública deberían garantizar altos niveles de ciberseguridad.	PIARC
Centro de gestión de tráfico (CGT)	El Centro de Gestión de Tráfico o CGT es una estructura operativa en la que una AC puede recopilar datos y coordinar las situaciones y condiciones de tráfico y transporte. Puede interactuar con los responsables de la toma de decisiones de manera oportuna basándose en datos en tiempo real.	PIARC GE C.1
Ciberataque	Un ciberataque es un ataque a los sistemas informáticos con fines maliciosos. Se dirige a diferentes dispositivos informáticos: computadoras o servidores, aislados o en redes, conectados o no a Internet, equipos periféricos como impresoras o dispositivos de comunicación como teléfonos móviles, teléfonos inteligentes o tabletas. Hay cuatro tipos de riesgos cibernéticos con diversas	Gobierno francés http://www.gouvernement.fr/risques/risques-cyber

	consecuencias, que afectan directa o indirectamente a las personas, las administraciones y las empresas: ciberdelincuencia, daños a la imagen, espionaje y sabotaje.	
Conciencia (sobre la seguridad púbica)	La conciencia sobre la seguridad pública es el conocimiento y la actitud que los miembros de una organización poseen con respecto a la protección de los activos físicos, y especialmente informativos, de esa organización.	PIARC GE C.1
Consecuencia	Resultado de un evento que afecta a los objetivos. Un evento puede provocar una serie de consecuencias. Una consecuencia puede ser determinada o indeterminada y puede tener efectos positivos o negativos en los objetivos.	ISO Guía 73
Consecuencia local	La condición no deseada de un activo infligida por un impacto, expresada como daño físico o interrupción (tiempo fuera de servicio). Cuantificada en términos de costo de reparación y tiempo de interrupción: Consecuencia local = Valor expuesto × Vulnerabilidad	Proyecto AllTraIn [9]
Criticidad	La relevancia de un elemento o sección de la infraestructura para la disponibilidad de un sistema de infraestructura carretera.	Proyecto AllTraIn [9]
Daño	Lesión física o daño a la salud de las personas, o daño a la propiedad o al medio ambiente.	PIARC
Detección	La acción de ser consciente de la ocurrencia de un evento. [Generalmente, una detección puede ser humana (ver, escuchar, oler, etc.) o depender de un sistema (detección de calor, detección automática de incidentes, nivel de CO, etc.)]	PIARC
Escenario	Una combinación de eventos, estados del sistema y condiciones que conducen a un resultado de interés. Este conjunto de eventos y condiciones puede ser utilizado en una evaluación de riesgos u otro modelo. Por ejemplo, puede incluir una amenaza específica para un activo u objeto, con probabilidades y consecuencias asociadas.	Proyecto SeRoN [8]
Emergencia	Evento repentino e inesperado que requiere una acción inmediata debido a amenazas potenciales para la salud y la seguridad, el medio ambiente o la propiedad.	PIARC
Evaluación de riesgos	Proceso de comparación de los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.	ISO Guía 73
Evento	La ocurrencia de un conjunto particular de circunstancias, que pueden causar daño.	PIARC
Frecuencia	Número de eventos o resultados por unidad de tiempo definida.	ISO Guía 73
Gestión de la resiliencia	Actividades coordinadas para dirigir y controlar una organización con respecto a la resiliencia.	PIARC GE C.1
Gestión de riesgos	Actividades coordinadas para dirigir y controlar una organización en materia de riesgos.	ISO Guía 73
Incertidumbre	La incertidumbre es el estado, incluso parcial, de la deficiencia de la información relacionada con un evento, su comprensión o conocimiento, así como sus consecuencias o probabilidad.	ISO Guía 73
Incidente	Evento anormal e imprevisto (incluidos los accidentes) que afectan negativamente las operaciones y la seguridad vial del túnel.	PIARC
Infraestructura crítica	Un activo, sistema o parte del mismo que es esencial para el mantenimiento de las funciones sociales vitales, la salud, la seguridad vial, la seguridad pública, el bienestar económico o social de las personas, cuya interrupción o destrucción tendría un impacto significativo como resultado de no mantener dichas funciones" (cf. [CE, 2008]).	Proyecto SeRoN [8]
Ingeniería social	La ingeniería social es un término amplio que se refiere a actividades delictivas para engañar, embaucar y manipular a sus víctimas con el fin de obtener información confidencial o fondos. Los delincuentes se aprovechan de personas confiadas para averiguar sus datos bancarios,	www.interpol.int

	contraseñas u otros datos personales. Las estafas se llevan a cabo en línea, por ejemplo - por correo electrónico o a través de sitios de redes sociales - por teléfono o incluso en persona.	
Medidas con consecuencia global	Medidas que pueden activarse en función de los distintos niveles de riesgo y amenaza.	Directiva 2008/114/EC
Medidas de seguridad pública permanentes	Medidas que identifican las inversiones indispensables en materia de seguridad pública y los medios que deben emplearse en todo momento, como las medidas técnicas (incluida la instalación de medios de detección, control de acceso, protección y prevención); las medidas organizativas (incluyendo los procedimientos para las alertas y la gestión de crisis); las medidas de control y verificación; la comunicación; la concientización y la capacitación; y la seguridad de los sistemas de información.	Directiva 2008/114/EC
Peligro	Fuente potencial de daño.	PIARC
Personal de control	Todos los empleados que se ocupan de la gestión del tráfico y/o técnica.	PIARC
Plan de operación de emergencias	Plan que cada servicio o agencia y el organismo que opera el túnel tienen y mantienen para responder apropiadamente a los peligros.	PIARC
Preparación para emergencias	La disciplina que garantiza la preparación de una entidad para responder a una emergencia de manera coordinada, oportuna y efectiva.	PIARC
Probabilidad	Medida de la probabilidad de ocurrencia expresada como un número entre 0 y 1, donde 0 es la imposibilidad y 1 es la certeza absoluta. En este Informe, se usa también con el significado de la probabilidad de que algo suceda.	ISO Guía 73 PIARC GE C.1
Red carretera	El sistema completo de las rutas relacionadas con el transporte por carretera, disponible en un área en particular, generalmente toda la red de la que es responsable el usuario de este manual.	Proyecto SecMan
Redundancia	La redundancia es la presencia adicional de recursos funcionalmente idénticos o comparables de un sistema técnico, si normalmente no son necesarios para un funcionamiento sin problemas.	PIARC GE C.1
Resiliencia	La resiliencia es la capacidad de una organización para evitar o resistirse a ser afectada por un evento o la capacidad de volver a un nivel aceptable de rendimiento, en un período de tiempo aceptable, cuando se ve afectada por un evento.	ISO 28001:2001
Resiliencia cibernética	La resiliencia cibernética se refiere a la capacidad de ofrecer continuamente el resultado deseado a pesar de los eventos cibernéticos adversos.	PIARC GE C.1
Resiliencia de la infraestructura	La resiliencia de la infraestructura es la capacidad de reducir la magnitud y/o duración de los eventos perturbadores. La eficacia de una infraestructura o empresa resiliente depende de su capacidad para anticiparse, absorber, adaptarse y/o recuperarse rápidamente de un evento potencialmente perturbador.	PIARC GE C.1
Riesgo	Efecto de la incertidumbre sobre los objetivos. El riesgo se caracteriza a menudo por la referencia a eventos potenciales y las consecuencias. El riesgo se expresa a menudo en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la probabilidad de ocurrencia asociada.	ISO Guía 73
Sección carretera	Es un extracto definido de una parte de una red de carreteras, basado en las diferencias en los parámetros de tráfico vehicular.	Proyecto SecMan [19]
Seguridad pública (*security*)	Las amenazas a la seguridad pública se refieren a daños intencionales, como el comportamiento ilegítimo o delictivo deliberado. Las amenazas a la seguridad pública incluyen, entre otras, ataques terroristas, piratería, ataques cibernéticos, etc.	Maria G. Burns: Logistics and Transportation Security, A Strategic, tactical and operational Guide to Resilience, CRC Press, 2016;

		Bernard Besson et Jean Claude Possin IFIE (institut français de l'intelligence économique)
Seguridad vial (*safety*)	Las amenazas a la seguridad vial se refieren a desastres naturales (como huracanes, inundaciones, terremotos, etc.) o actividades humanas no intencionales, como negligencia, error humano, daños accidentales, etc.	Maria G. Burns: Logistics and Transportation Security, A Strategic, tactical and operational Guide to Resilience, CRC Press, 2016; Bernard Besson et Jean Claude Possin IFIE (institut français de l'intelligence économique)
Servicios de emergencia	Bomberos, policías y médicos.	PIARC
Situación crítica	Situación (congestionamiento vehicular, avería del vehículo, accidente, incendio) que requiere una atención especial o acción por parte de los usuarios.	PIARC
Terrorismo	El terrorismo es el uso ilegal o la amenaza de uso de fuerza o violencia contra individuos o propiedades para coaccionar o intimidar al gobierno o a las sociedades, a menudo para lograr objetivos políticos, religiosos o ideológicos.	PIARC GE C.1
Tratamiento del riesgo	Proceso para modificar el riesgo.	ISO Guía 73
Vandalismo	El vandalismo es el daño ilegal deliberado, la degradación o destrucción de propiedades como un fin en sí mismo.	PIARC GE C.1
Vulnerabilidad	Las características y circunstancias de una comunidad, sistema o activo que lo hacen susceptible a los efectos dañinos de un peligro (amenaza, evento). Está vinculada al riesgo por un evento o escenario específico.	Proyecto SeRoN [8]

11. REFERENCIAS

[1] WRA-PIARC TASK FORCE 2 ON SECURITY *"Security of road infrastructure – Final Report"*, referencia 2015R01EN, WRA-PIARC, París, 2015

[2] Palchetti S., *Introduction to terrorism and road security*, April 27 2017, PIARC GE C.1

[3] Palchetti S., "Upgrade from beginning 2017 : a journalistic report", 14 de septiembre 2017, PIARC GE C.1.

[4] *Standard on BIM Security* https://www.cpni.gov.uk/building-information-modelling

[5] PAS 1192-5 *Specification for security-minded building information modelling, digital built environments and smart asset management*, CNPI, mayo 2015, enlaces disponibles en: http://shop.bsigroup.com/ProductDetail/?pid=000000000030314119; https://www.cpni.gov.uk/open-data

[6] HB 167:2006 *Security risk management handbook*, New Zealand Standards

[7] CPNI*, Integrated Security – A Public Realm Design Guide for Hostile Vehicle Mitigation*, Segunda Edición, 2014.

[8] SERON *"Security of Road Transport Networks"*, proyecto de la Unión Europea, terminado en 2012, disponible en https://www.seron-project.eu.

[9] ALLTRAIN *"All-hazard guide for transport infrastructure"*, proyecto de la Unión Europea, terminado en 2015, disponible en https://www.alltrain-project.eu

[10] NIST SP 800-53A methodology.

[11] CYBER-SAFE "*Schutz von Verkehrs- und Tunnelleitzentralen vor Cyber-Angriffen*", proyecto nacional alemán, terminado en 2018, disponible en: www.bast.de/cyber-safe

[12] ESIMAS *"Echtzeit-Sicherheits-Management-System für Straßentunnel"*, proyecto nacional alemán, terminado en 2015, disponible en https://www.esimas.de.

[13] SKRIBT and SKRIBTplus *"Schutz kritischer Brücken und Tunnel im Zuge von Straßen"*, proyecto nacional alemán, terminado en 2013, disponible en https://www.skribt.org.

[14] Palchetti S., *Workshop "Road infrastructure security"*, Instant Book, PIARC Roma, Italia, 7 de abril 2017.

[15] AMIVTAC - Instituto Mexicano del Transporte, Workshop "Seguridad y proteccion de infraestructura crítica", Instant Book, Querétaro, México, 8 de junio, 2017.

[16] AASHTO *Fundamental Capabilities of Effective All-Hazards Infrastructure Protection, Resilience, and Emergency Management for State Departments of Transportation*. American Association of State Highway and Transportation Officials, Washington, 2015.

[17]Ernest R. Frazier, Yuko J. Nakanishi and Mary Ann Lorimer*: Security 101: A Physical Security Primer for Transportation Agencies*. Surface Transportation Security, Volumen 14. National cooperative highway research program, Transportation research board, Washington, 2009.

[18] RADVANOVSKY, R. *"Critical infrastructure (Homeland security and emergency preparedness)"*, Taylor & Francis Group, Nueva York, 2006.

[19] SECMAN *"Security risk management processes for road infrastructure"*, proyecto de la Unión Europea, terminado en 2013, disponible en https://www.secman-project.eu.

APÉNDICES – EN REFERENCIA AL CAPÍTULO 7. "ESTUDIOS DE CASO"

APÉNDICE 1.1 : EXPLOSIÓN DE UNA BOMBA SUCIA EN UN ÁREA URBANA

Introducción

El estudio de caso propuesto es un ejemplo de ejercicio de defensa civil sobre las consecuencias de una explosión de una bomba sucia en un centro logístico intermodal privado, situado en un área suburbana. Dicha explosión causa una fuga de contaminantes radioactivos en una amplia área urbana. Un día de acción está representado de las 5 a.m. a las 4 p.m.

En el escenario propuesto, los servicios de inteligencia habían comunicado información sobre un presunto transporte ilegal, probablemente por el seguimiento de las actividades de búsqueda en la web; sin embargo, la información sigue siendo prácticamente infructuosa. Debido a la falta de procedimientos, no se difundió ninguna comunicación en todos los niveles. La policía y todos los Centros de Gestión de Tráfico fueron alertados, pero el centro intermodal no recibió ninguna alarma, al igual que otra plataforma privada. En cualquier caso, el centro logístico intermodal no estaba preparado para un evento de seguridad pública. Además, los Centros de Gestión de Tráfico no tienen procedimientos de seguridad pública, por lo que sólo podrían controlar los videos en las autopistas y carreteras si eventualmente se detectara el contenedor en el camión que lo transporta.

El Sistema Italiano de Manejo de Crisis de la Defensa Civil lleva a cabo periódicamente un simulacro oficial de atentado terrorista en diferentes áreas del territorio nacional para comprobar el comportamiento real del sistema en caso de un atentado. El escenario propuesto es una adaptación simplificada de un gran ejercicio en un centro urbano italiano en el que participan todas las estructuras locales y nacionales de la administración pública a cargo de las crisis.

Contexto

Un centro logístico intermodal es una infraestructura especial dedicada a reunir en una misma zona una terminal carretera y una estación ferroviaria que atiende mercancías transportadas en contenedores marítimos, cajas intercambiables y semirremolques, vagones especiales para cargas a granel y automóviles. Un centro logístico intermodal no se considera una infraestructura crítica y, por lo tanto, no tiene preparación específica para la seguridad pública. Una postura de prevención inadecuada provoca consecuencias muy graves que van mucho más allá de la infraestructura privada. Las fuerzas policiales y los cuerpos de bomberos desempeñan sus funciones con diligencia.

Nuestro interés es el punto de vista de una Administración de Carreteras (AC) en situaciones de caos, incidentes, siniestros, congestionamiento y su implicación a diferentes niveles:

- la interacción entre las estructuras de seguridad pública y los propietarios/operadores privados (como el propietario del centro logístico intermodal);
- la interacción y las interdependencias con diferentes propietarios/operadores de infraestructura (carreteras, ferrocarriles, metro, red eléctrica, telecomunicaciones);
- la interacción con la ciudadanía a través de comunicaciones apropiadas;
- la disponibilidad de la red de carreteras, la gestión adecuada de las carreteras principales, las carreteras secundarias y los puntos de interés como cruceros y conexiones, así como un centro logístico intermodal.

Un aspecto relevante está relacionado con las condiciones climáticas, al inicio del ejercicio había brisa proveniente del Noroeste y la nube contaminante estaba dirigiéndose hacia el Sureste, para investir en el área urbana de la gran ciudad. En las siguientes 72 horas se esperaba una disminución del viento y de la lluvia.
En el escenario, tenemos cuatro fases:

i. la fase de alerta,
ii. la fase de ataque(s),
iii. la fase de respuesta (bomberos, patrullas de policía, Administración de Carreteras para gestionar los puntos de cierre de la infraestructura, las colas y los desvíos, los equipos de primeros auxilios, etc.)
iv. la fase de descontaminación, con la participación de personas y medios: vehículos, trenes, etc.

La última fase de descontaminación no se describirá en la acción. Las autoridades públicas tienen que declarar los límites con acceso prohibido de las zonas contaminadas. La definición de una "zona roja", la detención de cada tipo de tráfico, carretero, ferroviario y aéreo, la necesidad de descontaminar a los automóviles, trenes y personas crea problemas muy difíciles de gestionar y la falta de preparación agrava todo el proceso. Las personas directamente involucradas deben permanecer en las áreas contaminadas y deben evitar cualquier contacto dentro y fuera de esos lugares. Todas las medidas de descontaminación se mantendrán durante un tiempo indeterminado, también en función de las condiciones climáticas y de los efectos de la contaminación en la salud de la población a mediano y largo plazo.

Amenaza y objetivos

La amenaza en este escenario se refiere al transporte de sustancias radioactivas, biológicas y químicas, que es absolutamente legal pero no está bajo ningún control por la ley, y que se pueden utilizar para causar daños graves. El escenario radiactivo es más impredecible debido a las condiciones climáticas que afectan el movimiento de la nube contaminante. Por otro lado, el escenario químico está más localizado y su desplazamiento puede predecirse en relación con la sustancia.

La amenaza proveniente específicamente de un DDR, Dispositivo de Dispersión Radioactiva, llamada bomba sucia, funciona simplemente con un explosivo detonante de material radioactivo. El impacto previsto sobre los ciudadanos y el tráfico por carretera es intenso, con daños tremendos en una gran área debido a la dispersión de una nube contaminante. Los casos "involuntarios" de bombas sucias pueden afectar a vehículos que transportan combustibles como gasolina o diésel, con graves consecuencias en términos de vidas (ver al final de este escenario los ***Eventos comunicados por la prensa***) humanas y en la infraestructura, incluso si tienen menos impacto en el territorio.

En este escenario, el objetivo de la acción terrorista es paralizar una gran parte de una red de infraestructura nacional mediante la dispersión de cesio 137 y cobalto 60, causada por la explosión de un contenedor marítimo que se encuentra sobre un camión en un centro logístico intermodal. Las consecuencias afectan, en particular, al transporte por carretera (y ferrocarril) y, por supuesto, a toda la población de un área urbana y sus alrededores. Los daños físicos, psicológicos y económicos son considerables.

El ataque golpea a un lugar de trabajo -el centro logístico intermodal- e indirectamente a través de la contaminación, al entretenimiento, la salud, la educación, que son las esferas que afectan la vida diaria de una comunidad más amplia, e incluso impactan a la opinión pública de una nación. El atentado terrorista produce, en consecuencia, una comunicación agresiva que pretende desestabilizar localmente la vida cotidiana de una comunidad productiva, con un intenso movimiento diario de transporte por carretera.

Probabilidad y riesgo

En el mundo desarrollado, por muchas razones, el uso de fuentes radioactivas es muy elevado y no es inconcebible que un grupo terrorista pueda tomar posesión de ellas. Existen miles de fuentes radioactivas utilizadas para diferentes fines: médicos o industriales. Si no se mantienen seguras, pueden dar lugar a accidentes, contaminación y a la muerte de personas. Entonces, se puede considerar un evento de "baja probabilidad y alto impacto". Los daños económicos pueden estimarse en unos millones de euros.

El manejo del material radioactivo es, sin duda, para especialistas, porque es muy peligroso y los involucrados estarían en alto riesgo de contaminación y muerte antes de realizar un ataque. Sin embargo, la amenaza radioactiva parece más probable que un ataque químico o bacteriológico, ya que estos últimos son mucho más complicados de organizar. El terrorismo ha mostrado interés en experimentar con este tipo de dispositivos.

En el escenario, se considera que los terroristas son ciudadanos europeos, como en la mayoría de los casos de actos terroristas ocurridos desde el 2013 en toda Europa. Este es el llamado terrorismo molecular que implica la actividad de los "lobos solitarios". En el escenario propuesto, la complejidad de las acciones puede ser realista según la posibilidad probada de que los sujetos europeos reciban instrucciones a través de mensajes encriptados por parte de células terroristas ubicadas en África o el Medio Oriente.

Descripción

EXPLOSIÓN DE UNA BOMBA SUCIA EN UN ÁREA URBANA	
Parámetro	**Descripción de eventos**
Naturaleza del incidente	*La dispersión radioactiva empezó desde un gran centro logístico intermodal para bloquear la infraestructura circundante, en un crucero carretero importante y para contaminar el área urbana cercana.*
Tipo de incidente	*Una bomba sucia o Dispositivo de Dispersión Radioactiva (DDR), funcionando como un explosivo que detona con material radioactivo para contaminar una gran área.*
Hora del incidente	*En la mañana, durante la hora pico para ingresar al centro logístico intermodal.*
Objetivo (blanco)	*Tráfico vehicular en la infraestructura carretera (y el ferrocarril) y la población del área.*
Número de atacantes	*Dos terroristas en tres acciones criminales paralelas.*
Severidad del incidente	*El incidente afecta cruceros importantes de la infraestructura nacional, alrededor de la ciudad. Se ve afectado el tráfico carretero y ferroviario, en general, el transporte y la población entera de un área urbana, así como los alrededores. El impacto previsto sobre los ciudadanos y el tráfico por carretera es intenso, y la comunicación para decir que "mantengan la calma"*

	es muy problemática en el caso de un ataque radioactivo. Los diferentes problemas que surgieron van desde la definición de una "zona roja" hasta el bloqueo de cada tipo de tráfico carretero, ferroviario y aéreo. La necesidad de descontaminar los automóviles, los trenes y las personas crea problemas muy difíciles de manejar; y la falta de planeación por parte de la Autoridad Carretera, p. ej. sobre las rutas alternas congestionadas, agrava todo el proceso. Como consecuencia, el transporte de carga y personas se ve obstruido.
El progreso del incidente	*Se desarrollaron tres acciones criminales al mismo tiempo en un día, entre las 5 a.m. y las 8 a.m., en el área de una ciudad importante, que es afectada progresivamente por una nube contaminante. La ciudad está localizada en una región plana entre una autopista (al norte) y varias carreteras tanto nacionales como urbanas (alrededor). También está localizada en el crucero de ferrovías nacionales y regionales (al oeste, sur, este). Un gran centro intermodal, con cerca de 4000 movimientos de vehículos pesados al día, está localizado en los suburbios al norte de la ciudad, cercano a una salida hacia la autopista y directamente conectado a la línea de ferrocarril (con una terminal adentro). Desde dicho centro intermodal una nube contaminante es liberada y se dispersa hacia la ciudad debido al viento desfavorable. El pronóstico de que habrá lluvia favorece la detención de la nube con sus consecuencias en tierra.* *<u>Acción A:</u> dos inmigrantes fueron arrestados después de un tiroteo. En un camión que transportaba cloro se detectó un detonante para ser activado a través de un celular, por lo que generaría una explosión.* *<u>Acción B:</u> un accidente que involucra un camión cisterna que transporta gasolina y diésel (robado con la complicidad del conductor) y algunos automóviles en el cruce de una autopista que conecta la ciudad con el centro intermodal, el objetivo es hacer más lento el rescate.* *<u>Acción C:</u> en el centro intermodal se produce una explosión, en la terminal ferroviaria junto al área de estacionamiento de los camiones que transportan contenedores, en donde había también muchos contenedores. Los bomberos tienen dificultades para llegar al lugar debido al congestionamiento vehicular que produjo el accidente del camión cisterna, también porque algunos de ellos ya habían sido asignados a la extinción del incendio provocado por el camión cisterna. La radioactividad es detectada en uno de los contenedores involucrados en la explosión y una zona roja fue establecida en el área del centro intermodal. Se produce una nube radioactiva y es necesario emitir una comunicación para bloquear el paso de vehículos e informar a la población civil. La nube se mueve lentamente hacia la ciudad*
Consecuencias inmediatas en la infraestructura	*Bloqueo del tráfico en la carretera y el ferrocarril, en todos los niveles alrededor de la ciudad y en el centro intermodal, permitiendo la intervención de los vehículos de rescate, se requirió establecer rutas alternas incluso para largo itinerario. La necesidad de descontaminación y de gestionar el personal de rescate en las carreteras. La necesidad de crear coordinación para dar directrices y gestionar la comunicación durante la crisis.*
Número de víctimas	*Las explosiones provocaron otros accidentes automovilísticos, además del causado por el ataque criminal. La zona roja generó pánico. Las fuerzas de rescate no pudieron rescatar a todas las personas implicadas.*
Eventos secundarios	*En las rutas alternas congestionadas ocurrieron más accidentes. La contaminación originó consecuencias que no pudieron ser estimadas inmediatamente.*
Respuesta de los servicios de emergencia	*Los bomberos y los equipos de rescate se activaron rápidamente, pero la intervención se vio complicada por el evento distractor producido por el accidente del camión cisterna, que sirvió para bloquear las calles y crear confusión. Su llegada al área contaminada se ralentizó debido al caos en las carreteras. La Unidad de Gestión de Crisis de la Prefectura de la Ciudad inició*

	inmediatamente la coordinación de las operaciones. La compañía dueña del camión cisterna podría haber sido más cuidadosa en la detección del robo y, por lo tanto, dar la alarma en primer lugar.
Reportes de los medios de comunicación	*El ataque se produjo en la mañana durante la hora pico, en un crucero importante de la infraestructura nacional. La Dirección del centro intermodal tenía una lista de transportistas a los que les dio aviso para que ya no mandaran sus camiones y también dio inmediatamente aviso a la Prefectura de la Unidad de Crisis y, directamente, a la AC. Ésta última proporcionó información a los ciudadanos a través de la policía y a los operadores carreteros, de las autopistas y ferroviarios, quiénes difundieron, en los paneles de mensaje variable, las noticias del incidente y las acciones que se debían realizar.* *Al mismo tiempo, todos los medios de comunicación fueron informados del ataque, debido a la difusión total de la información prácticamente en tiempo real y sin ninguna posibilidad de control a través de las redes sociales y de los teléfonos inteligentes.*
El papel de la AC en el proceso de respuesta	*La AC debe ser informada por la policía y las fuerzas de rescate, y directamente por parte del centro intermodal, de tal manera que se pueda gestionar el bloqueo del tráfico en la infraestructura. Hubo víctimas. Especialistas para la descontaminación se involucraron para apoyar en la gestión de la crisis. El problema radica en la descontaminación de las carreteras y su restauración. Los problemas de gestión: ¿quién piensa limpiar después – existen los recursos- los barrederos? ¿Qué agua utilizar? Asegurar el paso de las ayudas.*

Resiliencia del sistema de la infraestructura carretera

La resiliencia del sistema de la infraestructura carretera depende de la capacidad para reaccionar rápidamente ante el atentado, a diferentes niveles, para evitar las consecuencias negativas (respuesta, recuperación) del atentado terrorista a todos los niveles: el centro intermodal, las carreteras locales y vialidades urbanas, las carreteras departamentales y nacionales, las autopistas, otro tipo de infraestructura y los servicios de rescate.

Ésta requiere una preparación adecuada previa al incidente (preparar, prevenir, proteger). Se postula que la organización de la Defensa Civil Nacional tuvo un buen desempeño: los cuerpos de brigadas contra incendios y manejo de material QBRN (Químico, Biológico, Radioactivo y Nuclear) son los primeros en llegar al área del ataque, se ejecutó según lo previsto la planificación integral establecida entre la Prefectura, el cuerpo de bomberos y las empresas municipales para compartir tanto los sistemas de videovigilancia como las comunicaciones, y, por último, se implementó y funcionó de manera excelente la Dirección única de información sobre movilidad, que permite a todos los operadores colaborar a través de sus respectivas estructuras.
Siguiendo el escenario propuesto, desde el punto de vista de una AC, nos centraremos entonces en la debilidad y la deficiencia en los cuatro dominios de participación, definidos anteriormente, en el contexto de:

- la interacción entre las estructuras de seguridad pública y los propietarios/operadores privados;
- la interacción y las interdependencias con diferentes propietarios/operadores de infraestructura (carreteras, ferroviarias, metro, red eléctrica, telecomunicaciones);
- la interacción con la ciudadanía por medio de comunicaciones adecuadas;
- la disponibilidad de la red de carreteras, la gestión adecuada de las carreteras principales, carreteras secundarias y los puntos de interés como cruceros y conexiones, así como un

centro logístico intermodal.

Hay que destacar los problemas que plantea una prevención inadecuada - que en sí mismos no son complejos ni costosos - porque pueden producirse consecuencias muy graves que van mucho más allá de los límites de la infraestructura privada. La moraleja es que: las fuerzas policiales y los cuerpos de bomberos no son suficientes y es necesario tomar conciencia de la necesidad de un amplio enfoque orientado a la seguridad pública, que incluya también a las entidades privadas (y, si es necesario, incluso a la ciudadanía). El eslogan es "si ves algo, dilo" (campaña que nace de la recomendación del Departamento de Seguridad Pública de EE. UU. en 2010). Son entonces fundamentales: los controles rutinarios del territorio (también privados), la detección de señales que denotan situaciones potencialmente anómalas (por ejemplo, el centro intermodal no registró quién entró y quién salió, ni tampoco registró los camiones que estaban estacionados en el interior sin los conductores).

Con respecto a los vehículos que transportan mercancías peligrosas, se debe considerar que el vehículo es un arma que circula y es un blanco que puede ser alcanzado. Por lo tanto, además de los controles y verificaciones, sería importante conocer la posición en tiempo real del vehículo, para evitar el robo o secuestro para pedir rescate y establecer una prohibición de paso en ciertas áreas.

Sin una cooperación preventiva, la libertad fundamental de circulación en el territorio europeo puede traducirse en una libertad para organizar ataques. Lo que impone tomar conciencia de la necesidad de vigilancia y seguimiento. Conseguir una mayor integración y cooperación eficiente en la relación público-privada no es un problema nuevo ni complejo.

En las siguientes fases del ciclo de la resiliencia se identifican problemas técnicos, organizativos y del personal.

<u>En la fase de preparación:</u>

- la falta de un proyecto de seguridad pública por parte del propietario/administración del centro intermodal conduce a la falta de procedimientos de control, no se establece un plan de alarma para los clientes/empresas de transporte y para la población vecina, lo que resulta en un alto nivel de vulnerabilidad de los bienes y el territorio;
- la falta de un proyecto de seguridad pública por parte de las empresas de carreteras y autopistas impide la definición de procedimientos adecuados para el funcionamiento de los centros de control, que no tienen capacidad preventiva, lo que se traduce en un alto grado de vulnerabilidad de la infraestructura carretera en relación a los vehículos que transportan mercancías peligrosas, y en la imposibilidad de cooperar mediante la transmisión de datos sobre los tránsitos vehiculares a otros centros;
- difundir la cultura y la capacidad de compartir y colaborar, la AC no puede hacerlo sola, las entidades deben hablar y colaborar entre sí.

<u>En la fase de prevención</u>:

- no hay control de los accesos/salidas de aproximadamente 4000 vehículos que usan diariamente la infraestructura (sólo un boleto a la entrada para ser entregado a la salida);
- no hay control de los espacios interiores (también llamados propiedades en condominio) y, en particular, de las áreas de estacionamiento y del comportamiento de los conductores;
- no hay control en las zonas que la AC considera sensibles;
- los sistemas de videovigilancia proporcionan imágenes que no se procesan posteriormente por razones de seguridad pública;
- no hay sensores específicos;
- no hay personal capacitado que pueda intervenir mientras se espera la llegada de los

vehículos de rescate;
- no hay control en los andenes de la estación de tren;
- no existe una lista de contactos (puntos de enlace) para el caso de las comunicaciones urgentes, en particular a las empresas de transporte;
- falta de controles y verificación de rutas, de las relaciones con empresas privadas que producen y transportan, especialmente para el transporte más crítico, por ejemplo, el cianuro y el cloruro de vinilo.

En la fase de protección:

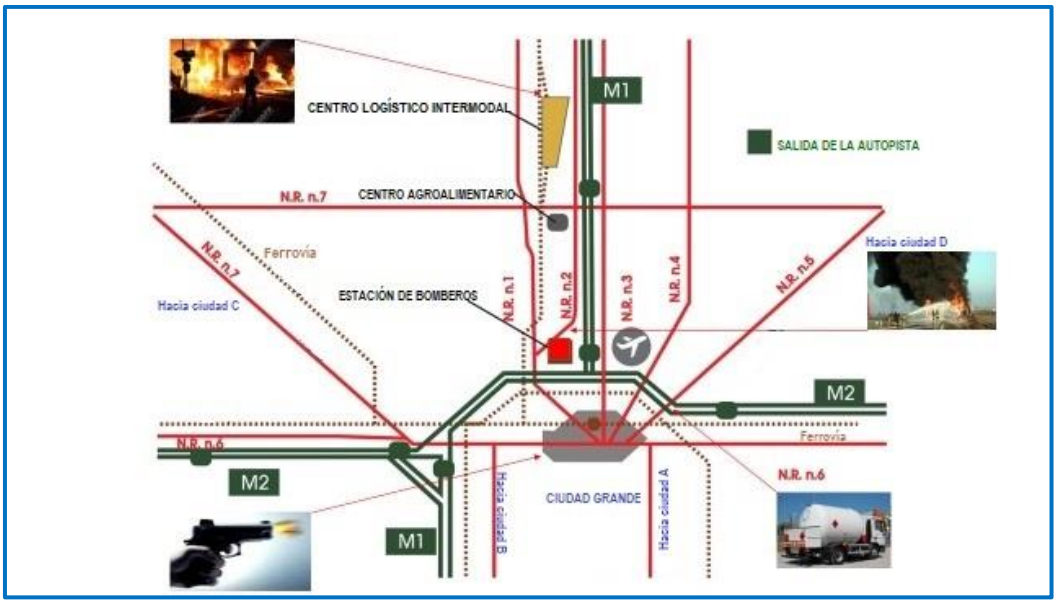
- la falta de comunicación por parte de las autoridades públicas hace que el centro intermodal y las autopistas sean incapaces de reaccionar, de alguna manera, ante la situación;

En la fase de respuesta:

- la prevención y la protección no pueden impedir el ataque y sus efectos y, por lo tanto, el acto delictivo se desarrolla sin control;
- está claro que la capacidad de reacción es muy importante y, por lo tanto, las primeras 3-4 horas esenciales se perdieron debido a la falta de preparación;
- un gran problema es el manejo de la comunicación correcta para gestionar a la población, una comunicación para decir "mantén la calma" es ineficaz o contraproducente;
- el sistema de coordinación del tráfico funciona pero en una red totalmente desprevenida, por lo que es necesario decidir los bloques y las salidas que requieren aproximadamente 500 personas y 100 vehículos, que a su vez necesitan tiempo para ponerse en marcha;
- mientras tanto, las mercancías destinadas al lugar del ataque llegan a la entrada y contribuyen a la parálisis del tráfico, involucrando no sólo las carreteras locales y nacionales sino también las autopistas, lo que impide la llegada de los vehículos de emergencia.
- se define una zona roja en el centro intermodal que es una medida no planificada, lo que crea confusión y pánico, con fuga de los vehículos de transporte que perforan las vallas en cada lado, lo que provoca la dispersión de los vehículos probablemente contaminados a lo largo de la red de carreteras locales;
- la capacidad de la policía para patrullar el territorio evitó la explosión del camión cisterna de transporte de cloro.

En la fase de recuperación:

- no existe un plan de continuidad de negocio que mitigue los efectos del ataque, que desafortunadamente fue exitoso, en toda la infraestructura; el máximo resultado se obtuvo con el mínimo esfuerzo;
- se debe considerar la necesidad de usar equipos de limpieza que actualmente no se suministran, con las responsabilidades y habilidades correspondientes.

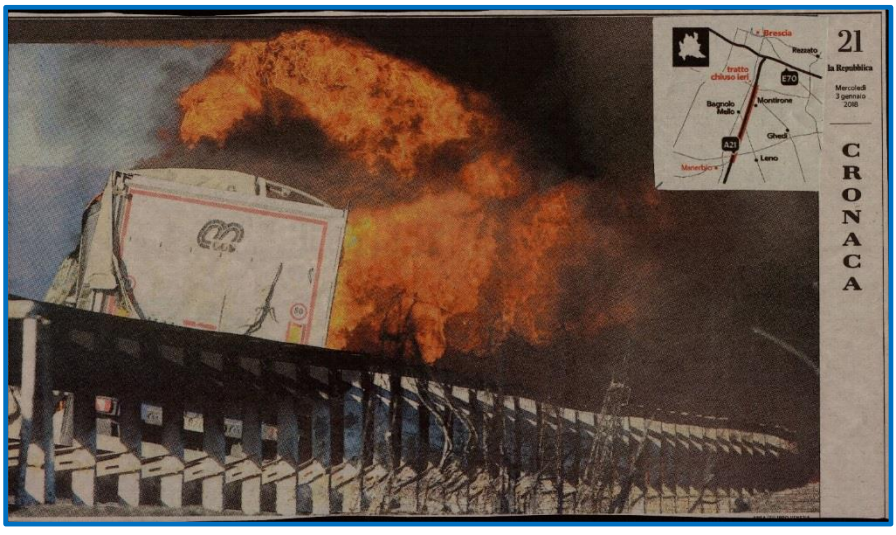


El escenario de una bomba sucia en un área urbana

Eventos comunicados por la prensa

ACCIDENTE EN ITALIA, EN LA AUTOPISTA A21, QUE AFECTÓ A DOS VEHÍCULOS PESADOS, INCLUYENDO UN CAMIÓN CISTERNA CON COMBUSTIBLE DIÉSEL Y UN AUTOMÓVIL CON UNA FAMILIA DE CINCO PERSONAS; TODOS MURIERON JUNTO CON UNO DE LOS CONDUCTORES

El 3 de enero de 2018, en la autopista A21 Turín-Brescia cerca de Brescia, el conductor de un camión, que transportaba cereales, al no darse cuenta de que una cola de vehículos frenaba delante él, se estrelló violentamente contra un automóvil con cinco personas a bordo. El automóvil quedó prensado contra el camión cisterna que le precedía, cargado con combustible diésel y que se convirtió en un detonador que causó un gran incendio. El accidente ocurrió bajo un puente que sufrió daños. El saldo fue de seis muertos, además de la interrupción del tráfico durante algunas horas y la necesidad de realizar controles estáticos en el puente.



APÉNDICE 1.2 - ATAQUE CIBER-FÍSICO A UN CENTRO DE CONTROL DE TÚNELES.

Introducción

En un centro de control de túneles ubicado en el sur de Alemania, que controla túneles importantes para el tráfico hacia Francia, Suiza y Austria, se produjo un ataque de *ransomware* (programa que bloquea el acceso a los dispositivos y que pide un rescate). Los delincuentes cibernéticos lograron encriptar los archivos y manipular los PLC (controladores lógicos programables) que bloqueaban el acceso a los sistemas de monitoreo y control de túneles.

El ataque se llevó a cabo utilizando un troyano, que se disfrazó como documentos adjuntos a una solicitud para una vacante vigente de trabajo. Se engañó al usuario para que abriera el archivo adjunto del correo electrónico y el *ransomware* viajó automáticamente desde las Tecnologías de Información (TI) de la oficina a las TI del control de túneles, ya que ambos sistemas no estaban físicamente separados entre sí. Después de que el *malware* se infiltró en el sistema de control de túneles, apareció un mensaje en las pantallas de la computadora, que informaba al usuario de que los datos se habían encriptado y que serían descifrados tras el pago de 1 Bitcoin (aproximadamente 7,000.00 €).

La policía y los equipos de rescate fueron informados inmediatamente. Su llegada a los túneles afectados se retrasó debido al caos en las carreteras. También se informó al Grupo para la Gestión de Crisis del Ministerio de Transporte, a la Oficina Federal de Seguridad de la Información y al Buró Federal de Investigaciones, quiénes comenzaron a trabajar lo antes posible.

Después de su propagación en el sistema de control de túneles, el *ransomware* comenzó a manipular los PLC para provocar falsas alarmas, también bloqueó todos los sistemas operativos. El *ransomware* logró apagar la iluminación en todos los túneles, lo que provocó accidentes vehiculares. Las fuerzas de rescate tuvieron problemas para rescatar a todas las personas involucradas. Debido a la pérdida de operaciones y control, cuarenta y cuatro túneles tuvieron que cerrarse localmente a través del control manual. Esto condujo a efectos en cascada como rutas alternas congestionadas y también afectó el tráfico vehicular hacia los países vecinos. En consecuencia, el transporte de mercancías y personas quedó obstruido. En las rutas alternas congestionadas se produjeron más accidentes que de costumbre, por lo que las fuerzas de rescate estuvieron trabajando constantemente.

A pesar de que se realizó el pago del rescate, los atacantes no proporcionaron la clave de descifrado. El operador tuvo que limpiar todos los sistemas de TI con la ayuda de especialistas externos. Durante el tiempo de recuperación de seis semanas, sólo los túneles más importantes fueron operados localmente con mayores requisitos de seguridad vial, tales como menores límites de velocidad y un número limitado de vehículos que podían pasar al mismo tiempo por ellos.

El ataque ocurrió durante la hora pico. En el lapso de una hora, todos los medios de comunicación cubrieron el ataque. La comunicación con los medios de comunicación fue coordinada por el Grupo para la Gestión de Crisis del Ministerio de Transporte.

Descripción

ATAQUE CIBER-FÍSICO A UN CENTRO DE CONTROL DE TÚNELES	
Parámetro	**Descripción de eventos**
Naturaleza del ataque	*Ataque con "ransomware": ataque criminal para bloquear el acceso al monitoreo y control de túneles hasta que se pague un rescate.*
Tipo de ataque	*Extorsión a través de la encriptación de archivos y la manipulación de los Controladores Lógicos Programables (PLC, por las siglas en inglés de "Programmable Logic Controller").*
Hora del ataque	*En la mañana, durante la hora pico.*
Objetivo (blanco)	*Infraestructura carretera (centro de control de túneles).*
Número de atacantes	*Un grupo organizado de ciberdelincuencia.*
Severidad del ataque	*Veinte túneles que estaban bajo el control del centro de control de túneles tuvieron que ser cerrados, porque no se pudo garantizar la operación segura de los túneles. Esto provocó efectos en cascada, como el congestionamiento de rutas alternas. En consecuencia, el transporte de mercancías y personas quedó obstruido. A pesar de que se realizó el pago del rescate, los atacantes no proporcionaron la clave de descifrado.* *El operador tuvo que limpiar todos los sistemas de Tecnologías de Información (TI) con la ayuda de especialistas externos. Durante el tiempo de recuperación de seis semanas, sólo los túneles más importantes fueron operados localmente con mayores requisitos de seguridad vial, tales como disminución de los límites de velocidad y un número limitado de vehículos que podían pasar por ellos al mismo tiempo.*
El progreso del ataque	*El ataque se llevó a cabo utilizando un troyano, que se disfrazó como documentos adjuntos a una solicitud para una vacante vigente de trabajo. Se engañó al usuario para que abriera el archivo adjunto del correo electrónico y el "ransomware" viajó automáticamente desde las Tecnologías de Información (TI) de la oficina a las TI del control de túneles, ya que ambos sistemas no estaban físicamente separados entre sí.*
Consecuencias inmediatas en la infraestructura	*Después de su propagación en el sistema de control de túneles, el "ransomware" comenzó a manipular los PLC para provocar falsas alarmas, también bloqueó todos los sistemas operativos. Debido a la pérdida de operaciones y control, cuarenta y cuatro túneles tuvieron que cerrarse localmente a través del control manual.*
Número de víctimas	*El "ransomware" logró apagar la iluminación en todos los túneles, lo que provocó accidentes vehiculares. Las fuerzas de rescate tuvieron problemas para rescatar a todas las personas involucradas.*
Eventos secundarios	*Debido a la eficacia del ataque, no se inició ningún ataque secundario. En las rutas alternas congestionadas se produjeron más accidentes que de costumbre, por lo que las fuerzas de rescate estuvieron trabajando constantemente.*
Respuesta de los servicios de emergencia	*Después de que el malware se infiltró en el sistema de control de túneles, apareció un mensaje en las pantallas de la computadora, que informaba al usuario de que los datos se habían encriptado y que serían descifrados tras el pago de 1 Bitcoin (aproximadamente 7,000.00 €).* *La policía y los equipos de rescate fueron informados inmediatamente. Debido al caos en las carreteras, su llegada a los túneles afectados se retrasó. También se informó al Grupo para la Gestión de Crisis del Ministerio de Transporte, a la*

	Oficina Federal de Seguridad de la Información y al Buró Federal de Investigaciones, quiénes comenzaron a trabajar inmediatamente.
Reportes de los medios de comunicación	*El ataque ocurrió durante la hora pico. En el lapso de una hora, todos los medios de comunicación cubrieron el ataque. La comunicación con dichos medios fue coordinada por el Grupo para la Gestión de Crisis del Ministerio de Transporte. El ataque llamó la atención de medios de comunicación internacionales.*
El papel de la AC en el proceso de respuesta	*Una vez realizado el ataque, la AC informó a la policía y a las fuerzas de rescate a fin de evitar daños a la infraestructura y víctimas. Se informó a especialistas del Ministerio Federal de Transporte, de la Oficina Federal de Seguridad de la Información y del Buró Federal de Investigaciones para que apoyaran la gestión de la crisis.*

La resiliencia carretera ante los ataques ciber-físicos a los centros de control

Las medidas de resiliencia cibernética se dividen en tres categorías:

1. Medidas físicas y técnicas.

2. Medidas del personal.

3. Medidas organizativas.

RESILIENCIA	**Medidas**		
Fases	Físicas y técnicas	Del personal	Organizativas
Preparar	Analizar y entender su red de TI. Identificar los sistemas críticos para el negocio. Identificar y remediar las vulnerabilidades.	Aumentar en el personal la conciencia de la seguridad cibernética, mediante ejercicios regulares de educación y seguridad.	Definir e implementar una política/cultura de resiliencia. Nombrar a un oficial de resiliencia. Crear conciencia sobre el panorama de amenazas externas e INTERNAS y aprender sobre las interdependencias con otras infraestructuras, incluida la cadena de suministro.
Prevenir	Proteger los sistemas críticos para el negocio frente a las amenazas cibernéticas, la pérdida de datos y el acceso ilegal.	La habilidad de los empleados para acceder a información corporativa sensible va en aumento, por lo que se debe capacitar al personal y mantenerlos informados sobre las amenazas e incidentes actuales.	Monitorear y hacer cumplir la política de resiliencia cibernética.
Proteger/ Detectar	Ejemplos de medidas de protección: • Controlar el acceso físico. • Controlar el acceso a los sistemas de TI a través de una combinación segura de contraseña de usuario	La mayoría de las vulneraciones de los datos son causadas por factores humanos como empleados o contratistas negligentes.	Crear un departamento de TI proactivo y mantenerse actualizado sobre las posibles amenazas.

RESILIENCIA	**Medidas**		
Fases	Físicas y técnicas	Del personal	Organizativas
	• Usar programas de protección antivirus constantemente actualizados. • Proteger el acceso remoto a través de un *firewall* externo • Proteger los puntos finales y los puertos de enlace. • Realizar actualizaciones de seguridad periódicas para los sistemas operativos. • Implementación regular de copias de seguridad del sistema. • Crear dispositivos de arranque de emergencia para todos los sistemas informáticos • Desactivar las interfaces de oficina de las TI	• Capacitar regularmente al personal en aspectos de seguridad de las TI. • Capacitar regularmente al personal sobre la Ingeniería Social. • Capacitar para la concientización de los empleados • Capacitar a un administrador de sistemas y a un suplente. • Capacitar a los empleados para el manejo seguro de dispositivos y soportes de datos móviles (p. ej. tabletas, teléfonos inteligentes, etc.).	
Responder	Crear un plan que priorice la respuesta técnica a los diferentes tipos de ataque.	Que el personal practique; enséñele cómo responder de acuerdo con el plan de respuesta.	Crear un plan de respuesta que indique claramente a las personas qué hacer cuando ocurre un incidente. Especifique los roles y las responsabilidades. Gestionar los informes a los medios de comunicación sobre los ataques.
Recuperar	Para recuperarse lo más rápido posible, piense en la redundancia de las copias de seguridad de datos y software, de los componentes técnicos como los discos duros, los teléfonos móviles y las computadoras portátiles.	Organizar un informe sistemático de eventos pasados. Definir las consecuencias en los procedimientos y la capacitación del personal.	Desarrolle un plan de recuperación para restaurar los datos y los servicios lo más rápido posible, a fin de volver a las operaciones normales. También asegúrese de que los sistemas críticos estén disponibles durante un incidente. Comprender qué datos son realmente importantes para las operaciones. Aprender de los incidentes pasados.

APÉNDICE 1.3 : VEHÍCULO UTILIZADO COMO ARMA.

Descripción

VEHÍCULO UTILIZADO COMO ARMA	
Parámetro	**Descripción de eventos**
Naturaleza del ataque	*Las amenazas con el uso de vehículos van desde el vandalismo hasta ataques sofisticados o agresivos por parte de determinados delincuentes o terroristas.*
Tipo de ataque	*Un vehículo puede usarse como un arma para embestir y dañar la infraestructura o para herir y matar a personas.*
Hora del ataque	*El uso de un vehículo como arma para herir y matar a personas es más probable que ocurra cuando el actor de la amenaza sabe que en un área habrá muchas personas.*
Objetivo (blanco)	*Es probable que los objetivos o blancos sean áreas públicas en las que se puede predecir que la densidad de público será muy alta. También podrán utilizarse los accesos a las zonas en las que sea posible que un vehículo conduzca a gran velocidad.*
Número de atacantes	*Hasta la fecha, los ataques han involucrado en gran medida a un sólo vehículo, a menudo con un único ocupante.*
Severidad del ataque	*Es probable que la severidad de las consecuencias del ataque dependa de: el tipo de vehículo utilizado y la velocidad del impacto; el tamaño, la densidad y la dispersión de la multitud; la capacidad de las personas para reconocer que se está produciendo un ataque y para alejarse de él inmediatamente; la presencia y efectividad de las medidas de protección; y la respuesta de los servicios de emergencia.*
El progreso del ataque	*Es común que estos tipos de ataques comiencen en el dominio público y duren poco tiempo. El conductor puede continuar con el ataque hasta el momento en que el vehículo haya sido incapacitado o dominado. Durante el ataque, es muy poco probable que el conductor obedezca las reglas normales de la carretera y acelere, conduzca por el lado equivocado de la carretera, ignore los semáforos, cruce las medianas (camellones) y se suba a las aceras.*
Consecuencias inmediatas en la infraestructura	*Puede haber algún daño en el equipamiento de la calle y en los edificios, pero el objetivo principal de este tipo de ataque es causar lesiones y matar a miembros del público o grupos específicos de personas.*
Número de víctimas	*El número de víctimas dependerá del tipo de vehículo utilizado y de la velocidad del impacto; el tamaño, la densidad y la dispersión de la multitud; de la capacidad de las personas para reconocer que se está produciendo un ataque y para apartarse inmediatamente de él; de la presencia y efectividad de las medidas de protección; la naturaleza de cualquier ataque secundario; y de la respuesta de los servicios de emergencia.*
Eventos secundarios	*El uso de un vehículo como arma suele ir acompañado de otra forma de ataque subsecuente, en donde el conductor del vehículo y cualquier otro atacante intentan causar más lesiones en las personas que se encuentren en las proximidades del lugar donde se ha conducido el vehículo o donde éste se ha detenido.*
Respuesta de los servicios de emergencia	*Debido a la duración relativamente corta de un ataque de esta naturaleza, la rapidez de la respuesta de la policía y luego de los servicios médicos, así como las acciones de los miembros del público, serán más significativas para reducir el número de víctimas cuando el vehículo como arma es el antecesor de un ataque secundario.*

Reportes de los medios de comunicación	*Los ataques con vehículos como armas han atraído la atención de los medios de comunicación tanto en el país donde ocurrieron como a nivel internacional.*
El papel de la AC en el proceso de respuesta	*Un ataque de esta naturaleza a menudo lleva a las autoridades viales competentes, y a otros, a revisar las disposiciones que tienen en vigor para reducir la probabilidad y la gravedad del resultado de un ataque de esta naturaleza, que se produce en lugares similares. Las medidas de mitigación adoptadas incluyen la instalación de medidas físicas (incluyendo la integración de elementos en el entorno o en el paisaje urbano) que pueden ser pasivas (estáticas) o activas (con controles de seguridad pública). Las medidas para controlar el tráfico y el trazado de las carreteras pueden utilizarse para reducir la velocidad de los vehículos, mientras que otras características como los bolardos, las puertas, las jardineras y el mobiliario urbano reforzado pueden utilizarse para evitar que un vehículo se desplace más allá de un punto determinado.*

APÉNDICE 1.4 : VANDALISMO Y ACTOS MALICIOSOS EN LA OPERACIÓN DE UNA CARRETERA.

Introducción

La parte de la red nacional de carreteras que presenta los mayores problemas de seguridad vial y seguridad pública se encuentra principalmente a las afueras de las pequeñas y grandes ciudades:

- los problemas de seguridad vial tienen lugar debido al alto nivel de mantenimiento, de los trabajos continuos y del gran nivel tanto de tráfico local como de tráfico de largo itinerario;
- los problemas de seguridad pública tienen lugar debido a la presencia de pandillas, de pequeños contratistas sin escrúpulos o población de inmigrantes ilegales no controlados, de conductores violentos, quiénes generan robos, vandalismo, actos maliciosos y depositan escombros.

El escenario está inspirado en hechos reales en un momento que pudieran haber evolucionado.

En particular, la inseguridad puede disminuir en intensidad en un sector geográfico debido a la transferencia de delincuentes a un área cercana, por las numerosas intervenciones de la fuerza policial o de los servicios aduaneros.

Por lo tanto, este escenario de operación carretera es un buen ejemplo para un estudio de caso de seguridad pública.

Descripción

VANDALISMO Y ACTOS MALICIOSOS EN LA OPERACIÓN DE UNA CARRETERA		
Parámetro	**Descripción de eventos**	
Naturaleza de los eventos	*Vandalismo, robo, conducta antisocial (incivilidad o gamberrismo), degradación intencional por dejar materiales de desecho (escombros).*	
Tipo de eventos	***Daños a la propiedad de los operadores de carreteras:*** *robo de equipos y cables, vertederos en su mayor parte de materiales de construcción, grafiti o etiquetas en estructuras y señales viales.* ***Daños a la propiedad inmaterial de los operadores de carreteras:*** *imagen de un servicio público dañado o incompetente.* ***Daños al personal operativo de las carreteras:*** *agresiones verbales (insultos y amenazas) por parte de los conductores.*	
Lugar de los eventos	*Suburbio de una gran ciudad, con un importante tráfico vehicular por carretera.*	*Fenómenos regulares, cíclicos.*

Hora de los eventos	***Robos – vandalismo – degradación por el vertido de material de desecho**: durante la noche cuando hay poco tráfico vehicular.* ***Conducta antisocial:** cuando hay luz de día, en la zona de obras o accidentes, cuando las restricciones de tráfico causan atascos.*
Objetivo (blanco)	*Cualquier carretera equipada con paneles de mensaje variable, estaciones de conteo o meteorológicas, depósitos de materiales para el mantenimiento, instalaciones técnicas aisladas, en suburbios sensibles o cerca de campamentos ilegales.*
Número de atacantes o perpetradores	***Robos – vandalismo:** grupo organizado de varias decenas de personas.* ***Vertederos ilegales:** equipos de pequeños contratistas que trabajan ilegalmente.* ***Conducta antisocial:** muchos conductores delincuentes.*
Severidad de los daños	***El robo de cables** provocó, en general, la desconexión con el centro de gestión de información y tráfico, así como el apagón de los paneles de mensaje variable.* ***El vandalismo** encuentra expresión en el grafiti o las etiquetas (pegatinas) en las instalaciones, estructuras o equipos de la carretera, incluyendo señales de tránsito o de policía.* ***Los vertederos muy frecuentes de materiales de construcción o de desecho** le dificultan al personal operativo realizar las actividades de mantenimiento (por ejemplo, el corte de hierba o pasto) y pueden ser peligrosos para los conductores (por ejemplo, si hay material de desecho en el acotamiento o arcén).* ***Los actos regulares de conducta antisocial** desaniman al personal que hace todo lo posible para reducir las molestias relacionadas con los accidentes o cuando se trata de trabajos con restricciones de tráfico. Muchos empleados se quejan ante sus jefes que esperan un buen flujo vial durante una gestión local complicada.*
El progreso de los eventos	*El centro de gestión de tráfico (que funciona 24/7) detecta una anomalía en los enlaces de la carretera nacional número X.* *Originalmente, una banda (delincuentes, matones, migrantes ilegales, ladrones, contrabandistas) de un campamento ilegal o de un suburbio con alta delincuencia robó material de las obras públicas en un sitio de construcción, rompieron los ductos eléctricos y registros para robar cable de cobre, fibra óptima, tarjetas de programación, cualquier material de valor e incluso las tapas de los registros durante la noche.* *El personal de patrullaje que está de guardia busca el origen del problema, pero no puede encontrar nada durante la noche.* *Es la hora de la salida al trabajo de muchos conductores y los paneles de mensaje variable no funcionan, por lo que se deja de regular el tráfico y la congestión vehicular es inevitable.* *Los conductores "madrugadores" no son un problema, pero los atascos de tráfico se hacen más grandes. La irritación y el nerviosismo de los conductores crece, el personal en el lugar es insultado y nombrado incompetente. La información fluye en las redes sociales (Facebook, Twitter), a veces con fotografías.* *El equipo de operaciones diurnas realiza un seguimiento continuo y descubre las etiquetas (pegatinas) en las señales y en las barreras antiruido cerca de un área de desaceleración; un poco más lejos, los vertederos de desechos se encuentran en el arcén. Algunas piezas de yeso para paredes y electrodomésticos están en el carril lento. Por lo que es necesario quitarlos rápidamente.* *Las furgonetas que vinieron a tirar sus desechos durante la noche en la rampa de salida y el área de descanso lo hicieron por segunda vez durante la semana.* *El personal operativo está enojado y desanimado.*
Consecuencias inmediatas en la infraestructura	*Perturbación del tráfico vehicular (como resultado de la destrucción del equipamiento).*

	Deterioro del activo vial: estructuras, señales, espacios verdes (como consecuencia del vandalismo y del vertido de desechos) *Falta de equipamiento o materiales para la construcción, el mantenimiento o la operación de la carretera (como consecuencia de los robos).* *Afecta a la seguridad vial en caso de accidente o incidente.*
Número de víctimas	*Por lo general, algunas víctimas: no son accidentes importantes, sino incidentes debido a los atascos de tráfico.* *Es probable que haya víctimas por el ajuste de cuentas entre pandillas, pero no es fácil de vincular con la infraestructura.* *El personal operativo se ve afectado psicológicamente.*
Eventos secundarios	*Consecuencias económicas importantes en términos de reparaciones urgentes de las carreteras.* *Una cuasirenuncia a la eliminación del grafiti o a la remoción de etiquetas (pegatinas) en algunas zonas, debido a que el fenómeno es generalizado.*
Respuesta de los servicios de emergencia	*Frente a estos eventos, las fuerzas del orden organizan operaciones regulares que, por lo general, reducen temporalmente las acciones maliciosas ya que se transfieren a zonas vecinas, pero no cesan.* *Otros servicios operan en relación a la seguridad pública de la misma manera que en los accidentes (seguridad vial).*
Reportes de los medios de comunicación	*Los medios de comunicación no informan específicamente sobre estos actos maliciosos, pero plantean regularmente los problemas de las pandillas, los campamentos ilegales y los diversos tráficos en los suburbios desfavorecidos.* *Sin embargo, los bloqueos del tráfico vehicular se transmiten en tiempo real.*
El papel de la AC en el proceso de respuesta ante acciones maliciosas	*La Administración de Carreteras (AC) está consciente de estas dificultades, pero tiene que tomar decisiones sobre el mantenimiento de la red nacional. Deja que los prestadores de servicios regionales encuentren las soluciones prácticas y los apoya financieramente.* *Así que se instalaron los equipos y los cables en una ubicación menos accesible que el acotamiento o arcén, por ejemplo, en la mediana (camellón). También se aseguraron los registros.* *Para asegurar que los ductos de cableado permanecieran sobre el acotamiento o arcén, se vertió arena o se colocaron bloques de hormigón sobre los registros para bloquear cualquier acceso (pero algunos grupos ya han podido removerlos con equipo).* *En cuanto a los conductores descontentos o violentos, por lo general, se les pide a los trabajadores operativos que den un informe de los hechos por la noche al cerrar o por la mañana al reabrir la infraestructura. Se trata claramente de un fenómeno social sobre el que la Administración de Carreteras no tiene ningún control.* *Sin embargo, hay poca coordinación con las fuerzas policiales, los servicios encargados del control de las mercancías (aduanas) y las comunidades involucradas.* *Las quejas presentadas ante las fuerzas de seguridad pública no son sistemáticas porque los autores de los actos son difíciles de identificar.* *En cuanto a los desechos, proceden en su mayoría de pequeños contratistas del ámbito de la construcción, o incluso de personas (ilegales o sin trabajo), que no pagan en algún vertedero oficial y dejan sus desechos (escombros, grandes electrodomésticos, etc.) a un lado de las carreteras. Hay otros vertederos en campamentos ilegales, cuyos residentes lucran con el manejo de desechos (almacenan los residuos de los contratistas del ámbito de la construcción dentro de los campamentos por una tarifa baja).* *La tarifa del relleno sanitario oficial es de 100€-150€/tonelada, además se le debe añadir el costo de la mano de obra de los empleados de la carretera, más*

	el costo de la recogida y transporte de residuos, por lo que el impacto económico para la AC es elevado. *Es un problema importante de seguridad pública el hecho de que los vehículos comerciales ligeros (menos de 3.5 toneladas) se utilicen ampliamente, sean rápidos y poco controlados (poca regulación en comparación con los camiones pesados en Europa y Francia).*

Resiliencia carretera ante vandalismo-robos-conducta antisocial

Las medidas de protección se dividen en tres categorías:

1. Las medidas de protección física y técnica.
2. Las medidas de protección de las personas.
3. Las medidas de protección organizacional.

Resiliencia – medidas -> elementos del ciclo de resiliencia	Protección física y técnica	Protección de las personas	Protección organizacional
Preparar	-Definir una política de seguridad pública para las instalaciones y equipamiento de la carretera.	-Sensibilizar al personal operativo sobre la seguridad pública y la seguridad vial en las carreteras.	-Diseñar el puesto de oficial o responsable de la seguridad pública. -Preparar ejercicios regulares de seguridad pública.
Prevenir	- Reforzar la videovigilancia en los tramos de la red de carreteras susceptibles de sufrir ataques, robos y vertidos ilegales. -Realizar un mapa (esquema) de los tramos susceptibles.	- Capacitar al personal para hacer frente a la conducta antisocial. -Disponer de mecanismos de apoyo psicológico en caso de agresión verbal. - Capacitar al personal para comunicarse con los usuarios "enojados" de la carretera.	-Proporcionar procedimientos de seguridad pública. -Coordinarse mejor con la policía, las aduanas, las comunidades encargadas del saneamiento y el medio ambiente. -Reforzar la comunicación con el público y los usuarios de la carretera.
Proteger	-Mover cables sensibles o susceptibles a las medianas (camellones). -Cubrir los registros que están en el acotamiento o arcén (con arena o bloques de concreto) para que requieran equipo para moverlos. -Reforzar las cerraduras de las instalaciones. - Configurar más videovigilancia	-No intervenir sólo con un trabajador operativo.	-Facilitar el control de los vehículos comerciales ligeros mediante el reporte en tiempo real de cualquier comportamiento anormal.
Responder	-Respetar los tiempos de intervención de los equipos	-No intervenir sin previo aviso (equipo, recursos,	-Optimizar las patrullas de vigilancia de la red carretera

	operativos -Presentar sistemáticamente denuncias contra los delincuentes o infractores.	ubicación, etc.) y rastrear las intervenciones nocturnas. .	en combinación con las de la policía y aduanas, así como las de inspección laboral (lucha contra el trabajo ilegal).
Recuperar	-Restaurar lo más rápido posible (incluyendo la eliminación de pegatinas y del grafiti)	-Organizar un informe sistemático de los eventos pasados. -Definir las consecuencias en los procedimientos y la capacitación del personal.	-Gestionar la comunicación con los medios sobre los hechos maliciosos. -Informar a los usuarios de las carreteras sobre la rehabilitación de la infraestructura (agenda, costos, etc.)

APÉNDICE 1.5 - ROBO DE CARGA

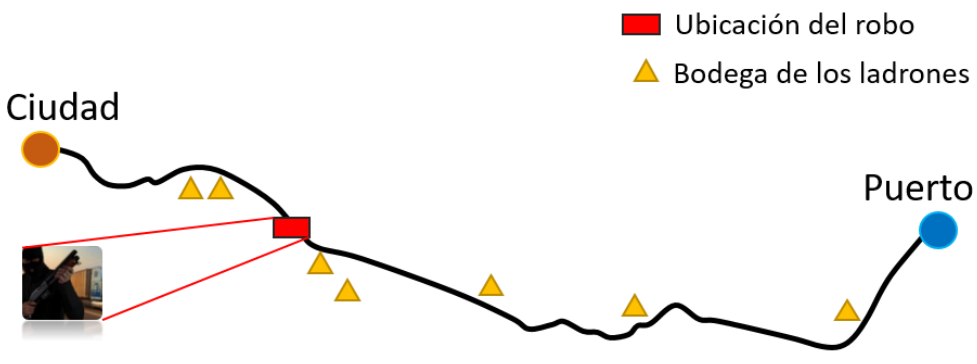
Introducción

En los últimos años, la seguridad del transporte se ha convertido en un gran desafío para el sector del transporte carretero, causando enormes pérdidas a los transportistas y a las empresas. Los productos de conveniencia y los alimentos son fáciles de distribuir en el mercado gris y pueden terminar en mercados callejeros, donde las ventas no están reguladas y representan una competencia desleal en la economía.

Estos grupos delictivos son autodidactas y mejoran constantemente su metodología, tecnología e infraestructura, lo que resulta en un enfoque operativo eficiente. Además, de alguna manera obtienen información precisa sobre los flujos de la carga y la hora exacta de los viajes.

El estudio de caso propuesto es un ejemplo de un *modus operandi* que consiste en: bloquear el paso de un camión de carga con dos camionetas, luego cinco personas armadas descienden y amenazan al conductor, quién es obligado a descender para ser golpeado y atado a un lado de la carretera. Después de eso, uno de los asaltantes toma el teléfono móvil y la cartera del conductor, y al mismo tiempo otro activa el dispositivo anti-rastreo "*Jammer*". Posteriormente, uno de los miembros del grupo conduce el camión robado a un almacén cercano acompañado por las dos camionetas, toman inmediatamente la mercancía y la colocan en unas furgonetas para poder transportarla fácilmente y venderla. Algunas horas más tarde, el camión robado con el contenedor vacío es abandonado a un lado de alguna carretera.

Descripción

ROBO DE CARGA EN EL TRANSPORTE CARRETERO	
Parámetro	**Descripción de los eventos**
Naturaleza del incidente	*Robo de carga*
Tipo de incidente	*Daño a la propiedad de los miembros de la cadena de suministros: robo de la carga de un tracto camión (que incluye el robo del tracto camión para obtener la carga y después abandonarlo).*
Lugar del incidente	 *Tramo carretero entre una ciudad y un puerto marítimo.*
Hora del incidente	*Podía ocurrir a cualquier hora, pero es más probable entre 2:00 a.m. y 3:00 a.m., entre 6:00 a.m. y 8 a.m. o entre 1:00 p.m. y 3:00 p.m. En este caso, el incidente ocurrió a las 6:30 a.m.*
Objetivo (blanco)	*Un tracto camión que transportaba un contenedor con carga, en la ruta entre una ciudad y un puerto marítimo.*

Número de atacantes o transgresores	*Ladrones: 5 personas en dos vehículos*
Severidad del incidente	• *El conductor del camión herido* • *Pérdida de la carga* • *Penalización económica por no entregar a tiempo la carga.*
El progreso del incidente	*El martes, a las 6:30 a.m. dos camionetas le cortan el paso a un tracto camión, después descienden cinco personas armadas (uno de ellos es el líder de la operación) y amenazan al chofer para obligarlo a descender del camión, finalmente lo golpean y lo dejan atado al lado de la carretera; ahí despojan al conductor de su cartera y celular, mientras que otro de los ladrones activa el dispositivo anti-rastreo "Jammer". Posteriormente, uno del grupo maneja el camión hasta una bodega cercana, seguido de las dos camionetas, en dicha bodega descargan el contenedor y colocan la mercancía en furgonetas, para transportarla fácilmente y venderla.* *A las 6:33 a.m., en la empresa transportista, un trabajador a cargo del rastreo de los camiones se da cuenta de que perdió la señal de uno de ellos, inmediatamente trata de contactar al conductor pero éste no responde, por lo que llamó a la policía federal para informar de un posible robo, dándoles la hora estimada y última ubicación, así como las características del tracto camión.* *A las 7:00 a.m., dos de las patrullas de policía más cercanas llegaron al lugar estimado e iniciaron la búsqueda del tracto camión.* *A las 7:20 a.m., una patrulla encontró al conductor al lado de la carretera, pero no encontraron el camión robado ni a los rateros.* *A las 9:30 a.m., el conductor hizo una declaración en la estación de la policía estatal más cercana.* *A las 4:55 p.m., el camión robado con el contenedor vacío fue dejado al lado de alguna carretera.* *A las 5:00 p.m., en la empresa transportista, el empleado detectó la señal del tracto camión e informó nuevamente a la policía.* *A las 6:30 p.m., las autoridades recuperaron el tracto camión robado, pero lo mantuvieron bajo su resguardo.* *El miércoles a las 9:00 a.m., un empleado de la empresa transportista fue a recuperar el tracto camión, para ello presentó los papeles que acreditan la propiedad del camión a las autoridades y realizó un pago por el tiempo que permaneció el vehículo bajo resguardo de las autoridades.*
Consecuencias inmediatas en la infraestructura	*Las consecuencias no fueron en la infraestructura, pero sí en la interrupción de la cadena de suministros.*
Número de víctimas	*Un conductor de camión herido.*
Eventos secundarios	*En el mediano plazo: pérdida de posibles inversores en el país debido a la percepción de alto riesgo.*
Respuesta de los servicios de emergencia	*Ninguna*
Reportes de los medios de comunicación	*El periódico escribió la noticia sin muchos detalles.*
El papel de la AC en el proceso de respuesta	*Ninguno*

Recomendaciones para el ciclo de resiliencia

Preparación:

- Tener todos los papeles del camión listos para presentarlos a la autoridad y a las compañías de seguros si es necesario.
- Dar mantenimiento preventivo a los camiones, para evitar paradas por averías.
- Investigar los antecedentes personales antes de contratar a los conductores de los camiones de carga.
- Identificar los puntos críticos de las rutas, con la mayor probabilidad de robo por tipo de carga.

Prevención:

- Tener control del acceso a los horarios programados de los camiones de carga.
- Rotar a los conductores en diferentes rutas
- Mantener un registro de los conductores que ya fueron asaltados.
- Colocar dos dispositivos de rastreo (GPS), uno en el camión y otro en la carga (lejos de la cabina del camión).
- Programar geo-cercas para alertar en caso de desvíos.
- Desactivar la toma del encendedor de la cabina del camión para evitar que se utilice para conectar dispositivos de bloqueo "Jammer".
- Cargar combustible antes de recoger la carga y sólo en las estaciones de combustible designadas en la ruta.
- Los conductores de los camiones deben notificar antes de hacer una parada no programada.

Protección:

- Viajar en grupos de camiones (caravanas).
- Escoltar al camión en algunos puntos críticos de la ruta (con la mayor probabilidad de robo según el tipo de carga).

Respuesta:

- Tener un botón de alarma instalado en el camión.
- Continuar con el intento de rastrear el camión.

Recuperación:

- Desactivar el motor del camión de forma remota.
- Notificar sobre el robo a las autoridades y a los clientes del servicio de transporte.

APÉNDICE 1.6 - TRANSPORTE DE MATERIALES PELIGROSOS

Introducción

La seguridad de la infraestructura carretera es un tema delicado en todo el mundo debido a los eventos globales que han tenido lugar en la última década, en términos de ataques terroristas.

La pregunta principal que cualquier agencia o administración de carreteras debe considerar es: *"Si ocurre tal escenario (ataque, incidente, terrorismo, etc.), ¿qué debemos hacer como agencia o administración de carreteras para mitigar las consecuencias?"*

Hasta el momento, en Rumanía no se han producido trágicos acontecimientos de pérdidas humanas o económicas como consecuencia de atentados terroristas, debido a factores que han sido afortunados y que no pueden definirse con claridad, como por ejemplo: un país que no ha entrado en conflicto con organizaciones terroristas u otros Estados que apoyan a estas organizaciones, una actividad sostenida y fructífera de los servicios de inteligencia, etc.

Cabe señalar, sin embargo, que la falta de un ataque terrorista o evento similar hasta el momento no implica que no podría ocurrir en el futuro. Para mantener la funcionalidad de las redes de infraestructura carretera, sus administradores deben diferenciar entre la seguridad vial y seguridad pública e, implícitamente, implementar medidas adecuadas para cada una de esas categorías. Cuando hablamos de seguridad pública, hablamos de eventos intencionados que pueden influir en la integridad de la infraestructura carretera.

A continuación se presenta una simulación de las pérdidas estimadas en caso de que se repita un suceso trágico (intencional o no), similar a los dos casos de accidentes trágicos en la red nacional de carreteras de Rumanía, que provocan la pérdida de vidas humanas, pérdidas económicas y el cierre de esas secciones de las carreteras nacionales.

Descripción

TRANSPORTE DE MATERIALES PELIGROSOS	
Parámetro	**Descripción de los eventos**
Naturaleza de los eventos	*Mercancías peligrosas, terrorismo.*
Tipo de eventos	***Daños a la propiedad de los operadores de carreteras:*** *destrucción de parte de la infraestructura carretera como los carriles en uso, puentes y túneles, redes de telecomunicaciones, sistemas informáticos integrados.* ***Daños a la propiedad inmaterial de los operadores de carreteras:*** *imagen de un servicio público dañado o incompetente, que infunde miedo en la población.* ***Daños al personal operativo de las carreteras:*** *muerte o lesiones a los empleados, disminución de la moral.*
Lugar de los eventos	*Rumanía - Sur - Este*
Hora de los eventos	***Momento de producción:*** *posibilidad de producción en cualquier momento.* ***Conducta antisocial:*** *cualquier momento del día, mayor probabilidad con luz del día.*

Objetivo (blanco)	*Infraestructura carretera, personas: conductores y personal operativo.*
Número de atacantes o transgresores	***Terroristas:*** *un terrorista o un grupo organizado de varias docenas de personas.* ***Mercancías peligrosas:*** *al menos un camión con mercancías peligrosas.*
Severidad de los daños	***Destrucción de la infraestructura carretera:*** *cráter en la infraestructura carretera (en los carriles en uso) y destrucción completa de puentes o pasos a desnivel de la infraestructura carretera.* ***Destrucción de equipamiento vial:*** *destrucción de los sistemas de peaje y de las cámaras de tráfico.*
El progreso de los eventos (punto de inicio – experiencia/eventos similares)	*El 24 de mayo de 2004, a las 5:50 horas en Mihăileşti, condado de Buzău, en la DN2 (sección de la carretera europea E85), a 32 kilómetros al sur de Buzău, hubo una explosión ocasionada por el accidente de un camión que transportaba 20 toneladas de nitrato de amonio.* *El informe de las víctimas muestra que hubo 18 muertos (incluyendo siete bomberos, tres personas de la localidad y dos periodistas de un canal de televisión) y 13 heridos graves.* *Se formó un cráter con una profundidad de 6.5 metros y un diámetro de 21 metros alrededor del lugar de la explosión, y trozos de metal salieron lanzados en un radio de 200 metros, mismos que afectaron los techos de varias casas en el área.*  *Figura No. 1 - El lugar donde ocurrió el accidente (localidad de Mihăileşti)*  *Figura No. 2 - Fotos del lugar donde ocurrió el evento en 2004 (Mihăileşti)* ***1.1. El relato del evento en el año 2004.*** *El 24/05/2004, a las 04:56 horas, una persona no identificada, en tránsito en la DN Urziceni-Buzau, telefoneó a la Inspección de Policía del Condado de Buzau a través del teléfono central 955, cerca de Mihăileşti, para informar que en la dirección hacia Buzau, un camión de carga se volcó y salía humo de la cabina del vehículo. Inmediatamente después de tomar este mensaje, el oficial de la estación de policía del condado les notificó a los bomberos militares sobre el evento.*

Simultáneamente al aviso a los bomberos, la Inspección de Policía del Condado de Buzau fue informada de que había llamas en la cabina del camión, que no había víctimas humanas y que la carga consistía en bolsas de nitrato de amonio, por lo que era necesario combatir el incendio. La policía tomó medidas para quitar a los curiosos y dirigió el movimiento, llamando la atención de todos los presentes para que se alejaran, especificando que había peligro de que ocurriera un accidente grave.

Desde el momento del aviso, 24/05/2004, 04:56-04:57 horas, la subestación de intervención estaba alerta y se estableció la participación de dos automóviles para la misión. La salida de los automóviles se registró a las 5:00 horas y tuvieron que recorrer bajo la lluvia 36 km hasta el lugar donde ocurrió el evento. En el lugar del suceso, se iniciaron los procedimientos para extinguir el fuego, junto con la evaluación de la situación por parte del comandante de la guardia de intervención y la transmisión de los datos al despachador de la estación de bomberos.

Durante la preparación para la intervención, entre 60 y 90 segundos después de la llegada de los bomberos, ocurrieron las dos explosiones (la primera a las 05:47:42, la segunda 1 minuto y 2 segundos después), registrándose ambas explosiones en la estación sísmica de Istria; los componentes del remolque se extendieron en un radio de unos 400 metros desde el lugar de la deflagración, identificado por el cráter producido. Inmediatamente después del evento, se tomaron medidas para desviar el tráfico y preservar el lugar del accidente, con el fin de identificar las pruebas necesarias para llevar a cabo la investigación. Al mismo tiempo, se identificó el daño material producido en la localidad de Mihăileşti.

En el momento de la explosión, los bomberos militares estaban llevando a cabo los procedimientos de evaluación y de preparación para la extinción del incendio. Las condiciones existentes de los eventos y el poco tiempo disponible no les permitieron a los bomberos anticipar si la carga explotaría ni el momento de la deflagración.

1.2. Las cifras del evento de 2004.

Las cifras del evento de 2004, en resumen:

- *18 muertos y 13 heridos;*
- *Un cráter con una profundidad de 6.5 metros y un diámetro de 21 metros;*
- *500 metros del tramo carretero afectado;*
- *5 horas después de la tragedia, la excavadora empieza a trabajar;*
- *Después de 2 días, el camino fue asfaltado y la circulación regresó a la normalidad.*

1.3. El relato del evento en el año 2016.

El 10 de junio de 2016, en Mihăileşti, el lugar de la terrible tragedia del 2004, cuando murieron 18 personas, tuvo lugar un evento similar. Esta vez, un camión que transportaba 800 tanques de gas metano se incendió y decenas de los tanques explotaron.

Las autoridades aplicaron el código rojo de incitación y evacuaron toda el área en un radio de 700 metros. Afortunadamente, nadie resultó herido y los bomberos apagaron el fuego de manera segura. En la carretera, además del camión hecho cenizas, había cientos de tanques muy cerca de las casas de la gente, porque fueron lanzados durante la explosión.

El camión tuvo el accidente después de que se le pinchara una llanta. Dicho accidente ocurrió en la localidad de Mihăileşti, en el condado de Buzău, cuyo nombre está vinculado a la horrible tragedia de 2004. Por temor a que se repitiera el escenario, las autoridades evacuaron muchas casas.

Ni los bomberos pudieron acercarse. Utilizaron de forma remota las latas de espuma. Ocho especialistas llegaron al lugar. Las fuerzas de intervención se acercaron hasta que el incendio se extinguió.

El tráfico por carretera en la DN2 en Mihăileşti se reanudó en condiciones normales el viernes a las 17:45, casi 8 horas después del accidente, después de que el área fuera verificada por el equipo detector de gases y de incendios de Buzău.

<table>
<tr><td></td><td>

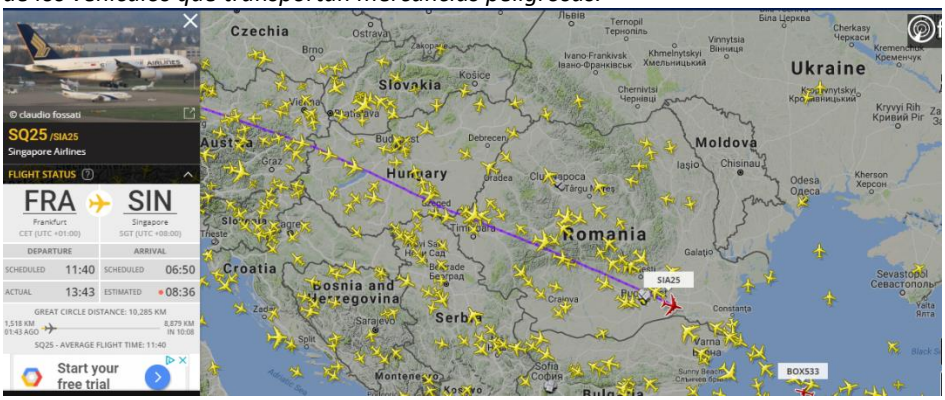

Figura No. 3 - Fotos del evento del 2016 (Mihăileşti)
1.4. Cifras del evento del 2016
Las cifras del evento del año 2016, en resumen:

Un herido;
500 m del tramo carretero afectado;
8 horas después de la tragedia, la circulación vehicular fue reabierta.

</td></tr>
<tr><td>El progreso de los eventos (Escenario)</td><td>
Los eventos del 2004 y 2016 se produjeron accidentalmente, pero si a una célula terrorista quisiera realizar ataques con mercancías peligrosas, los resultados serían mucho más graves que esos accidentes porque habrían elegido los puntos importantes o vitales de la infraestructura carretera.
Al hablar de las redes de infraestructura carretera, sus puntos vitales deben protegerse adecuadamente, ya que las inmensas pérdidas económicas pueden resultar de la interrupción en estos puntos, los primeros sectores de interés son las infraestructuras para conectar (puentes, túneles, pasos a desnivel, etc.).
Los puentes o pasos a desnivel son importantes o vitales para cualquier infraestructura carretera, ya que generalmente es la única ruta de acceso entre dos áreas por ser puntos de la infraestructura que salva obstáculos como agua, asentamientos u otros objetivos.
Otro aspecto importante es que se ha realizado un esfuerzo financiero considerable para construirlos y su cierre o bloqueo generaría unos costos colosales para la economía en general y, especialmente, para el área en la que se ubica dicha infraestructura.
Un punto vital de la red puede ser un "puente X" que consiste en un puente y una caseta de peaje cerca del puente.
Los terroristas podrían conseguir un transporte de mercancías peligrosas y hacerlo explotar cerca de la caseta de peaje.
</td></tr>
<tr><td>Consecuencias inmediatas en la infraestructura</td><td>
Considerando que esta simulación tiene en cuenta la superposición de un evento producido previamente en otra carretera, sin alterar las cifras en la realidad, las pérdidas económicas resultantes, según las cifras del evento de 2004, se verían de esta manera:
<table>
<tr><th rowspan="2">Evento</th><th colspan="3">Costos de acuerdo a la Estrategia para la Seguridad de las Carreteras Nacionales</th></tr>
<tr><th>No.</th><th>Valor (Euros)</th><th>Valor total (Euros)</th></tr>
<tr><td>Número de muertos</td><td>18</td><td>1,048,000</td><td>18, 864,000</td></tr>
<tr><td>Número de heridos</td><td>13</td><td>136,200</td><td>1,770,600</td></tr>
<tr><td>Días que duró dañada la carretera (hasta que regresó a sus condiciones óptimas)</td><td>2</td><td>279,727</td><td>559,454</td></tr>
<tr><td></td><td></td><td>TOTAL</td><td>21,194,054</td></tr>
</table>
</td></tr>
<tr><td>Número de víctimas</td><td>
Teniendo en cuenta el caso real de 2004, el número sería de:

18 fallecidos
13 heridos.

</td></tr>
</table>

Eventos secundarios	*Consecuencias financieras importantes en términos de reparaciones urgentes de la carretera. Dos días de cierre de la carretera y si la mercancía peligrosa explota en el puente (cerca de la caseta de peaje) se tendría cerrada la carretera por semanas/meses.*
Respuesta de los servicios de emergencia	*Los servicios operan en la seguridad pública de la misma manera que en los accidentes (seguridad vial).*
Reportes de los medios de comunicación	*Los medios de comunicación transmitirán el caso en tiempo real.*
El papel de la AC en el proceso de respuesta ante acciones maliciosas	*Lo que hay que tener en cuenta es el hecho de que la producción de un evento de este tipo, o una explosión como la del suceso propuesto en la simulación, podría destruir el puente, lo que provocaría algunas pérdidas impredecibles, teniendo en cuenta que dicho tramo carretero podría conectar lugares muy importantes.* *Las Administraciones de Carreteras deben considerar todas las "amenazas" que pueden influir en la integridad de las redes carreteras que tienen bajo su administración y, en este punto, de acuerdo al análisis de las tendencias globales, se puede concluir que es imperativo poner énfasis no sólo en la seguridad vial sino también en la protección de la infraestructura carretera, es decir, en la seguridad pública.* *Una solución óptima para prevenir, controlar y actuar rápidamente en caso de un atentado terrorista similar con mercancías peligrosas (o accidentes) sería crear un mapa en tiempo real sustentado en un SIG, en donde se puedan identificar todos los vehículos que transportan mercancías peligrosas.* *La existencia de un mapa de este tipo, similar al utilizado en el ámbito de la aviación, llevaría al control e identificación de posibles acciones delictivas mediante el monitoreo de los vehículos que transportan mercancías peligrosas.*  *Figura No. 4 - Mapa del ámbito de la aviación.* *Otra medida que las Administraciones de Carreteras pueden aplicar muy rápidamente es la implementación de sistemas de video para controlar el tráfico de mercancías peligrosas cerca de áreas sensibles (casetas de peaje, puentes, túneles).*

APÉNDICE 1.7- ACCIDENTE EN UNA AUTOPISTA

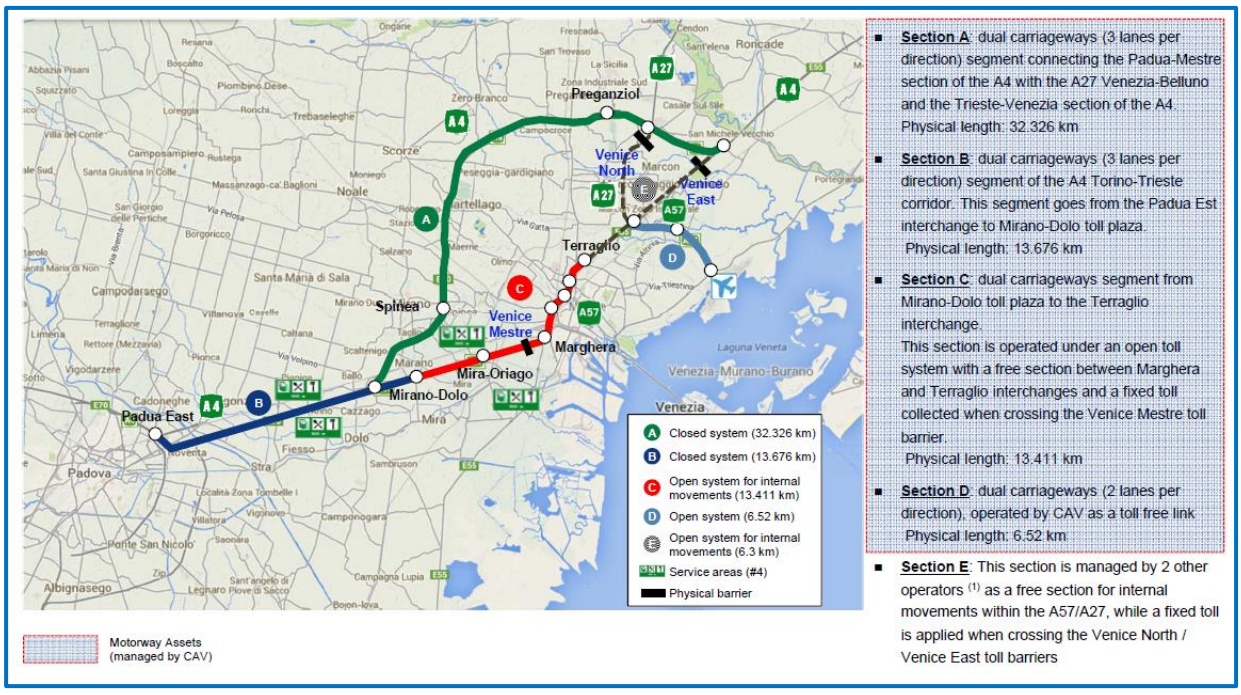
Resiliencia del sistema de infraestructura carretera

Introducción

Concessioni Autostrade Venete S.p.A. (CAV) es un operador de autopistas establecido en el año 2008, controlado conjuntamente por dos entidades públicas: ANAS S.p.A. (50%) y Regione Veneto (50%).

En el 2010, el Ministerio de Infraestructuras y Transportes (MIT) le otorgó una concesión a CAV hasta el 2032, que cubre una red de autopistas de 74 km ubicadas alrededor del área de Venecia, que se considera una de las secciones más estratégicas del sistema italiano de autopistas.
La red de carreteras a cargo de CAV está compuesta por 4 secciones:

- A4 Passante di Mestre
- Autopista A4 Padua-Venecia
- A57 Tangenziale di Mestre
- Autopista de enlace al aeropuerto Marco Polo de Venecia.



Las secciones A y B son sistemas de autopistas cerradas, mientras que las secciones C y D son sistemas de autopistas abiertas, lo que significa que también están abiertas al tráfico local libre de peaje.

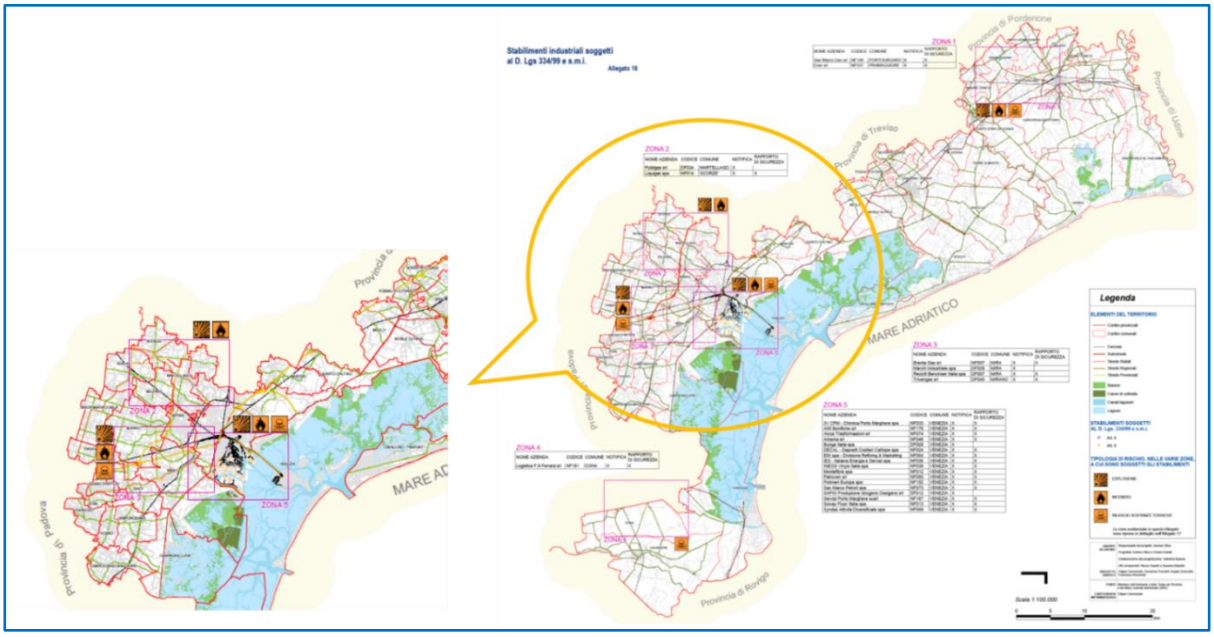
Passante es un nodo esencial para el noreste de Italia, ya que permite a los conductores eludir el área metropolitana de Venecia.
CAV opera en un área de servicio intenso:

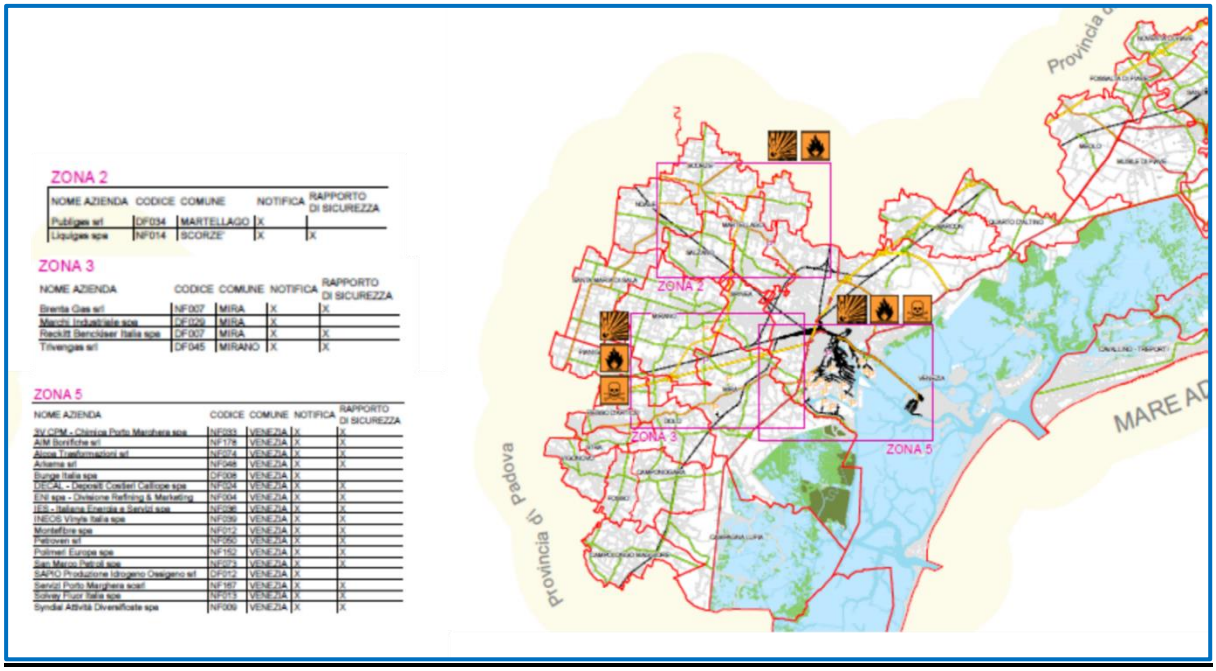
- CAV es un punto de intersección crucial de dos de las principales rutas europeas de clase A:

  - La E 70 que se extiende desde La Coruña hasta la ciudad georgiana de Pot.
  - La E 55 que conecta Helsingborg en Suecia con Kalamatà en Grecia.
- Además, CAV es un enlace esencial en el sistema de autopistas italianas, que es vital para la importación/exportación italiana hacia Europa Central y Oriental.
- Antes de la apertura de Passante di Mestre en 2009, Mestre era un cuello de botella en el corredor de la autopista de peaje A4, lo que repercutía negativamente en las zonas altamente desarrolladas.
- El área metropolitana de Venecia-Padua-Treviso es la cuarta más poblada de Italia después de Milán, Roma y Nápoles, con 2,7 millones de habitantes:
  - una de las zonas más ricas e industrializadas, no sólo de Italia sino también de Europa;
  - uno de los destinos turísticos más importantes de Italia, que tiene los aeropuertos italianos de origen y destino más importantes (Venecia Marco Polo, Treviso Canova)/estaciones de tren (Venecia Mestre)/ puertos (Venecia, Chioggia)/centros logísticos (Venecia, Padua).
- En caso de accidente, CAV toma el control, mediante protocolos de operación, de todas las alternativas en su red de autopistas.
- El volumen de tráfico de CAV siempre ha sido más resiliente que el promedio.
- La red de carreteras de CAV atraviesa la zona industrial química más importante de Italia.

Industria	Lugar	No. de plantas
Planta química o petroquímica	Mira	2
Producción y distribución de gases industriales y especializados	Venecia	1
Almacenamiento de gas licuado de petróleo	Borbiagio di Mira	1
Planta metalúrgica	Fusina	1
Estación de energía termoeléctrica	Porto Marghera	1
Almacenamiento de petróleo	Porto Marghera	4
Refinamiento de petróleo	Porto Marghera	1
Planta química o petroquímica	Porto Marghera	5

Características críticas de la zona industrial que atraviesa la red de CAV





ZONA 2

NOME AZIENDA	CODICE	COMUNE	NOTIFICA	RAPPORTO DI SICUREZZA
Publigas srl	DF034	MARTELLAGO	X	
Liquigas spa	NF014	SCORZE'	X	X

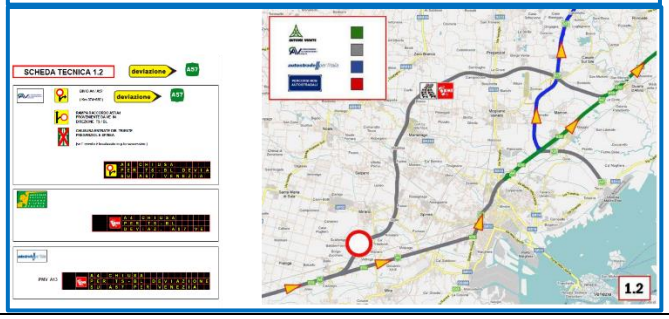
ZONA 3

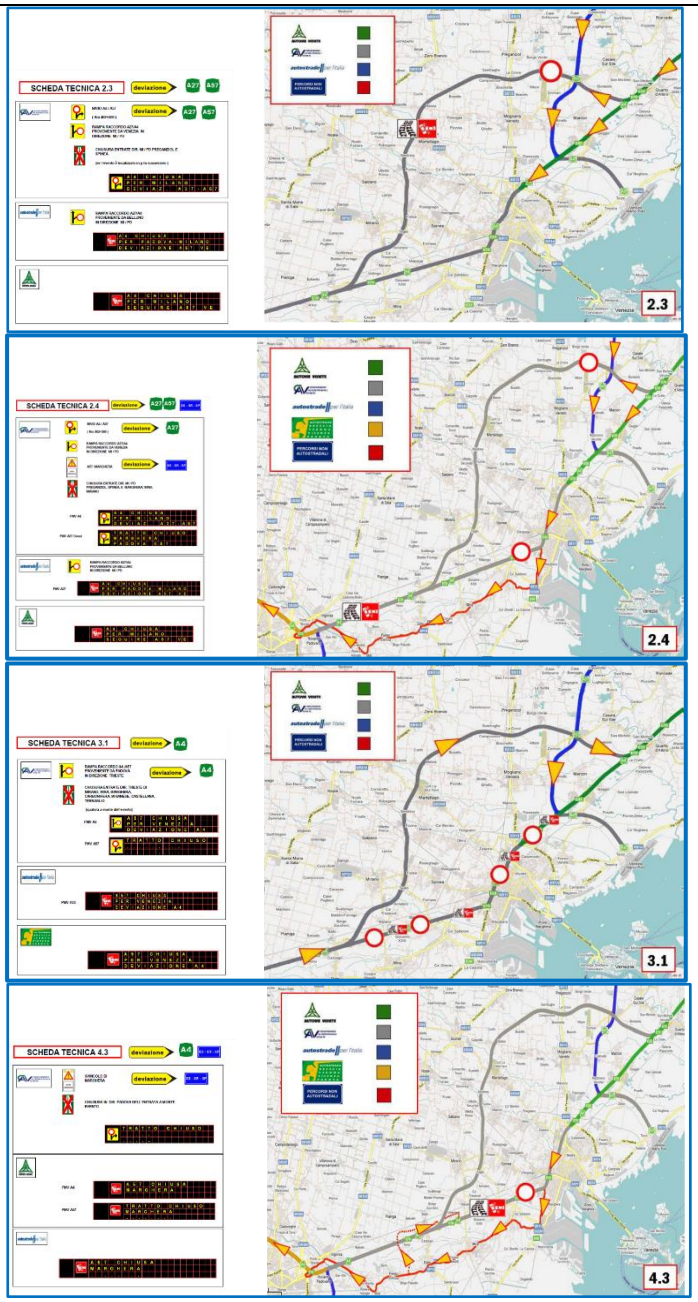
NOME AZIENDA	CODICE	COMUNE	NOTIFICA	RAPPORTO DI SICUREZZA
Brenta Gas srl	NF007	MIRA	X	X
Marchi Industriale spa	DF029	MIRA	X	
Reckitt Benckiser Italia spa	DF007	MIRA	X	X
Trivengas srl	DF045	MIRANO	X	X

ZONA 5

NOME AZIENDA	CODICE	COMUNE	NOTIFICA	RAPPORTO DI SICUREZZA
3V CPM - Chimica Porto Marghera spa	NF093	VENEZIA	X	X
A/M Bonifiche srl	NF178	VENEZIA	X	X
Alma Trasformazioni srl	NF074	VENEZIA	X	X
Arkema srl	NF048	VENEZIA	X	X
Bunge Italia spa	DF008	VENEZIA	X	
DECAL - Depositi Costieri Calloope spa	NF024	VENEZIA	X	X
ENI spa - Divisione Refining & Marketing	NF004	VENEZIA	X	X
IES - Italiana Energia e Servizi spa	NF036	VENEZIA	X	X
INEOS Vinyls Italia spa	NF039	VENEZIA	X	X
Montefibre spa	NF012	VENEZIA	X	X
Petroven srl	NF050	VENEZIA	X	X
Polimeri Europa spa	NF150	VENEZIA	X	X
San Marco Petroli spa	NF073	VENEZIA	X	X
SAPIO Produzione Idrogeno Ossigeno srl	DF012	VENEZIA	X	
Servizi Porto Marghera scarl	NF167	VENEZIA	X	X
Solvay Fluor Italia spa	NF013	VENEZIA	X	X
Syndial Attività Diversificate spa	NF009	VENEZIA	X	X

Descripción

ACCIDENTE EN UNA AUTOPISTA (INFRAESTRUCTURA CRÍTICA)	
Parámetro	**Descripción de los eventos**
Naturaleza del evento	*Accidente*
Tipo de evento	***Daños a la propiedad de los operadores de carreteras:*** *destrucción de partes de la infraestructura carretera: carriles en uso, pasos vehiculares superiores, puentes, túneles, obras de arte, cámaras de videovigilancia (cámaras con sensores de tráfico), sistemas informáticos integrados (control del tráfico vehicular y de las carreteras).* ***Daños a la propiedad inmaterial de los operadores de carreteras:*** *imagen de un servicio público dañado o incompetente, inserción del miedo en la población, mala imagen de la empresa*
Lugar del evento	*Italia, autopista de CAV llamada A4/A57*
Hora del evento	*En cualquier momento del día y de la noche.*
Objetivo (blanco)	Infraestructura carretera. Conductores.
Número de atacantes o transgresores	***Camiones/automóviles:*** *uno o más camiones, automóviles, camiones con mercancías peligrosas.*
Severidad de los daños	***Destrucción de infraestructura vial:*** *destrucción de puentes, pasos vehiculares superiores, obras de arte, túneles, carriles en uso.* ***Destrucción de equipamiento vial:*** *destrucción de sistemas de peaje y cámaras de tráfico (sistema de tráfico y monitoreo).*
Evento típico (Escenario)	 

	 *Cada escenario involucra tanto a la autopista como a la carretera urbana.* *El centro de monitoreo de la empresa clasifica la información de la red de los sistemas de monitoreo.*
Eventos secundarios	*Consecuencias financieras importantes en términos de reparaciones viales urgentes y pérdida de ganancias por el cierre de la autopista.*
Respuesta de los servicios de emergencia	*La aplicación del protocolo de operación es esencial y obligatoria, así como la aplicación de la regulación y el sistema de información para los usuarios, la aplicación de la gestión dinámica de los carriles de emergencia, el uso de semáforos para regular el acceso a la carretera ("ramp metering") así como el monitoreo del tráfico vehicular y de las carreteras mediante cámaras de tráfico.* *El sistema de control de tráfico, compuesto por HW y SW, identifica la estrategia de ajuste y la información que se le dará al usuario (paneles de mensaje variable).* *Al menos, el centro de monitoreo cuenta con la ayuda de administradores de tráfico que hacen que la carretera esté vigilada y que haya seguridad vial.*
Reportes de los medios de comunicación	*Los medios de comunicación transmitirán el caso en tiempo real.* *El sitio web de la empresa transmitirá en tiempo real el caso y también se comunicará el caso con los sistemas de información de la carretera (paneles de mensaje variable).*

El papel de la AC en el proceso de respuesta ante acciones maliciosas	*El protocolo operativo sobre la gestión de crisis de tráfico incluye el intercambio de información entre la institución y las empresas responsables de la gestión de eventos. Otra medida para prevenir, controlar y actuar rápidamente en caso de un acto similar a un accidente es utilizar una imagen en tiempo real del tráfico (por cámara de tráfico) y sistemas de vídeo para controlar el tráfico cerca de las áreas sensibles (estación de peaje, puentes, túneles, pasos vehiculares superiores, obras de arte).*

Asociación Mundial de la Carretera (PIARC)
Arche Sud 5° niveau
92055 La Défense Cedex, France

ISBN: 978-2-84060-526-3