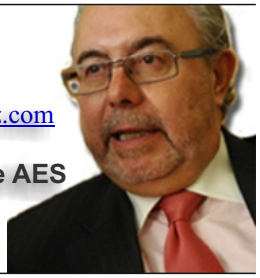
Recomendaciones para el diseño de instalaciones de sistemas de seguridad para la protección de las infraestructuras críticas y estratégicas

Manuel Sánchez Gómez-Merelo
www.manuelsanchez.com
Miembro de la Junta Directiva de AES



Un documento de la Asociación Española de Empresas de Seguridad (AES), con representación mayoritaria del sector de sistemas de seguridad, que ha tomado como referente lo establecido en la Ley 8/2011, por la que se establecen medidas para la Protección de las Infraestructuras Críticas, para el estudio, análisis y el establecimiento de recomendaciones para la implantación de sistemas de seguridad en este tipo de infraestructuras.

Protección de las infraestructuras críticas, nuevos retos para la seguridad privada.

Si observamos algunos datos o antecedentes, vemos que la inquietud por la necesidad de proteger determinadas infraestructuras consideradas como críticas se hace patente inicialmente con la adopción por parte del Consejo Europeo del 2004, de un Programa Europeo de Protección de Infraestructuras Críticas (EPCIP) así como de una Red de información de alerta (CIWIN).

En España, las actuaciones necesarias para optimizar la seguridad de las infraestructuras se enmarcan principalmente en el ámbito de la protección contra agresiones deliberadas y, muy especialmente, contra ataques terroristas, resultando por ello lideradas por el Ministerio del Interior.

Pero, ¿qué es la protección de las infraestructuras criticas y cuáles son?

Por Protección de las Infraestructuras Críticas se entiende *"el proceso de identificación, análisis, evaluación, estudio e implantación de los medios y medidas preventivas dirigidas para reducir el riesgo en situaciones, principalmente, de desastre natural, sabotaje, vandalismo o terrorismo".*

En este sentido, son infraestructuras críticas o estratégicas, aquellas determinadas por el Centro Nacional para la Protección de Infraestructuras Críticas (CN PIC) integradas dentro de los sectores de actividad siguientes:

Administración (servicios básicos, instalaciones, redes de información, y principales activos y monumentos del patrimonio nacional);
Instalaciones del Espacio; **Industria Química y Nuclear** (producción, almacenamiento y transporte de mercancías peligrosas, materiales químicos, biológicos, radiológicos, etc.);
Agua (embalses, almacenamiento, tratamiento y redes);
Centrales y Redes de Energía (producción y distribución);
Tecnologías de la Información y las Comunicaciones (TIC);
Salud (sector e infraestructuras sanitarias);
Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico, etc.);
Alimentación (producción, almacenamiento y distribución); y
Sistema Financiero y Tributario (entidades bancarias, información, valores e inversiones).

Por consiguiente, en el campo de la seguridad en infraestructuras críticas hay un importante trabajo realizado y por realizar y es por este motivo que el CN PIC, que es el órgano director y coordinador de cuantas actividades relacionadas con la protección de las infraestructuras críticas tiene encomendadas la Secretaría de Estado de Seguridad del Ministerio del Interior, a la que está adscrito, tiene como principal objetivo el prestar una eficaz colaboración para mantener seguras las infraestructuras críticas españolas que proporcionan los servicios esenciales a nuestra sociedad.

Todas y cada una de las Infraestructuras Críticas, requieren el estudio e implantación de medios y medidas con un enfoque

de seguridad integral e integrada que reúna y coordine las diferentes implicaciones y medidas nacionales e internacionales, puesto que hemos de pensar en global, aunque actuemos en local, teniendo en cuenta que la inseguridad está globalizada.

Igualmente, es fundamental que el sector de la seguridad privada, las empresas de servicios, instalaciones y proveedores de seguridad privada, se pongan en disposición especial para la participación e implicación en todo el proceso de este Programa de Protección de las Infraestructuras Críticas, dados los medios, conocimiento y experiencia que en esta materia tiene.

Antecedentes. Legislación y Normativa

En España, el Plan Nacional de Protección de Infraestructuras Críticas las define como: *"Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas".* Esta definición ya fue establecida por la Directiva europea 2008/114/CE del 8 de diciembre de 2008, subrayando sobre la importancia de *"la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección".*

Ley española 8/2011 de protección de infraestructuras críticas

En consecuencia, y dada la complejidad de la materia, su incidencia sobre la seguridad de las personas y sobre el funcionamiento de las estructuras básicas nacionales e internacionales, y en cumplimiento de lo estipulado por la Directiva 2008/114/CE, se hace preciso elaborar una norma cuyo objeto es, por un lado, regular la protección de las infraestructuras críticas contra ataques deliberados de todo tipo (tanto de carácter físico como cibernético) y, por otro lado, la definición de un sistema organizativo de protección de dichas infraestructuras que aglutine a las administraciones públicas y entidades privadas afectadas.

Por todo ello, se promulga la Ley 8/2011 por la que se establecen medidas para la Protección de las Infraestructuras Críticas y su desarrollo por el Reglamento por el RD 7047/2011. Como pieza básica de este sistema, la Ley crea el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) como órgano de asistencia al Secretario de Estado de Seguridad en la ejecución de las funciones que se le encomiendan a éste como órgano responsable del sistema.

Planteamiento de las seguridades. En un planteamiento de seguridad global, los objetivos básicamente son: prevenir los riesgos, aumentar la protección, garantizar la intervención, minimizar los daños o pérdidas, incrementar la resiliencia, sistematizar las inspecciones y facilitar el apoyo y las ayudas exteriores. Todo enmarcado en el cumplimiento de la legislación y la normativa vigente.

Marco, en el que como ya se ha definido, *"infraestructuras críticas son aquellas cuyo funcionamiento resulta indispensable y no permite soluciones alternativas, por lo que su destrucción o alteración tendría un grave impacto derivado de los tipos de riesgos y de sus magnitudes o consecuencias".*

Por tanto, para su protección hay que desarrollar especialmente y en profundidad los criterios para la identificación y evaluación de los riesgos y las amenazas derivadas de la naturaleza, de los riesgos tecnológicos, de los antisociales

o actos deliberados y delictivos, e incluso, de los derivados de las actividades sociales y laborales.

Planes de Seguridad. La Ley 8/2011, así como el Reglamento que la desarrola, han establecido un conjunto de Planes de Protección de aquellas, que para una mejor comprensión, se ha considerado adecuado clasificarlas en relación al responsable de su creación, que en unos casos corresponde a la Administración Pública y en otros al Operador Crítico.

Clasificación de los Planes del Sistema de Protección

• **Responsabilidad de la Administración:**

1. PLAN NACIONAL DE PROTECCIÓN DE PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS (Secretaría de Estado de Seguridad del Ministerio del Interior).

2. PLANES ESTRATÉGICOS SECTORIALES (Elaborado por el Grupo de Trabajo coordinado por el CNPIC).

3. PLAN DE APOYO OPERATIVO (Cuerpo Policial Estatal o Autonómico, en su caso).

• **Responsabilidad del Operador:**

1. PLAN DE SEGURIDAD DEL OPERADOR.

2. PLAN DE PROTECCIÓN ESPECÍFICO (De cada instalación crítica).

Planes de Protección Específicos. De especial incidencia e implicación para los medios y sistemas de seguridad se encuentran los Planes de Protección Específicos (PPE) que se definen y desarrollan con el esquema siguiente:

Concepto: los Planes de Protección Específicos son los documentos operativos donde se deben definir las medidas concretas ya adoptadas y las que se vayan a adoptar por los operadores críticos para garantizar la seguridad integral (física y lógica) de cada una de sus infraestructuras críticas.

Contenido: los Planes de Protección Específicos de las diferentes infraestructuras críticas incluirán todas aquellas medidas que los respectivos operadores críticos consideren necesarias en función de los análisis de riesgos realizados respecto de las amenazas, en particular, las de origen terrorista, sobre sus activos, incluyendo los sistemas de información. Cada Plan de Protección Específico deberá contemplar la adopción tanto de medidas permanentes de protección, sobre la base de lo dispuesto en el párrafo anterior, como de medidas de seguridad temporales y graduadas, que vendrán en su caso determinadas por la activación del Plan Nacional de Protección de las Infraestructuras Críticas, o bien como consecuencia de las comunicaciones que las autoridades competentes puedan efectuar al operador crítico en relación con una amenaza concreta sobre una o varias infraestructuras por él gestionadas

La Secretaría de Estado de Seguridad, a través del CNPIC, establecerá los contenidos mínimos de los Planes de Protección Específicos, así como el modelo en el que fundamentar la estructura y contenido de éstos que, en todo caso, cumplirán las directrices marcadas por sus respectivos Planes de Seguridad del Operador.

En la resolución de aprobación o modificación, el CNPIC, basándose en los informes o proyectos presentados efectuará al operador crítico las recomendaciones que estime pertinentes, proponiendo en todo caso un calendario de implantación gradual donde se fije el orden de

preferencia de las medidas y los procedimientos a adoptar sobre las infraestructuras afectadas.

Los Medios y Sistemas de Seguridad. Sistemas y Tecnologías

En la actualidad, los medios técnicos, los sistemas y tecnologías en su aplicación para la protección de las Infraestructuras Críticas y Estratégicas, están lo suficientemente evolucionados como para no existir problema alguno en el planteamiento de la prevención y protección de todos y cada uno de los riesgos y amenazas que comportan el amplio catálogo de aplicación a este tipo de instalaciones. No obstante, una serie de aspectos pueden condicionar o recomendar la implantación de ciertos tipos de sistemas de seguridad.

Así, los medios técnicos se dispondrán prioritariamente para el cumplimiento de la legislación y la normativa vigente en cada caso o comunidad social, que se centran, principalmente, en la instalación de los medios para la prevención y protección contra actividades antisociales y terrorismo, así como el establecimiento de los medios y sistemas complementarios para facilitar la ejecución de los planes de autoprotección.

Con independencia de las disposición de los medios y medidas de seguridad por imperativo legal, pueden existir -según los casos y circunstancias- muchas otras situaciones donde, con carácter general, otros tipos de riesgos relacionados directamente con las Infraestructuras Críticas, pasen igualmente a la consideración de prioritarios o muy importantes en función de su análisis y evaluación, como es el caso de algunos riesgos de tipo técnico y, sobre todo, los agrupados en el ámbito de los riesgos derivados de las actividades antisociales o actos deliberados.

De cualquier modo, como contraposición a cada uno de los grupos de riesgo diferenciados, se dispondrán los medios de protección física o pasiva, medios técnicos de control, video vigilancia, sistemas de detección alarma, comunicaciones, etc. que, en cada caso, correspondan. Todo ello, sin olvidar el mantenimiento de los objetivos que prioritariamente nos hemos fijado de eficacia, celeridad y flexibilidad y, desde luego, sin perder la perspectiva de la optimización de los recursos disponibles o a disponer.

En este sentido, como es sabido, el mercado de la oferta de medios técnicos agrupados por áreas de riesgo diferenciadas, tanto en sus campos de lo que podríamos denominar la protección pasiva (medios físicos y mecánicos) como la protección activa (medios electrónicos) así como la seguridad lógica, presenta para sus aplicaciones -generales y específicas- en las Infraestructuras Críticas y Estratégicas, una muy amplia gama de materiales, productos, equipos y sistemas perfectamente adecuados para responder a la exigencia de seguridad ante los riesgos planteados y sus distintas y posibles valoraciones o necesidades.

Planteamiento y recomendaciones

En general, los medios técnicos para la prevención de los riesgos o para la protección de personas y bienes se dispondrán directamente relacionados con los tipos de riesgos y amenazas ante los que han de enfrentarse, con la correspondiente evaluación de éstos y, consecuentemente, con la decisión final al respecto de la reducción, asunción o transferencia de estos riesgos y amenazas potenciales o reales.

Los medios técnicos de prevención y protección son, por tanto, todos aquellos materiales, elementos, dispositivos,

equipos y sistemas que se pueden emplear o se emplean, en general o específicamente, como contraposición a los riesgos o amenazas identificados y evaluados.

El marco de trabajo y tratamiento establecido para los medios técnicos en este documento como "RECOMENDACIONES PARA EL DISEÑO DE INSTALACIONES DE SISTEMAS DE SEGURIDAD PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS Y ESTRATÉGICAS", se centra en el esquema de contenido siguiente:

1. OBJETO. INTRODUCCIÓN, sobre la base del planteamiento y desarrollo de la Ley 8/2011;

2. FASES DE PROYECTO, desde un esquema de tratamiento integral del diseño y análisis, la instalación, la operación y el mantenimiento de los sistemas;

3. ÁREA DE IMPLANTACIÓN DE LAS MEDIDAS, desde el esquema de aplicación sobre áreas perimetrales, áreas periféricas o áreas interiores;

4. SISTEMAS DE PROTECCIÓN, bajo la clasificación de la Protección Contra la Intrusión, el Control de Accesos, la Protección de Información y Valores, la Centralización e Integración de Sistemas y los Sistemas de Control y Coordinación de Medidas de Seguridad Físicas y Lógicas.

Todos los sistemas de seguridad clasificados en este Documento de Recomendaciones se especifican por su tipo de equipo, su instalación para cada nivel de riesgo, sus observaciones a tener en cuenta y sus recomendaciones de aplicación.

Finalmente, y sin ánimo de ser exhaustivos, se considera que el sector y la industria de las seguridades presentan múltiples medios y medidas de prevención y protección de total aplicación a las Infraestructuras Críticas y Estratégicas, tanto en su aplicación general como específica.