

III. OTRAS DISPOSICIONES

MINISTERIO DEL INTERIOR

18439 *Resolución de 15 de noviembre de 2011, de la Secretaría de Estado de Seguridad, por la que se establecen los contenidos mínimos de los planes de seguridad del operador y planes de protección específicos conforme a lo dispuesto en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de infraestructuras críticas.*

El Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de Infraestructuras Críticas, como desarrollo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas dispone, en los artículos 22.4 y 25.5, que la Secretaría de Estado de Seguridad establecerá, respectivamente, los contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos, comprendidos en el artículo 14 de la Ley.

En su virtud, resuelvo ordenar la publicación en el «Boletín Oficial del Estado» de los contenidos mínimos para la elaboración de los citados Planes, que se insertan como anexos, dando cumplimiento a lo establecido en el artículo 7, apartado e), del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de Infraestructuras Críticas.

Madrid, 15 de noviembre de 2011.—El Secretario de Estado de Seguridad, Justo Tomás Zambrana Pineda.

ANEXO I

Guía Contenidos Mínimos

Plan de Seguridad del Operador (PSO)

Índice

1. Introducción.
 - 1.1 Base Legal.
 - 1.2 Objetivo de este Documento.
 - 1.3 Finalidad y Contenido del PSO.
 - 1.4 Método de Revisión y Actualización.
 - 1.5 Protección y Gestión de la Información y Documentación.
2. Política general de seguridad del operador y marco de gobierno.
 - 2.1 Política General de Seguridad del Operador.
 - 2.2 Marco de Gobierno de Seguridad.
 - 2.2.1 Organización de la Seguridad.
 - 2.2.1.1 El Responsable de Seguridad y Enlace.
 - 2.2.1.2 El Delegado de Seguridad de la Infraestructura Crítica.
 - 2.2.2 Formación y Concienciación.
 - 2.2.3 Modelo de Gestión Aplicado.

3. Relación de Servicios Esenciales Prestados por el Operador Crítico.
 - 3.1 Identificación de los Servicios Esenciales.
 - 3.2 Mantenimiento del Inventario de Servicios Esenciales.
 - 3.3 Estudio de las Consecuencias de la Interrupción del Servicio Esencial.
 - 3.4 Interdependencias.
4. Metodología de Análisis de Riesgos.
 - 4.1 Descripción de la Metodología de Análisis.
 - 4.2 Tipologías de Activos que Soportan los Servicios Esenciales.
 - 4.3 Identificación y Evaluación de Amenazas.
 - 4.4 Valoración y Gestión de Riesgos.
5. Criterios de Aplicación de Medidas de Seguridad Integral.
6. Documentación Complementaria.
 - 6.1 Normativa, Buenas Prácticas y Regulatoria.
 - 6.2 Coordinación con Otros Planes.

1. *Introducción*

1.1 Base Legal.

El normal funcionamiento de los servicios esenciales que se prestan a la ciudadanía descansa sobre una serie de infraestructuras de gestión tanto pública como privada, cuyo funcionamiento es indispensable y no permite soluciones alternativas: las denominadas infraestructuras críticas. Por ello, se hace necesario el diseño de una política de seguridad homogénea e integral en el seno de las organizaciones que esté específicamente dirigida al ámbito de las infraestructuras críticas, en la cual se definan los subsistemas de seguridad que se van a implantar para la protección de las mismas con el objetivo de impedir su destrucción, interrupción o perturbación, con el consiguiente perjuicio de la prestación de los servicios esenciales a la población.

Este es precisamente el espíritu de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, que tiene como objeto el establecer las estrategias y las estructuras organizativas adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las administraciones públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, impulsando la colaboración e implicación de los organismos y empresas gestoras y propietarias (operadores críticos) de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados tanto físicos como lógicos, que puedan afectar a la prestación de los servicios esenciales.

Dicha Ley tiene su desarrollo a través del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

El artículo 13 de la Ley explicita una serie de compromisos para los operadores críticos públicos y privados, entre los que se encuentra la necesidad de elaboración de un Plan de Seguridad del Operador (en adelante PSO) y de los Planes de Protección Específicos que se determinen (en adelante PPE).

Por su parte, el artículo 22.4 del Real Decreto 704/2011 responsabiliza a la Secretaría de Estado de Seguridad, a través del CNPIC, del establecimiento y puesta a disposición de los operadores de los contenidos mínimos con los que deben contar los PSO, así como el modelo en el que basar la elaboración de los mismos.

1.2 Objetivo de este Documento.

Con el presente documento se pretende dar cumplimiento a las instrucciones emanadas del Real Decreto 704/2011, estableciendo los contenidos mínimos sobre los que se debe de apoyar el operador a la hora del diseño y elaboración de su PSO. A su

vez, se establecen algunos puntos explicativos sobre aspectos recogidos en la normativa de referencia.

Igualmente, se pretende orientar a aquellos operadores que hayan sido o vayan a ser designados como críticos en el diseño y elaboración de su respectivo Plan, con el fin de que éstos puedan definir el contenido de su política general y el marco organizativo de seguridad, que encontrará su desarrollo específico en los PPE de cada una de sus infraestructuras críticas.

1.3 Finalidad y Contenido del PSO.

El PSO definirá la política general del operador para garantizar la seguridad integral del conjunto de instalaciones o sistemas de su propiedad o gestión.

El PSO, como instrumento de planificación del Sistema de Protección de Infraestructuras Críticas, contendrá, además de un índice referenciado sobre los contenidos del Plan, al menos la siguiente información:

- Política general de seguridad del operador y marco de gobierno.
- Relación de Servicios Esenciales prestados por el Operador Crítico.
- Metodología de análisis de riesgo (amenazas físicas y lógicas).
- Criterios de aplicación de Medidas de Seguridad Integral.

1.4 Método de Revisión y Actualización.

Conforme al artículo 24 del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, entre las obligaciones del operador, además de la elaboración y presentación del PSO al Centro Nacional de Protección de Infraestructuras Críticas (en adelante CNPIC), se incluye su revisión y actualización periódica:

- Revisión: Bienal.
- Actualización: Cuando se produzca algún tipo de modificación en los datos incluidos en el PSO. En este caso, el PSO quedará actualizado cuando dichas modificaciones hayan sido validadas por el CNPIC, o en las condiciones establecidas en su normativa sectorial específica.

1.5 Protección y Gestión de la Información y Documentación.

La información es un valor estratégico para cualquier organización, por lo que en este sentido, el operador debe definir sus procedimientos de gestión y tratamiento de la información, así como los estándares de seguridad precisos para prestar una adecuada y eficaz protección de la información, independientemente del formato en el que ésta se encuentre.

Además, los operadores designados como críticos, deberán tratar los documentos que se deriven de la aplicación de la Ley 8/2011 y su desarrollo normativo a través del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, según el grado de clasificación que se derive de las citadas normas.

En virtud de la disposición adicional segunda de la Ley 8/2011, la clasificación del PSO constará de forma expresa en el instrumento de su aprobación. Una vez aprobado, el PSO tendrá la clasificación de Confidencial, siéndole de aplicación desde ese momento los requisitos y medidas de seguridad previstos en su normativa regulatoria específica.

2. Política general de seguridad del operador y marco de gobierno

2.1 Política General de Seguridad del Operador.

El objetivo de una Política de Seguridad es dirigir y dar soporte a la gestión de la seguridad. En ella, la Dirección de la Organización debe establecer claramente cuáles son sus líneas de actuación y manifestar su apoyo y compromiso con la seguridad.

Por tanto, en este apartado, el operador deberá reflejar el contenido de su Política de Seguridad de una forma homogénea e integral que esté específicamente dirigida al ámbito de las infraestructuras críticas, y que sirva de marco de referencia para la protección de las mismas, con el objetivo de impedir su perturbación o destrucción.

Los aspectos mínimos que debe recoger la Política de Seguridad son:

- Objeto: La meta que pretende conseguir la Organización con la Política y su posterior desarrollo y aplicación.
- Ámbito o Alcance de Aplicación: Una política puede estar limitada a determinados campos o aspectos o, por el contrario, ser de aplicación a toda una Organización. El Operador deberá reflejar a qué partes de su Organización es aplicable la Política de Seguridad, sin perder de vista que la misma ha de tener un carácter integral, considerando tanto la seguridad física como la lógica.
- Compromiso de la Alta Dirección: El Operador debe garantizar que a la seguridad debe dársele la misma importancia que a otros factores de la producción o negocio de la organización. Por ello, el compromiso de la Organización con la Política de Seguridad y lo que de ella se desarrolle deberá quedar plasmado mediante la aprobación, sanción y apoyo de la misma por el órgano (Consejo de Administración, Consejo de Dirección, etc.) o la persona (Presidente, Consejero Delegado, etc.) de gobierno o dirección de la misma, así como su firme y explícito compromiso con la protección de los servicios esenciales prestados.
- Carácter Integral de la Seguridad: La seguridad física y lógica son áreas que deben ser abordadas de forma interrelacionada y con una perspectiva holística de la seguridad. Esto redundará en una visión global de la seguridad, posibilitando el diseño de una estrategia corporativa única, optimizando el conocimiento, los recursos, y los equipos. Por ello, el Operador deberá remarcar el carácter integral de la seguridad aplicada a sus infraestructuras críticas. En este sentido, una respuesta integral a las diferentes amenazas existentes requiere la aplicación coordinada de medidas de seguridad tanto físicas como lógicas.
- Relación del PSO con otras normativas o reglamentaciones aplicables: Esta referencia podrá ser incorporada en el punto 6 de esta guía.
- Actualización de la Política: Al ser la política un documento de alto nivel, no suele requerir cambios significativos a lo largo del tiempo. No obstante, el Operador deberá asegurarse de que ésta se mantenga actualizada y refleje aquellos cambios requeridos por variaciones en los activos a proteger, del entorno que les pueda afectar (amenazas, vulnerabilidades, impactos, salvaguardas), o en la reglamentación aplicable. En este apartado, el Operador deberá recoger el proceso a seguir para la actualización y mantenimiento de la Política, incluyendo el responsable de llevar a cabo estas acciones.

2.2 Marco de Gobierno de Seguridad.

2.2.1 Organización de la Seguridad.

El Operador Crítico debe designar a un responsable de seguridad y enlace y a unos delegados de seguridad de acuerdo a los requisitos establecidos en la Ley 8/2011. Deberá, por tanto, asegurarse de que éstos estén en un nivel jerárquico suficiente en su estructura organizacional, de tal forma que los designados puedan garantizar el cumplimiento y la aplicación de la Política y de los requisitos establecidos para la protección de las infraestructuras críticas bajo su responsabilidad.

En este apartado, el Operador Crítico deberá describir su organigrama de seguridad (afectando a la Seguridad Física y la Seguridad Lógica), con indicación de las figuras recogidas en la Ley, así como los niveles jerárquicos que les correspondan en su

estructura organizativa. Además, deberá dejar constancia de que los designados tienen capacidad suficiente para llevar a cabo todas aquellas acciones que se deriven de la aplicación de la Ley y el Real Decreto:

- Organigrama de Seguridad.
- Organigrama general en el que se señale dónde se integran las distintas funciones de seguridad en la organización.

Asimismo, el Operador Crítico deberá señalar los Comités u órganos de decisión existentes en materia de seguridad física y lógica.

A su vez se deberá de reflejar si la gestión y el mantenimiento de la seguridad integral en alguno de sus ámbitos es propia o subcontratada. En este último supuesto se deberá de reflejar el tipo de servicios y compromisos acordados entre el operador y la empresa contratada.

2.2.1.1 El Responsable de Seguridad y Enlace.

Conforme al artículo 16.2 de la Ley, el Operador Crítico deberá designar a una persona en la organización que deberá estar habilitada por el Ministerio del Interior como Director de Seguridad, en virtud de lo dispuesto en el Real Decreto 2364/1994, de 9 de diciembre, en el que se aprueba el Reglamento de Seguridad Privada, o tener una habilitación equivalente, según su normativa sectorial específica.

El operador crítico deberá hacer constar en este apartado el nombre y datos de contacto (dirección, teléfonos y email) de la persona que fue designado como Responsable de Seguridad y Enlace así como de su sustituto. Sus funciones en relación con el artículo 34.2 del Real Decreto 704/2011 son las siguientes:

- Representar al operador crítico ante la Secretaria de Estado de Seguridad:
 - En materias relativas a la seguridad de sus infraestructuras.
 - En lo relativo a los diferentes planes especificados en el Real Decreto.
- Canalizar las necesidades operativas e informativas que surjan.

2.2.1.2 El Delegado de Seguridad de la Infraestructura Crítica.

Conforme al artículo 17 de la Ley, el Operador Crítico con infraestructuras designadas como críticas o críticas europeas comunicará a las Delegaciones del Gobierno o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquellas se ubiquen, la persona designada como Delegado de seguridad y su sustituto.

El operador crítico deberá hacer constar en este apartado el nombre y datos de contacto (dirección, teléfonos y email) de la persona que fue designado como Delegado de Seguridad así como de su sustituto, cumpliendo los plazos establecidos desde su designación como operador crítico así como su participación a las Autoridades correspondientes, según lo establecido en el artículo 35.1 del Real Decreto 704/2011. Sus funciones en relación con el artículo 35.2 del Real Decreto 704/2011, son las siguientes:

- Ser el enlace operativo y el canal de información con las autoridades competentes en materias relativas a la seguridad de sus infraestructuras.
- Canalizar las necesidades operativas e informativas que surjan.

2.2.2 Formación y Concienciación.

El Operador Crítico deberá colaborar con los programas o ejercicios que puedan derivarse del Plan Estratégico Sectorial, así como en su momento de los Planes de Apoyo Operativo.

El Operador Crítico deberá reflejar en este apartado el Plan de Formación previsto para el personal relacionado con la protección de las infraestructuras críticas.

En el caso de que disponga de un Plan de Formación General, especificará la parte relacionada con la protección de las infraestructuras críticas, y la incluirá en este punto.

El personal implicado directamente en la protección de los servicios esenciales e Infraestructuras críticas deberá ser formado para alcanzar las siguientes habilidades:

- Capacidad de comprensión de la seguridad integral (física y lógica).
- Capacidad de comprensión de la autoprotección.
- Capacidad de comprensión de la seguridad del medio ambiente.
- Habilidades organizativas y de comunicación.

El personal no directamente implicado deberá ser concienciado mediante la aplicación de las políticas de formación y operacionales activas en la organización.

2.2.3 Modelo de Gestión Aplicado.

La seguridad integral depende de un proceso de gestión integral que debe aportar el control organizativo y técnico necesario para determinar en todo momento el nivel de exposición a las amenazas y el nivel de protección y respuesta que es capaz de proporcionar la organización para la protección y seguridad de sus servicios esenciales e Infraestructuras Críticas.

Por tanto, de acuerdo con esta política de seguridad, el Operador Crítico deberá recoger dentro del PSO su modelo de gestión, que deberá contemplar al menos, los siguientes aspectos:

- Una implementación de controles de seguridad acorde con las prioridades y necesidades evaluadas.
- Una evaluación y monitorización periódica de seguridad.

3. *Relación de Servicios Esenciales Prestados por el Operador Crítico*

El PSO deberá incluir, a modo de introducción, la información de contexto suficiente para describir los siguientes aspectos:

- Presentación general del Operador Crítico, y sector/subsector principal/es de su actividad.
- Estructura organizativa y societaria (en el caso de Grupos empresariales).
- Presencia geográfica en los ámbitos nacional e internacional, con un resumen de las Comunidades Autónomas y países donde presten sus servicios.
- Principales líneas de actividad con la tipología general de servicios / productos que ofrecen.

3.1 Identificación de los Servicios Esenciales.

El PSO deberá identificar aquellos servicios esenciales para la ciudadanía, prestados por el operador a través del conjunto de sus infraestructuras estratégicas ubicadas en el territorio nacional, en relación al concepto de servicio esencial recogido en el artículo 2.a) de la Ley:

- Servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos.
- Eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

3.2 Mantenimiento del Inventario de Servicios Esenciales.

Periódicamente, el Operador Crítico deberá revisar la relación de servicios esenciales que figuran en su PSO, como consecuencia de la evolución normal que cualquier empresa experimenta respecto a los servicios que ofrece.

Así, en este mantenimiento deberá incorporar aquellos cambio/s que se produzcan:

- Por causas endógenas (por ejemplo, ajuste de cartera de servicios, fusiones, adquisiciones o ventas de activos, etc.).
- Como consecuencia de la adecuación a los períodos establecidos en el Plan conforme al punto 1.4 de esta guía.

3.3 Estudio de las Consecuencias de la Interrupción del Servicio Esencial.

El Operador Crítico deberá llevar a cabo un estudio de las consecuencias que supondría la interrupción y no disponibilidad del servicio esencial que presta a la sociedad, motivado por alguna alteración o interrupción en el tiempo o una destrucción parcial o total de las infraestructuras que gestionan dicho servicio.

3.4 Interdependencias.

En relación con el concepto de interdependencias recogido en el artículo 2.j) de la Ley, pueden existir efectos y repercusiones que afecten los servicios esenciales y las infraestructuras críticas propias y/o de otros operadores, tanto dentro del mismo sector como en ámbitos diferentes. Estas interdependencias deberán ser en todo caso consideradas en el análisis de riesgos que realicen los operadores en el marco global de su organización, dentro del PSO.

El Operador Crítico deberá hacer referencia dentro de su PSO a las interdependencias que, en su caso, identifique, explicando brevemente el motivo que las origina:

- Entre sus propias instalaciones o servicios.
- Con servicios esenciales prestados por otros Operadores Críticos del mismo sector.
- Con servicios esenciales prestados a otros Operadores Críticos de distinto sector.
- Con servicios esenciales prestados por operadores de otros países.
- Con sus proveedores dentro de la cadena de suministros.

4. Metodología de Análisis de Riesgos

En virtud de lo establecido en el artículo 22.3 del Real Decreto 704/2011, en el PSO se deberá establecer una metodología de análisis de riesgos que garantice la continuidad de los servicios proporcionados por dicho operador en la que se contemple, de una manera global, tanto las amenazas físicas como lógicas existentes contra la totalidad de sus activos, con independencia de las medidas mínimas que se puedan establecer para los Planes de Protección Específicos conforme a lo establecido por el artículo 25.

4.1 Descripción de la Metodología de Análisis.

Se describirá de forma genérica la metodología empleada por la Organización para la realización de los análisis de riesgos de los PPE que se deriven tras la designación de sus infraestructuras críticas. Al menos, se aportará la siguiente información:

- Etapas esenciales.
- Algoritmos de cálculo empleados.
- Carácter cuantitativo o cualitativo.
- Método empleado para la valoración de los impactos.
- Métricas de medición de riesgos aceptables, residuales, etc.
- En particular, se harán constar las relaciones entre los análisis de riesgos realizados a distintos niveles: A nivel de corporación, a nivel de servicios y el más concreto, a nivel de infraestructuras críticas.

4.2 Tipologías de Activos que Soportan los Servicios Esenciales.

Se denominan activos los recursos necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

Sobre la base de los servicios identificados en el apartado 3.1 anterior, se incluirán en este apartado, para cada servicio esencial, los tipos de activos que los soportan, diferenciando aquellos que son críticos de los que no lo son.

Algunas de las tipologías de activos a considerar son:

- Los servicios esenciales que prestan.
- Las instalaciones necesarias para la prestación del servicio esencial.
- Los sistemas informáticos (hardware y software).
- Las redes de comunicaciones que permiten intercambiar datos.
- Las personas que explotan u operan todos los elementos anteriormente citados.

No es objeto de esta sección la identificación exhaustiva de activos que soportan la actividad del operador, sino la identificación genérica de tipologías de activos asociadas a los servicios esenciales prestados por dicho operador, y sobre los que se focalizará el análisis de riesgos que efectúe el operador. El nivel de granularidad será aquel que permita una comprensión del funcionamiento de los servicios, así como las interrelaciones entre activos y servicios.

Los activos no serán necesariamente espacios físicos concretos, pudiendo por ejemplo considerarse como activos sistemas distribuidos, tales como una red de datos.

4.3 Identificación y Evaluación de Amenazas.

En el marco de la normativa de protección de infraestructuras críticas, y de cara a garantizar la adecuada protección de aquellas infraestructuras que prestan servicios esenciales, el Operador Crítico deberá considerar de forma especial aquellas amenazas de origen terrorista o intencionado. El Operador deberá indicar expresamente las amenazas que ha considerado para la realización de los análisis de riesgo, plasmando al menos:

- Las intencionadas, de tipo tanto físico como lógico, que puedan afectar al conjunto de sus infraestructuras, las cuales deberán identificarse de forma específica en sus respectivos PPE.
- Las procedentes de interdependencias, que puedan afectar directamente a los servicios esenciales, sean estas deliberadas o no.
- Las dirigidas al entorno cercano o elementos interdependientes que puedan afectar a los servicios esenciales, tanto del ante-perímetro físico como lógico.

4.4 Valoración y Gestión de Riesgos.

Los PSO recogerán la estrategia de gestión de riesgos implementada por el Operador en cuanto a:

- Criterios utilizados para la valoración de las diferentes categorías de clasificación de los riesgos.
- Metodología de selección de estrategia (reducción, eliminación, transferencia, etc.).
- Plazos para la implementación de medidas en el caso de elegir una estrategia de minimización del riesgo con indicación, si existe, de mecanismos de priorización de acciones.
- Tratamiento dado a las amenazas de ataques deliberados y, en particular, a aquellas que tengan una baja probabilidad pero un alto impacto debido a las consecuencias por su destrucción o interrupción en la continuidad de los servicios esenciales.
- Mecanismos de seguimiento y actualización periódicos de niveles de riesgo.

5. Criterios de Aplicación de Medidas de Seguridad Integral

Dentro del ámbito de la seguridad integral, el Operador definirá a grandes rasgos los criterios utilizados en su organización para la aplicación y administración de la seguridad. En este sentido incluirá de forma genérica las medidas de seguridad implantadas en el conjunto de activos y recursos sobre los que se apoyan los servicios esenciales y que se recogerán en sus respectivos PPE, al objeto de hacer frente a las amenazas físicas y lógicas identificadas en los oportunos análisis de riesgos efectuados sobre cada una de las tipologías de sus activos.

6. Documentación Complementaria

6.1 Normativa, Buenas Prácticas y Regulatoria.

El Operador recogerá en una breve referencia motivada toda la normativa de aplicación y aquellas buenas prácticas que regulen el buen funcionamiento de los servicios esenciales prestados por todas y cada una de sus infraestructuras.

La normativa a incluir comprenderá tanto las de rango nacional, autonómico, europeo e internacional, como las sectoriales, relativas a:

- Seguridad Física.
- Seguridad Lógica.
- Seguridad de la Información en cualquiera de sus ámbitos.
- Seguridad Personal.
- Seguridad Ambiental.
- Autoprotección y Prevención de Riesgos Laborales.

6.2 Coordinación con Otros Planes.

Se identificarán todos aquellos Planes diseñados por el operador relativos a otros aspectos (continuidad de negocio, gestión del riesgo, respuesta, autoprotección, emergencias, etc.) que puedan coordinarse con el Plan de Seguridad del Operador y los respectivos Planes de Protección Específicos, y que serán activados en el caso de que las medidas preventivas fallen y se produzca el incidente.

ANEXO II

Guía Contenidos Mínimos

Plan de Protección Específico (PPE)

Índice

1. Introducción.
 - 1.1 Base legal.
 - 1.2 Objetivo de este documento.
 - 1.3 Finalidad y contenido del PPE.
 - 1.4 Método de revisión y actualización.
 - 1.5 Protección y gestión de la información y documentación.
2. Aspectos organizativos.
 - 2.1 Delegados de seguridad de las infraestructuras críticas.
 - 2.2 Mecanismos de coordinación.
 - 2.3 Mecanismos y responsables de aprobación.
3. Descripción de la infraestructura crítica.
 - 3.1 Datos generales de la infraestructura crítica.

- 3.2 Activos / elementos de la IC.
- 3.3 Interdependencias.
- 4. Resultados del análisis de riesgos.
 - 4.1 Amenazas consideradas.
 - 4.2 Medidas existentes.
 - 4.2.1 Organizativas o de gestión.
 - 4.2.2 Operacionales o procedimentales.
 - 4.2.3 De protección o técnicas.
 - 4.3 Valoración de riesgos.
- 5. Plan de acción propuesto (por activo).
- 6. Documentación complementaria.

1. *Introducción*

1.1 Base legal.

Según establece la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, el operador designado como crítico se integrará como agente del sistema de protección de infraestructuras críticas, debiendo cumplir con una serie de responsabilidades recogidas en su artículo 13. De acuerdo con en el punto 1, letra «d», del citado artículo, el Operador deberá elaborar un Plan de Protección Específico (en adelante PPE) por cada una de las infraestructuras críticas de las que sea propietario o gestor.

El Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, a través del cual se da desarrollo reglamentario a la Ley 8/2011, establece, en su capítulo IV del Título III sobre los Instrumentos de Planificación, aquellos aspectos relativos a la elaboración, finalidad y contenido de dichos planes, formas de revisión y actualización, autoridades encargadas de su aplicación y seguimiento y compatibilidad con otros planes ya existentes.

En este sentido, y conforme al artículo 25.5 de dicho Real Decreto, se asigna a la Secretaría de Estado de Seguridad, a través del CNPIC, la responsabilidad de establecer los contenidos mínimos de los PPE, así como el modelo en el que fundamentar su estructura y compleción, sobre la base de las directrices y criterios marcados por el Plan de Seguridad del Operador (PSO).

En el PPE, el Operador Crítico público o privado recogerá de forma práctica los siguientes aspectos y criterios incluidos en su Plan de Seguridad del Operador, que afecten de manera específica a esa instalación:

- Aspectos relativos a su política general de seguridad.
- Desarrollo de la metodología de análisis de riesgos que garantice la continuidad de los servicios proporcionados por dicho operador a través de esa infraestructura crítica (IC).
- Desarrollo de los criterios de aplicación de las diferentes medidas de seguridad que se implanten para hacer frente a las amenazas, tanto físicas como lógicas, identificadas en relación con cada una de las tipologías de los activos existentes en esa infraestructura.

1.2 Objetivo de este Documento.

Con el presente documento se pretende dar cumplimiento a las instrucciones emanadas del Real Decreto 704/2011, estableciendo los contenidos mínimos sobre los que se debe de apoyar el operador a la hora de elaborar su respectivo PPE en las instalaciones catalogadas como críticas. A su vez, se establecen algunos puntos explicativos sobre aspectos recogidos en la Ley 8/2011 y el Real Decreto 704/2011.

1.3 Finalidad y Contenido del PPE.

Los PPE son los documentos operativos donde se definen las medidas concretas a poner en marcha por los operadores críticos para garantizar la seguridad integral (física y lógica) de sus infraestructuras críticas.

Además de un índice referenciado a los contenidos del Plan, los PPE deberán contener, al menos, la siguiente información específica sobre la infraestructura a proteger:

- Organización de la seguridad.
- Descripción de la infraestructura.
- Resultado del análisis de riesgos:
 - Medidas de seguridad (tanto las existentes como las que sea necesario implementar) permanentes, temporales y graduales para las diferentes tipologías de activos a proteger y según los distintos niveles de amenaza declarados a nivel nacional.
- Plan de acción propuesto (por activo).

Los PPE deberán estar alineados con las pautas establecidas en la Política General de Seguridad del Operador reflejada en el PSO. Asimismo, los análisis de riesgos, vulnerabilidades y amenazas que se lleven a cabo, estarán sujetos a las pautas metodológicas descritas en el PSO.

1.4 Método de Revisión y Actualización.

Conforme al artículo 27 del Real Decreto por el que se aprueba el Reglamento de protección de las infraestructuras críticas, entre las obligaciones del operador, además de la elaboración y presentación del PPE al Centro Nacional de Protección de Infraestructuras Críticas (en adelante CNPIC), se incluye su revisión y actualización periódica:

- Revisión: Bial.
- Actualización: cuando se produzca una modificación en los datos incluidos dentro del PPE. En este caso, el PPE quedará actualizado cuando dichas modificaciones hayan sido validadas por el CNPIC, o en las condiciones establecidas en su normativa sectorial específica.

1.5 Protección y Gestión de la Información y Documentación.

La información asociada con los PPE y aquella relativa a los análisis de riesgos y las medidas de seguridad implantadas sobre las infraestructuras críticas a las que hacen referencia es de carácter sensible, por lo que, en este sentido, el operador deberá definir sus procedimientos de tratamiento de dicha información, así como los estándares de seguridad precisos para prestar una adecuada y eficaz protección de la información utilizados, independientemente del formato en el que ésta se encuentre.

Además, los operadores designados como críticos, deberán tratar los documentos que se deriven de la aplicación de la Ley 8/2011 y su desarrollo normativo a través del Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras, según el grado de clasificación que se derive de las citadas normas.

En virtud de la disposición adicional segunda de la Ley 8/2011, la clasificación del PPE constará de forma expresa en el instrumento de su aprobación. Una vez aprobado, el PPE tendrá la clasificación de Confidencial, siéndole de aplicación desde ese momento los requisitos y medidas de seguridad previstos en su normativa regulatoria específica.

2. Aspectos Organizativos

2.1 Delegados de Seguridad de las Infraestructuras Críticas.

Conforme al artículo 17 de la Ley 8/2011, el Operador Crítico con infraestructuras designadas como críticas o críticas europeas comunicará a las Delegaciones del Gobierno o, en su caso al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquellas se ubiquen, la persona designada como Delegado de Seguridad y su sustituto para cada una de dichas infraestructuras.

El Operador Crítico deberá hacer constar en este apartado el nombre y datos de contacto (dirección, teléfonos y email) de la persona que fue designado como Delegado de Seguridad así como de su sustituto, cumpliendo los plazos establecidos desde su designación, así como su participación a las Autoridades correspondientes, según lo establecido en el artículo 35.1 del Real Decreto 704/2011.

Sus funciones en relación con el artículo 35.2 del Real Decreto 704/2011, son las siguientes:

- Ser el enlace operativo y el canal de información con las autoridades competentes en materia relativa a la seguridad de sus infraestructuras.
- Canalizar las necesidades operativas e informativas que surjan.
- Coordinarse adecuadamente con el Responsable de Seguridad y Enlace y, en su caso, con los otros Delegados de Seguridad del Operador Crítico.

El Operador Crítico deberá reflejar en este apartado los cursos o formación que el Delegado de Seguridad haya recibido, relacionados con las habilidades necesarias para el desempeño del puesto, de acuerdo con el Plan de Formación previsto en el PSO.

2.2 Mecanismos de Coordinación.

El Operador Crítico deberá reflejar dentro de su PPE los mecanismos existentes de coordinación:

- Entre el Delegado de Seguridad de la Infraestructura Crítica (IC) con otros Delegados de otras IC's y con el Responsable de Seguridad y Enlace del propio Operador.
- Con Autoridades y terceros (Fuerzas y Cuerpos de Seguridad del Estado/ Cuerpos Policiales autonómicos y locales / CNPIC /otros).
- Con otros planes existentes del Operador (planes de continuidad de negocio, planes de evacuación, etc.).

2.3 Mecanismos y Responsables de Aprobación.

El Operador deberá incluir dentro del PPE los siguientes aspectos relativos a su aprobación interna:

- Responsables de su aprobación.
- Procedimiento que se sigue para su aprobación.
- Fecha en la que se produjo su última aprobación.

3. Descripción de la Infraestructura Crítica

3.1 Datos Generales de la Infraestructura Crítica.

El Operador Crítico deberá incluir los siguientes datos e información sobre la infraestructura a proteger:

- Generales, relativos a la denominación y tipo de instalación, propiedad y gestión de la misma.
- Sobre localización física y estructura (localización, planos generales, fotografías, componentes, etc.).

- Sobre los sistemas TIC que gestionan la IC y su arquitectura (mapa de red, mapa de comunicaciones, mapa de sistemas, etc.).

- Datos estratégicos:

- Descripción del servicio esencial que proporciona y el ámbito geográfico o poblacional del mismo.

- Relación con otras posibles infraestructuras necesarias para la prestación de ese servicio esencial.

- Descripción de sus funciones y de su relación con los servicios esenciales soportados.

3.2 Activos / Elementos de la IC.

Se incluirán en este apartado los activos que soportan la infraestructura crítica, diferenciando aquellos que son vitales de los que no lo son. En concreto se detallarán:

- Las instalaciones o componentes de la IC que son necesarios y por lo tanto vitales para la prestación del servicio esencial.

- Los sistemas informáticos (hardware y software) utilizado.

- Las redes de comunicaciones que permiten intercambiar datos y que se utilicen para dicha IC.

- Las personas o grupos de personas que explotan u operan todos los elementos anteriormente citados.

- Los proveedores críticos que son necesarios para el funcionamiento de dicha IC.

Del mismo modo, se especificarán las dependencias existentes entre los diferentes activos que soportan o componen la IC. La información anterior deberá ser la suficiente para recoger de manera explícita el alcance de la infraestructura a proteger y con el mismo nivel de granularidad que se haya establecido dentro del PSO.

3.3 Interdependencias.

En relación con el concepto de interdependencias recogido en el artículo 2. j) de la Ley, pueden existir efectos y repercusiones que afecten los servicios esenciales y las infraestructuras críticas propias y/o de otros operadores, tanto dentro del mismo sector como en ámbitos diferentes. Estas interdependencias deberán ser en todo caso consideradas en el análisis de riesgos que realicen los operadores para la IC de que se trate, en el marco del PPE.

El Operador Crítico deberá hacer referencia dentro de sus diferentes PPE a las interdependencias que, en su caso, identifique, explicando brevemente el motivo que las origina:

- Con otras infraestructuras críticas del propio Operador.
- Con otras infraestructuras críticas de otros Operadores.
- Con otras infraestructuras estratégicas que soportan el servicio esencial.

4. Resultados del Análisis de Riesgos

El Operador Crítico deberá reflejar en su PPE los resultados del análisis de riesgos realizado sobre la infraestructura crítica. Dicho análisis de riesgos deberá seguir las pautas metodológicas recogidas en su PSO.

A continuación se reflejan los contenidos mínimos relativos al análisis de riesgos realizado que el operador deberá incluir dentro del PPE.

4.1 Amenazas Consideradas.

En el marco de la normativa de protección de infraestructuras críticas, y de cara a garantizar la adecuada protección de las infraestructuras críticas, el Operador Crítico deberá considerar de forma especial aquellas amenazas de origen terrorista o

intencionado. El Operador deberá indicar expresamente las amenazas que ha considerado para la realización de los análisis de riesgos, plasmando al menos:

- Las amenazas intencionadas, tanto de tipo físico como lógico, que afecten de forma específica a alguno de los activos que soportan infraestructura crítica.
- Las amenazas que puedan afectar directamente a la infraestructura procedentes de las interdependencias identificadas, sean éstas deliberadas o no.
- Las dirigidas al entorno cercano o elementos interdependientes tanto del antepérimetro físico como lógico que puedan afectar a la infraestructura.
- Las amenazas que afecten a los sistemas de información que den soporte a la operación de la infraestructura crítica y todos los que estén conectados a dichos sistemas sin contar con las adecuadas medidas de segmentación.

4.2 Medidas de Seguridad.

El Operador deberá describir las medidas de seguridad (medidas de protección de las instalaciones, equipos, datos, software de base y aplicativos, personal y documentación) implantadas en la actualidad, con las que se ha contado para la realización del análisis de riesgos. Deberá distinguir entre las medidas de carácter permanente, y aquellas temporales y graduales.

Por medidas permanentes se entienden aquellas medidas concretas ya adoptadas por el Operador Crítico, así como aquellas que considere necesarias instalar en función del resultado del análisis de riesgo realizado respecto de los riesgos, amenazas y consecuencias/impacto sobre sus activos, dirigidas todas ellas a garantizar la seguridad integral de su instalación catalogada como crítica de manera continua.

Por medidas temporales y graduales se entienden aquellas medidas de seguridad de carácter extraordinario que reforzarán a las permanentes y que se deberán implementar a raíz de la activación de alguno de los niveles de seguridad establecidos respectivamente en el Plan Nacional de Protección de las Infraestructuras Críticas (artículo 16.3 del RD 704/2011), o bien como consecuencia de las comunicaciones que las autoridades competentes puedan efectuar al Operador Crítico en relación con una amenaza concreta y temporal sobre la instalación por él gestionada.

Dichas medidas deberán permanecer activas durante el tiempo que esté establecido el nivel de alarma, modificándose gradualmente en función de dicho nivel.

Para su mejor comprensión, se recomienda una aproximación por capas, especificando para cada nivel las medidas de prevención y protección, el tiempo de respuesta y el tiempo de recuperación.

En concreto, el Operador deberá describir las medidas de que dispone relativas a:

4.2.1 Medidas Organizativas o de Gestión.

El Operador deberá indicar si dispone de al menos de las siguientes medidas organizativas o de gestión, y el alcance de cada una de ellas:

- Análisis de Riesgos: Evaluación y valoración de las amenazas, impactos y probabilidades para obtener un nivel de riesgo.
- Definición de roles y responsabilidades: Asignación de responsabilidades en materia de seguridad.
- Cuerpo normativo definido: Políticas, procedimientos y estándares de seguridad.
- Normas y/o regulaciones de aplicación a la infraestructura crítica, así como identificación de su nivel de cumplimiento.
- Certificación, acreditación y evaluación de seguridad obtenidas para la infraestructura crítica.

4.2.2 Medidas Operacionales o Procedimentales.

El operador deberá indicar si dispone de al menos las siguientes medidas operacionales o procedimentales, y el alcance de cada una de ellas.

- Procedimientos para la realización, gestión y mantenimiento de activos:

- Procedimiento de inventariado (Identificación/Catalogación/etc.):
 - Activos físicos.
 - Activos lógicos.
- Procedimiento de gestión continua de activos físicos y lógicos (Alta/Baja/Modificación).
 - Etc.
- Procedimientos de formación, concienciación y capacitación (tanto general como específica) para:
 - Empleados/Operarios.
 - Personal de seguridad.
 - Etc.
- Procedimientos de Contingencia / Recuperación, en función de los escenarios de contingencia que hayan sido definidos.
 - Procedimientos operativos para la monitorización, supervisión y evaluación/ auditoría de:
 - Activos Físicos de la infraestructura (Alcance / Operación / Seguimiento).
 - Activos Lógicos o de sistemas de operación (Alcance / Operación / Seguimiento).
 - Procedimientos para la gestión de acceso:
 - Gestión de usuarios: Altas, bajas y modificaciones, procesos de selección, régimen interno, procedimientos de cese.
 - Control de accesos temporales:
 - De personas, vehículos, etc... al recinto general o a recintos restringidos.
 - Identificadores de usuario temporal de los sistemas (mantenimiento...).
 - Control de entradas y salidas:
 - Paquetería, correspondencia, etc...
 - Soportes, equipos e información (medidas y tecnologías de prevención de fuga de información).
- Procedimientos operacionales del personal de seguridad (funciones, horarios, dotaciones, etc.).
- Procedimientos de gestión y respuesta de incidentes.

4.2.3 Medidas De protección o Técnicas.

- Medidas de Prevención y Detección:
 - Medidas y elementos de seguridad física y electrónica para la protección del perímetro y control de accesos:
 - Vallas, zonas de seguridad, detectores de intrusos, cámaras de video vigilancia / CCTV, puertas y esclusas, cerraduras, lectores de matrículas, arcos de seguridad, tornos, scanners, tarjetas activas, lectores de tarjetas, etc.
 - Medidas y elementos de seguridad lógica:
 - Firewalls, DMZ, IPSs, segmentación y aislamiento de redes, cifrado, VPNs, elementos y medidas de control de acceso de usuarios (tokens, controles biométricos, etc.), medidas de instalación y configuración segura de elementos técnicos, correladores de eventos y logs, protección frente Malware, etc.
 - Otros.
- Coordinación y Monitorización:
 - Centro de Control de Seguridad (control de alarmas, recepción y visionado de imágenes, etc.).

- Equipos de vigilancia (turnos, rondas, volumen, etc.).
- Sistemas de comunicación.
- Otros.

4.3 Valoración de Riesgos.

En este apartado se describirán las principales conclusiones obtenidas en el análisis de riesgos. Para cada par activo / amenaza se deberá especificar la valoración efectuada, sobre la base de los criterios especificados en la metodología de análisis de riesgos detallada en el PSO. Dentro de este apartado deberá incluirse, para cada par activo / amenaza, la siguiente información:

- Quién ha evaluado / aprobado el riesgo y la estrategia de tratamiento asociada.
- Criterios de valoración de riesgos adoptados.
- Fecha del último análisis llevado a cabo.
- Resultado / conclusión sobre el nivel de riesgo soportado.

En particular, deberán detallarse los riesgos asumidos con niveles de impacto elevado y baja probabilidad, que deberán ser validados por el CNPIC.

5. Plan de Acción Propuesto (por Activo)

En caso de ser pertinente y preverse la disposición de medidas complementarias a las existentes a implementar en los próximos tres años, se deberá describir, como parte integrante del PPE:

- La enumeración de las medidas complementarias a disponer (físicas o lógicas).
- Una explicación de la operativa resultante para cada tipo de protección (físico y lógico) y para cada uno de los horarios significativos, según el orden del apartado 4.2.

El Operador deberá especificar el conjunto detallado de medidas a aplicar para proteger el activo como consecuencia de los resultados obtenidos en el análisis de riesgos. En concreto, deberá incluir la siguiente información:

- Acción propuesta, con detalle de su ámbito (alcance) de aplicación.
- Activo de aplicación.
- Responsables de su implantación, plazos, mecanismos de coordinación y seguimiento, etc.
- Carácter permanente, temporal o gradual de la medida.

6. Documentación Complementaria

El Operador Crítico incorporará como anexo la planimetría general de la instalación o sistema y de sus sistemas de información, así como aquellos otros planos que incorporen la ubicación de las medidas de seguridad implementadas. A su vez, se podrá adjuntar aquella otra información que se pueda generar de los diferentes apartados de este documento.

Se hará una breve referencia a todos aquellos planes de diferente tipo (emergencia, autoprotección, etc.), que afecten a la instalación o sistema con el fin de establecer una adecuada coordinación entre ellos, así como toda aquella normativa y buenas prácticas que regulen el buen funcionamiento del servicio esencial prestado por esa infraestructura y los motivos por los cuales le son de aplicación.

La normativa a incluir comprenderá tanto las de rango nacional, autonómico, europeo e internacional, como las sectoriales, relativas a:

- Seguridad Física.
- Seguridad Lógica.
- Seguridad de la Información en cualquiera de sus ámbitos.
- Seguridad Personal.
- Seguridad Ambiental.
- Autoprotección y Prevención de Riesgos Laborales.