GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

SECRETARÍA DE ESTADO DE SEGURIDAD

GABINETE DE COORDINACIÓN

CONTENIDOS MÍNIMOS PLAN DE PROTECCIÓN ESPECÍFICO (PPE)

CNPIC
CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

***Texto refundido a partir de las siguientes Resoluciones**:*

- *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.*

- *Resolución de 29 de noviembre de 2011, de la Secretaría de Estado de Seguridad, por la que se corrigen errores en la de 15 de noviembre de 2011, 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.*

Contenidos Mínimos

Plan de Protección Específico (PPE)

Índice

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 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 delos servicios proporcionados por dicho operador a través de esa infraestructura crítica (IC).

- Desarrollo de los criterios de aplicación de las diferentes medidas de seguridad quese 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: Bienal

● Actualización: cuando se produzca una modificación en los datos incluidos dentrodel 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 08/2011, la clasificación del PPE constará de forma expresa en el instrumento de su aprobación. A tal fin, el tratamiento de los PPE deberá estar regido conforme a las orientaciones publicadas por la Autoridad Nacional para la Protección de la Información Clasificada del Centro Nacional de Inteligencia en lo que se refiere al manejo y custodia de información clasificada con grado de Difusión Limitada.

Las orientaciones de referencia se encuentran recogidas en los siguientes documentos:

SEGURIDAD DOCUMENTAL

OR-ASIP-04-01.03 – Orientaciones para el Manejo de Información Clasificada con Grado de Difusión Limitada.

SEGURIDAD EN EL PERSONAL

OR-ASIP-02-02.02 – Instrucción de Seguridad del Personal para acceso a Información Clasificada.

OR-ASIP-01-01.02 – Orientaciones para el Plan de Protección de una Zona de Acceso Restringido.

OR-ASIP-01-02.02 – Orientaciones para la Constitución de Zonas de Acceso Restringido.

2. Aspectos Organizativos

2.1 Delegados de Seguridad de las Infraestructuras

Conforme al artículo 17 de la Ley 8/2011, el Operador Crítico con infraestructuras designadas como críticas o criticas 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

3.1 Datos Generales de la Infraestructura

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 procedente de las interdependencias identificadas, sean éstas deliberadas o no.
- Las dirigidas al entorno cercano o elementos interdependientes tanto del ante-perímetro 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 continúa 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 Valores de Riesgo

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.