



GOBIERNO
DE ESPAÑA

MINISTERIO
DEL INTERIOR

SECRETARÍA DE ESTADO
DE SEGURIDAD

GABINETE DE
COORDINACIÓN Y ESTUDIOS

CONTENIDOS MÍNIMOS

PLAN DE SEGURIDAD DEL OPERADOR (PSO)

Texto elaborado a partir de la siguiente Resolución:

Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos.



CNPIC

CENTRO NACIONAL PARA LA PROTECCIÓN
DE LAS INFRAESTRUCTURAS CRÍTICAS



CONTENIDOS MÍNIMOS

PLAN DE SEGURIDAD DEL OPERADOR (PSO)

ÍNDICE

| | |
|--|-----------|
| 1. INTRODUCCIÓN..... | 2 |
| 1.1 BASE LEGAL..... | 2 |
| 1.2 OBJETIVO DE ESTE DOCUMENTO..... | 3 |
| 1.3 FINALIDAD Y CONTENIDO DEL PSO..... | 3 |
| 1.4 MÉTODO DE REVISIÓN Y ACTUALIZACIÓN..... | 3 |
| 1.5 PROTECCIÓN Y GESTIÓN DE LA INFORMACIÓN Y DOCUMENTACIÓN..... | 4 |
| 2. POLÍTICA GENERAL DE SEGURIDAD DEL OPERADOR Y MARCO DE GOBIERNO | 5 |
| 2.1 POLÍTICA GENERAL DE SEGURIDAD DEL OPERADOR CRÍTICO | 5 |
| 2.2 MARCO DE GOBIERNO DE SEGURIDAD | 7 |
| 2.2.1 Organización de la Seguridad y Comunicación..... | 7 |
| 2.2.2 Formación y Concienciación..... | 9 |
| 2.2.3 Modelo de Gestión Aplicado..... | 10 |
| 2.2.4 Comunicación..... | 11 |
| 3. RELACIÓN DE SERVICIOS ESENCIALES PRESTADOS POR EL OPERADOR CRÍTICO | 12 |
| 3.1 IDENTIFICACIÓN DE LOS SERVICIOS ESENCIALES..... | 12 |
| 3.2 MANTENIMIENTO DEL INVENTARIO DE SERVICIOS ESENCIALES | 12 |
| 3.3 ESTUDIO DE LAS CONSECUENCIAS DE LA INTERRUPCIÓN DEL SERVICIO ESENCIAL | 13 |
| 3.4 INTERDEPENDENCIAS..... | 13 |
| 4. METODOLOGÍA DE ANÁLISIS DE RIESGOS..... | 14 |
| 4.1 DESCRIPCIÓN DE LA METODOLOGÍA DE ANÁLISIS | 14 |
| 4.2 TIPOLOGÍAS DE ACTIVOS QUE SOPORTAN LOS SERVICIOS ESENCIALES..... | 15 |
| 4.3 IDENTIFICACIÓN Y EVALUACIÓN DE AMENAZAS | 15 |
| 4.4 VALORACIÓN Y GESTIÓN DE RIESGOS..... | 16 |
| 5. CRITERIOS DE APLICACIÓN DE MEDIDAS DE SEGURIDAD INTEGRAL | 16 |
| 6. DOCUMENTACIÓN COMPLEMENTARIA | 17 |
| 6.1 NORMATIVA, BUENAS PRÁCTICAS Y REGULATORIA..... | 17 |
| 6.2 COORDINACIÓN CON OTROS PLANES | 17 |





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/o 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 (órgano superior responsable del Sistema de Protección de Infraestructuras Críticas Nacionales, conforme al artículo 6 de la Ley 8/2011), a través del CNPIC, del establecimiento y puesta a disposición de los operadores críticos 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 un operador crítico 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, información sobre:

- 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 de ciberseguridad).
- 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 para la Protección de las 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.

Independientemente de todo ello, en el caso de que varíen algunas de las circunstancias indicadas en el PSO (modificación de datos, identificación de nuevas infraestructuras críticas, baja de infraestructuras críticas, cese de condiciones para ser considerado operador crítico, etc...), el operador deberá trasladar la información oportuna al CNPIC, a través de los canales habilitados al efecto (Sistema HERMES / PoC oficial), en el plazo máximo de diez días a partir de las circunstancias variadas.

1.5 PROTECCIÓN Y GESTIÓN DE LA INFORMACIÓN Y DOCUMENTACIÓN

La información es un valor estratégico para cualquier organización, siendo ésta de carácter sensible, por lo que en este sentido, el operador debe definir sus procedimientos de gestión y tratamiento, así como los estándares de seguridad precisos para prestar una adecuada y eficaz protección de esa 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 08/2011, la clasificación del PSO constará de forma expresa en el instrumento de su aprobación. A tal fin, el tratamiento de los PSO 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-04-01.04 – Orientaciones para el Manejo de Información Clasificada con Grado de Difusión Limitada.





SEGURIDAD EN EL PERSONAL

OR-ASIP-04-02.02 – Instrucción de Seguridad del Personal para acceso a Información Clasificada.

SEGURIDAD FÍSICA

OR-ASIP-01-01.03 – Orientaciones para el Plan de Protección de una Zona de Acceso Restringido.

OR-ASIP-01-02.03 – Orientaciones para la Constitución de Zonas de Acceso Restringido.

SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

OR-ASIP-03-01.04 – Orientaciones para la Acreditación de Sistemas de Información y Comunicaciones para el manejo de Información Clasificada.

2. POLÍTICA GENERAL DE SEGURIDAD DEL OPERADOR Y MARCO DE GOBIERNO

2.1 POLÍTICA GENERAL DE SEGURIDAD DEL OPERADOR CRÍTICO

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 dirigido 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 la Organización. El operador deberá reflejar sobre qué partes de su Organización es aplicable la Política de Seguridad de protección de infraestructuras críticas,



sin perder de vista que la misma ha de tener un carácter integral, considerando tanto la seguridad física como la ciberseguridad.

- **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 con capacidad suficiente para implantarla en la organización, así como su firme y explícito compromiso con la protección de los servicios esenciales prestados, compromiso que se debe ver reflejado en el propio plan.

- **Carácter Integral de la Seguridad:** La seguridad física y la ciberseguridad 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, y 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, indicando en todo caso el procedimiento por el que se pretende alcanzar dicha seguridad integral: aspectos concretos de la organización, estructuras, procedimientos, etcétera. En este sentido, una respuesta integral a las diferentes amenazas existentes requiere la aplicación coordinada de medidas de seguridad física y ciberseguridad.
- **Actualización de la Política General de Seguridad del Operador:** Al ser la política de seguridad 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 su Política de Seguridad, incluyendo la periodicidad y el responsable de llevar a cabo estas acciones.





2.2 MARCO DE GOBIERNO DE SEGURIDAD

2.2.1 Organización de la Seguridad y Comunicación

El operador crítico debe designar a un Responsable de Seguridad y Enlace y a los Delegados de Seguridad en cada una de las infraestructuras críticas identificadas, así como a los sustitutos de ambos, de acuerdo a los requisitos establecidos en la Ley 8/2011. Deberá, por tanto, asegurar que se encuentren en un nivel jerárquico suficiente dentro de su estructura organizativa, 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. Así mismo, deberá asegurar la presencia física del delegado de seguridad en la infraestructura en un tiempo prudencial, en caso de que ello sea necesario.

En este apartado, el operador crítico deberá describir su organigrama de seguridad (comprendiendo tanto la Seguridad Física como la Ciberseguridad), con indicación de las figuras recogidas en la Ley, así como los niveles jerárquicos que les correspondan en su estructura organizativa. Dicho organigrama debe incluir la ubicación física, estructura, jerarquía, órgano de gobierno e interrelación de todas las áreas de la organización con responsabilidad en cada uno de los ámbitos de la seguridad corporativa. 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. En este sentido, el operador crítico deberá presentar:

- Un organigrama general, donde se identifique la estructura de seguridad corporativa.
- Un organigrama específico de la estructura de seguridad que integre la información sobre las distintas funciones que desempeña en la organización.

En su caso, el operador crítico deberá señalar los comités u órganos de decisión existentes en materia de seguridad, así como las funciones de cada uno de ellos.

Igualmente, se reflejarán los procedimientos de gestión y mantenimiento de la seguridad, haciendo constar si éstos son de carácter propio o son subcontratados. En este último caso, será necesario relacionar la empresa o empresas subcontratadas, las certificaciones en materia de seguridad con las que cuentan aquéllas, la sede desde la que se ejercen dichos servicios contratados, así como los servicios y compromisos acordados entre ambos. De igual forma, se definirá la metodología mediante la cual se





lleva a cabo la comprobación del cumplimiento por parte de la empresa contratada, con los protocolos de seguridad implementados en su caso por el operador.

En el campo de la ciberseguridad, y en lo relacionado con la protección de infraestructuras críticas, el CERT de Seguridad e Industria (en adelante CERTSI) es el responsable de la resolución de incidencias cibernéticas que puedan afectar a la prestación de los servicios esenciales gestionados por los operadores críticos.

El CERTSI, en aplicación del Acuerdo Marco suscrito entre la Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, da apoyo directo al CNPIC en todo lo relativo a la prevención y reacción ante incidentes que puedan afectar a las redes y sistemas de los operadores de infraestructuras críticas y a la disponibilidad de los servicios que éstos prestan. Para todo ello, y previa suscripción de un acuerdo de confidencialidad entre las partes (operador crítico – CNPIC – CERTSI), dicho CERT podrá proporcionar servicios de prevención, detección, alerta temprana y respuesta a incidentes en apoyo a los departamentos encargados de esta labor en el seno de cada organización.

2.2.1.1 El Responsable de Seguridad y Enlace

Conforme al artículo 16.2 de la Ley, el operador crítico deberá nombrar, en el plazo de tres meses desde su designación como tal, al Responsable de Seguridad y Enlace de la organización, que deberá estar habilitado 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. Tal nombramiento deberá ser comunicado a la Secretaría de Estado de Seguridad, a través del CNPIC.

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, con idénticas condiciones, en ausencia del titular. 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 entre el operador crítico y el CNPIC.

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 aquéllas se ubiquen, la persona designada como Delegado de Seguridad y su sustituto. Esta comunicación deberá realizarse también al CNPIC, en el plazo de tres meses desde la notificación oficial de que es propietario o gestor de al menos una infraestructura crítica o crítica europea.

El operador crítico deberá hacer constar en este apartado el nombre y datos de contacto (dirección, teléfonos y email) de la persona designada como Delegado de Seguridad, así como de su sustituto, con idénticas condiciones, 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.

Es aconsejable que tanto el Delegado de Seguridad como su sustituto sean poseedores de titulación relativa a la rama de seguridad, además de pertenecer al departamento de seguridad de la entidad en cuestión.

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, a nivel infraestructura, entre el operador y las autoridades competentes.

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 reflejará en este apartado el Plan de Formación previsto para el personal relacionado con la protección de las infraestructuras críticas, indicando la





duración, objetivos que se pretende conseguir, mecanismos de evaluación que se contemplan para el mismo y periodos de actualización. Así mismo, se incluirá el responsable del plan y la capacitación del mismo.

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 operador crítico deberá reflejar en este apartado su participación en ejercicios de simulación en incidentes de seguridad (físicos y cibernéticos), y la periodicidad programada para tales ejercicios.

El personal implicado directamente en la protección de los servicios esenciales e infraestructuras críticas deberá ser formado para alcanzar conocimientos, a nivel básico:

- Sobre seguridad integral (seguridad física y ciberseguridad).
- Sobre autoprotección.
- Sobre seguridad del medio ambiente.
- Sobre habilidades organizativas y de comunicación.
- Sobre sus responsabilidades/actuaciones en caso de materializarse un incidente, o en el caso de que se active un nivel de amenaza 4 ó 5 del Plan de Prevención y Protección Antiterrorista y/o del Plan Nacional de Protección de las Infraestructuras Críticas.

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 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 la Política de Seguridad marcada, el operador crítico deberá recoger dentro del PSO su modelo de gestión elegido, que deberá contemplar como mínimo:





- Una implementación de controles de seguridad alineada con las prioridades y necesidades evaluadas.
- Una evaluación y monitorización continua de la seguridad, con identificación de procesos y periodos.
- En el supuesto de que el operador crítico haya diseñado un sistema de gestión y/o la evaluación de la seguridad de las tecnologías de la información, de acuerdo a algún estándar de referencia internacional se debe indicar éste, así como las certificaciones que posee dicho sistema y el organismo certificador.

2.2.4 Comunicación

El operador crítico deberá recoger explícitamente en este apartado los procedimientos establecidos para la comunicación e intercambio de información relativa a la protección de infraestructuras críticas, de la siguiente manera:

Comunicación al CNPIC:

- De aquellos incidentes o situaciones que puedan poner en riesgo o comprometer la seguridad de alguna de las infraestructuras de la que el operador es gestor y/o propietario, conforme al protocolo de comunicación de incidentes PIC elaborado por este Centro y puesto a disposición de los operadores críticos.
- De aquellas variaciones de carácter organizativo, de planificación o estructural que se produzcan en el seno del propio operador y que afecten de alguna manera a las infraestructuras críticas objeto de protección (por ejemplo, ajuste de cartera de servicios, fusiones, adquisiciones o ventas de activos, cambios técnicos, modificación de infraestructuras, cambio de instalaciones, etc.).

Comunicación al CERTSI:

- A través de la Oficina de Coordinación Cibernética del Ministerio del Interior (OCC), de los incidentes que puedan comprometer la seguridad cibernética de los sistemas y redes del operador crítico y la disponibilidad de los servicios que presta. Todo ello, conforme al protocolo de comunicación de incidentes PIC elaborado por el CNPIC y puesto a disposición de los operadores críticos.





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. En caso de grupos empresariales, se identificará claramente, con nombre y CIF, cuál de las empresas es el operador crítico.
- Estructura organizativa y societaria de todo el Grupo (en el caso de grupos empresariales).
- Presencia geográfica en los ámbitos nacional e internacional, con un resumen de las Comunidades Autónomas donde presten sus servicios esenciales, así como de aquellos países donde presten servicios similares.
- 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, al menos bienalmente, 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, cambios técnicos, modificación de infraestructuras, cambio de instalaciones, 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:

- Alteración o interrupción temporal del servicio prestado.
- Destrucción parcial o total de la infraestructura que gestiona el servicio.

Adicionalmente, deberá identificar claramente, para cada uno de los casos anteriores, la siguiente información:

- Extensión geográfica y número de personas que pueden verse afectadas.
- Efecto sobre operadores y servicios esenciales dependientes.
- Existencia de alternativas de prestación del servicio esencial o mecanismos de contingencia proporcionados por el propio operador y nivel de degradación que conllevan.

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 otros sectores 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.

El operador crítico deberá hacer referencia a las interdependencias que identifique, explicando en líneas generales el motivo que origina dichas dependencias:

- Entre sus propias instalaciones o servicios.



- Con operadores del mismo sector.
- Con operadores de distintos sectores.
- Con operadores de otros países, del mismo sector o no.
- Con sus proveedores de servicio dentro de la cadena de suministros.
- Con los proveedores de servicios TIC contratados, tales como: proveedor(es) de telecomunicaciones, Centros de Proceso de Datos, servicios de seguridad (Centro de Operaciones de Seguridad, CERT privado, etcétera) y cualesquiera otros que se considere, especificando para cada uno de ellos el nombre del proveedor, los servicios contratados, acuerdos de nivel de servicio (SLA) y cumplimiento del servicio provisto con la política general de seguridad del operador.

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 plasmará la metodología o metodologías de análisis de riesgos empleadas por el operador crítico. Dichas metodologías deberán estar internacionalmente reconocidas, garantizar la continuidad de los servicios proporcionados por dicho operador y contemplar, de una manera global, tanto las amenazas físicas como lógicas existentes contra la totalidad de sus activos críticos. Todo ello, 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 diferentes Planes de Protección Específicos (PPE) que se deriven tras la designación de sus infraestructuras críticas. Al menos, se aportará la siguiente información:

- Etapas esenciales.
- Algoritmos de cálculo empleados.
- 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 aquéllos que son críticos de los que no lo son.

Las tipologías de activos a considerar serán, al menos:

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

El objeto de esta sección es 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 detalle 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 tener como referencia el árbol de amenazas proporcionado por el CNPIC, considerando 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, en su caso.
- Las procedentes de interdependencias, que puedan afectar directamente a los servicios esenciales, sean estas deliberadas o no.

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 categorías de clasificación de los riesgos.
- Metodología de selección de estrategia (reducción, eliminación, transferencia, etc.)
- Plazos para la implantación 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 aquéllas 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 la normativa general y sectorial, tanto de rango nacional, autonómico, europeo e internacional, relativas a:

- Seguridad Física.
- Ciberseguridad.
- Seguridad de la Información.
- 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, ciberseguridad, autoprotección, emergencias, etc.) que puedan coordinarse con el Plan de Seguridad del operador y los respectivos Planes de Protección Específicos que serán activados en el caso de que las medidas preventivas fallen y se produzca un incidente. Así mismo, debe dejarse constancia de la coordinación existente con el Plan Nacional para la Protección de las Infraestructuras Críticas.

---oo00oo----

