La Ley PIC y la protección de infraestructuras críticas.

Formación, acompañamiento y desarrollo de los Planes de Seguridad del Operador (PSO) y los Planes de Protección Específicos (PPE)

Dentro del marco normativo asociado a la ciberseguridad industrial, tiene especial importancia en España la **Ley de Protección de Infraestructuras Críticas (Ley PIC 8/2011)** complementada por el Real Decreto 704/2011.

Los dos grandes objetivos de esta norma son:

- Catalogar el **conjunto de infraestructuras que prestan servicios esenciales** a nuestra sociedad.
- Diseñar un **planeamiento que contenga medidas de prevención y protección** eficaces contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la **seguridad física** como en el de la **seguridad de las tecnologías de la información y las comunicaciones.**

¿Cómo define la Ley PIC las infraestructuras críticas, los servicios esenciales y las infraestructuras estratégicas?

La Ley PIC define como **infraestructuras críticas** aquellas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los **servicios esenciales**. Estos a su vez, se definen como los servicios necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

Por último define como **infraestructuras estratégicas** las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

¿Qué sectores se han designado como prestadores de servicios esenciales?

Administración, agua, alimentación, energía, espacio, industria química, industria nuclear, instalaciones de investigación, salud, sistema financiero y tributario, tecnologías de la información y las comunicaciones y transporte.

¿Qué se entiende por protección de infraestructuras críticas?

La protección de infraestructuras críticas se define como el conjunto de actividades destinadas a **asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas** con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia.

¿Cuáles son las principales aportaciones de la Ley PIC?

1. **Crear el Sistema Nacional de Protección de Infraestructuras Críticas** que contiene aquellas instituciones, órganos y empresas, procedentes tanto del sector público como del privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos. Estos son: los operadores críticos, el CNPIC (Centro Nacional para la Protección de Infraestructuras Críticas), ministerios, CCAA, corporaciones locales, grupos de trabajo sectoriales, etc.

2. **Poner las bases para el Sistema de Planificación PIC**. Se trata de un conjunto de textos normativos que definen una serie de medidas para la protección de las infraestructuras críticas que se concretan en actuaciones que deben llevar a cabo los integrantes del Sistema de Protección de Infraestructuras Críticas.
   Teniendo en cuenta lo establecido por la Ley PIC, se desarrollarán tantos **PES (Planes Estratégicos Sectoriales)** como sectores se hayan definido. A su vez, las empresas que sean designadas como operadores críticos deberán presentar un **PSO (Plan de Seguridad del Operador) y un PPE (Plan de Protección Específico)** respecto a todas sus infraestructuras clasificadas como críticas. Por último, la administración competente, apoyada por el cuerpo policial, deberá desarrollar un **PAO (Plan de Apoyo Operativo).**

3. **Generar el Catálogo Nacional de Infraestructuras Estratégicas** que contiene la información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras estratégicas existentes en el territorio nacional. Para facilitar esta información se ha desarrollado el sistema **HERMES** a través del cual, los operadores críticos podrán dar de alta, acceder y modificar la información relativa a aquellas infraestructuras que gestionen.

4. **Establecer el CERT (Cyber Emergency Response Team) para la gestión de incidentes de ciberseguridad**. Apoyando al CNPIC, INTECO (Instituto Nacional de Tecnologías de la Comunicación) se convierte en el CERT especializado en la gestión de incidentes relacionados con las infraestructuras críticas a nivel nacional. La misión del CERT es dar respuesta a incidentes de seguridad especializado en el análisis y gestión de problemas e incidencias de seguridad tecnológica.

¿Cómo puede afectar la Ley PIC a mi empresa u organismo?

¿Puede mi empresa u organismo ser designado como operador crítico? ¿Quién realiza esta comunicación?

Los operadores críticos son las entidades u organismos responsables de las inversiones o del funcionamiento de una instalación, red, sistema, o equipo físico o de tecnología de la información **designada como infraestructura crítica** por proporcionar un servicio indispensable para la sociedad.

Para la designación de una empresa u organismo como operador crítico, bastará con que **al menos una de las infraestructuras por él gestionadas reúna la consideración de infraestructura crítica.**

El CNPIC es el encargado de realizar la comunicación, elaborando una propuesta de resolución y notificándola al titular o administrador de las infraestructuras.

¿A qué me obligan los Planes de Seguridad del Operador (PSO) y los Planes Específicos de Protección (PPE)?

La Ley PIC dispone el alcance, contenidos esenciales y plazos de elaboración, respuesta y revisión de los **PSO y los PPE**. En la siguiente se resumen:

Aspecto	PSO	PPE
Alcance	Políticas generales	Medidas concretas (adoptadas o a adaptar) para garantizar seguridad física y lógica
Plazo de elaboración a partir de notificación CNPIC	6 meses	4 meses
Contenidos esenciales	Metodología de análisis de riesgo y criterios de aplicación de medidas de seguridad	Medidas permanentes de protección y medidas de seguridad temporales y graduadas
Órgano resolutorio	Secretaría Estado u órgano delegado tras informe del CNPIC	Secretaría Estado u órgano delegado tras informe del CNPIC
Plazo respuesta	Máximo de 2 meses	Máximo de 2 meses
Plazo revisión	Cada dos años	Cada dos años

Industrial Cybersecurity by Logitek ayuda a los operadores críticos a desarrollar los Planes de Seguridad del Operador (PSO) y los Planes de Protección Específicos (PPE) asociados al cumplimiento de la Ley 8/2011 de Protección de Infraestructuras Críticas.

La elaboración de los PSO y los PPE es una tarea compleja que requiere la coordinación e involucración de diferentes áreas de una organización. Además, aunque **el plazo proporcionado para presentar dichos planes (6 meses para los PSO y 4 meses para los PPE)** parece razonable, las tareas cotidianas vinculadas al operador crítico, pueden hacer que dichos planes no se lleven a cabo en el tiempo determinado o con el alcance más completo y adecuado.

>Desarrollando de forma integral ambos planes

En el caso de los **PSO**, definiendo la política general de seguridad del operador y su marco de gobierno; identificando los servicios esenciales que presta; implantando una metodología de análisis de riesgo y desarrollando los criterios de aplicación de medidas de seguridad integral.

En el caso de los **PPE**, definiendo la organización de la seguridad asociada al operador crítico; describiendo los datos generales, activos, elementos e interdependencias de las infraestructuras que hayan sido designadas como críticas; identificando las amenazas internas o externas, físicas o lógicas, intencionadas o aleatorias; detallando las medidas de seguridad y valores de riesgo y proponiendo las medidas a aplicar para proteger los activos críticos como consecuencia de los resultados obtenidos en el análisis de riesgos.

>Acompañando al operador crítico en el desarrollo de determinados aspectos

En este caso el operador crítico determina el grado de involucración de los **consultores de Industrial Cybersecurity by Logitek,** detallando qué aspectos se quieren desarrollar de forma conjunta.

>Realizando una acción formativa al operador crítico.

Al operador crítico se le proporciona **una guía práctica personalizada que le ayude a elaborar tanto su PSO como el PPE.** Para ello se realiza una primera jornada de consultoría que permita conocer con más profundidad la/las infraestructuras críticas designadas, para posteriormente llevar a cabo una sesión de formación de un día de duración.

Dr. Fernando Sevillano | fernando.sevillano@logitek.es | Industrial Cybersecurity Manager